Original text

Contribute a better translation

Kali Linux Revelado

Dominar las pruebas de penetración Distribución

Kali Linux Revelado

Dominar las pruebas de penetración Distribución

por Raphaël Hertzog, Jim O'Gorman y Mati Aharoni

Kali Linux revelado

Copyright © 2017 Raphaël Hertzog, Jim O'Gorman y Mati Aharoni

Este libro está licenciado bajo una Licencia Creative Commons Reconocimiento-CompartirIgual 3.0 Unported.

[2] http://creativecommons.org/licenses/by-sa/3.0/

Algunas secciones de este libro toman prestado contenido del "Manual del administrador de Debian, Debian Jessie de Discovery to Mastery "escrito por Raphaël Hertzog y Roland Mas, que está disponible aquí:

[2] https://debian-handbook.info/browse/stable/

A los fines de la licencia CC-BY-SA, Kali Linux Revealed es una adaptación del administrador de Debian Manual.

"Kali Linux" es una marca registrada de Offensive Security. Cualquier uso o distribución de este libro, modificado o no, debe cumplir con la política de marcas definidas aquí:

[2] https://www.kali.org/trademark-policy/

Todos los derechos no otorgados explícitamente arriba están reservados.

ISBN: 978-0-9976156-0-9 (rústica)

Prensa Offsec
19701 Bethel Church Road, # 103-253
Cornelius NC 28031
Estados Unidos
www.offensive-security.com

Número de control de la Biblioteca del Congreso: 2017905895

La información en este libro se distribuye "tal cual", sin garantía. Si bien todas las precauciones ha sido tomado en la preparación de este trabajo, ni los autores ni Offsec Press tendrán ninguna responsabilidad. ity a cualquier persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directamente o indirectamente por la información contenida en el mismo.

Debido a la naturaleza dinámica de Internet, cualquier dirección web o enlace contenido en este libro puede tener

cambiado desde la publicación y puede que ya no sea válido.

Impreso en los Estados Unidos de América.

Tabla de contenido

1. Acerca de Kali Linux 1

1.1 Un poco de historia . . . 2
1.2 Relación con Debian . . . 4 4
1.2.1 El flujo de paquetes . . . 4 4
1.2.2 Gestión de la diferencia con Debian . . . 4 4
1.3 Propósito y casos de uso . . . 5 5
1.4 Características principales de Kali Linux . . . 7 7
1.4.1 Un sistema en vivo . . . 8
1.4.2 Modo forense . . . 8
1.4.3 Un kernel de Linux personalizado . . . 8
1.4.4 Completamente personalizable . . . 9 9
1.4.5 Un sistema operativo confiable . . . 9 9
1.4.6 Utilizable en una amplia gama de dispositivos ARM . . . 9 9
1.5 Políticas de Kali Linux . . . 9 9
1.5.1 Usuario raíz único por defecto . . . 10
1.5.2 Servicios de red deshabilitados por defecto . . . 10
1.5.3 Una colección curada de aplicaciones . . . 10
1.6 Resumen . . . 11

2. Comenzando con Kali Linux 13

2.1 Descargando una imagen ISO de Kali . . . 14
2.1.1 Dónde descargar . . . 14
2.1.2 Qué descargar . . . 14
2.1.3 Verificación de integridad y autenticidad . . . dieciséis
Confiar en el sitio web protegido por TLS . . . 17
Confiando en la Web de confianza de PGP . . . 17
2.1.4 Copiar la imagen en un DVD-ROM o llave USB . . . 19
Crear una unidad USB de arranque Kali en Windows . . . 19
Creación de una unidad USB de arranque Kali en Linux . . . 20
Creación de una unidad USB de arranque Kali en OS X / macOS . . . 23
2.2 Arranque de una imagen ISO de Kali en modo en vivo . . . 24
2.2.1 En una computadora real . . . 24
2.2.2 En una máquina virtual . . . 24

Observaciones preliminares . . . 25
VirtualBox . . . 26
VMware . . . 36
2.3 Resumen . . . 43

3. Fundamentos de Linux 47

3.1 ¿Qué es Linux y qué está haciendo? . . . 48

3.1.1 Conducción de hardware
3.1.2 Sistemas de archivos unificadores 48 49
3.1.3 Procesos de gestión 50
3.1.4 Gestión de derechos 51
3.2 La línea de comando 51
3.2.1 Cómo obtener una línea de comando 51
3.2.2 Conceptos básicos de la línea de comandos: exploración del árbol de directorios y administración de archivos 52
3.3 El sistema de archivos 54
3.3.1 El estándar de jerarquía del sistema de archivos 54
3.3.2 Directorio de inicio del usuario 55
3.4 Comandos útiles 56
3.4.1 Visualización y modificación de archivos de texto 56
3.4.2 Búsqueda de archivos y dentro de archivos 56
3.4.3 Procesos de gestión 57
3.4.4 Derechos de gestión 57
3.4.5 Obtener información del sistema y registros 60 60
3.4.6 Descubriendo el hardware 61
3.5 Resumen 62

4. Instalación de Kali Linux sesenta y cinco

4.1 Requisitos mínimos de instalación 66
4.2 Instalación paso a paso en un disco duro 66
4.2.1 Instalación simple 66
Arranque e inicio del instalador 66
Seleccionando el idioma 68
Seleccionando el país 69
Selección de la distribución del teclado 70
Detección de hardware 70
Cargando componentes 70
Detectar hardware de red 71
Configurando la red 71
Contraseña de root 72
Configurando el reloj 73
Detección de discos y otros dispositivos 74
El particionado 74

Copiando la imagen en vivo 80
Configurar el Administrador de paquetes (apt) 81
Instalación del cargador de arranque GRUB 83
Finalizando la instalación y reiniciando 85
4.2.2 Instalación en un sistema de archivos totalmente encriptado 85
Introducción a LVM 86
Introducción a LUKS 86
Configuración de particiones cifradas 86
Fin de la partición guiada con LVM cifrado 90
4.3 Instalaciones desatendidas 91 91
4.3.1 Presentación de respuestas 92
Con parámetros de arranque 92
Con un archivo presentado en el Initrd 92
Con un archivo presentado en los medios de arranque 93
Con un archivo presentado cargado desde la red 93
4.3.2 Crear un archivo presentado 93
4.4 Instalaciones ARM 94
4.5 Solución de problemas de instalaciones 95
4.6 Resumen 100

5. Configuración de Kali Linux 103

5.1 Configuración de la red 104
5.1.1 En el escritorio con *NetworkManager* 104
5.1.2 En la línea de comando con Ifupdown 105
5.1.3 En la línea de comando con *systemd-networkd* 106
5.2 Gestión de usuarios de Unix y grupos de Unix 107
5.2.1 Crear cuentas de usuario 107
5.2.2 Modificar una cuenta o contraseña existente 108
5.2.3 Deshabilitar una cuenta 109
5.2.4 Gestión de grupos de Unix 109

5.3 Configuración de servicios . . . 109
5.3.1 Configuración de un programa específico . . . 110
5.3.2 Configuración de SSH para inicios de sesión remotos . . . 110
5.3.3 Configuración de bases de datos PostgreSQL . . . 111
Tipo de conexión y autenticación de cliente . . . 111
Creación de usuarios y bases de datos . . . 112
Administrar clústeres de PostgreSQL . . . 113
5.3.4 Configuración de Apache . . . 113
Configuración de hosts virtuales . . . 114
Directivas comunes . . . 115
5.4 Gestión de servicios . . . 117
5.5 Resumen . . . 119

Página 8

6. Ayudarse a sí mismo y obtener ayuda 123
6.1 Fuentes de documentación . . . 124
6.1.1 Páginas del manual . . . 124
6.1.2 Documentos de información . . . 126
6.1.3 Documentación específica del paquete . . . 126
6.1.4 Sitios web . . . 127
6.1.5 Documentación de Kali en docs.kali.org . . . 127
6.2 Comunidades Kali Linux . . . 128
6.2.1 Foros web en foros.kali.org . . . 128
6.2.2 # Canal IRC kali-linux en Freenode . . . 128
6.3 Presentación de un buen informe de error . . . 129 129
6.3.1 Recomendaciones genéricas . . . 130
Cómo comunicarse . . . 130
Qué poner en el informe de errores . . . 130
Consejos misceláneos . . . 131
6.3.2 Dónde presentar un informe de error . . . 132
6.3.3 Cómo presentar un informe de error . . . 133
Presentación de un informe de error en Kali . . . 133
Presentación de un informe de error en Debian . . . 137
Presentación de un informe de error en otro proyecto de software libre . . . 144
6.4 Resumen . . . 146
7. Asegurar y Monitorear Kali Linux 149
7.1 Definición de una política de seguridad . . . 150
7.2 Posibles medidas de seguridad . . . 152
7.2.1 En un servidor . . . 152
7.2.2 En una computadora portátil . . . 152
7.3 Protección de servicios de red . . . 153
7.4 Firewall o filtrado de paquetes . . . 153
7.4.1 Comportamiento de Netfilter . . . 154
7.4.2 Sintaxis de iptables y ip6tables . . . 157
Comandos . . . 157
Reglas . . . 157
7.4.3 Crear reglas . . . 159
7.4.4 Instalación de las reglas en cada arranque . . . 160
7.5 Monitoreo y registro . . . 161
7.5.1 Registros de monitoreo con logcheck . . . 161
7.5.2 Actividad de monitoreo en tiempo real . . . 162
7.5.3 Detección de cambios . . . 162
Auditoría de paquetes con dpkg --verify . . . 162
Monitoreo de archivos: AIDE . . . 163
7.6 Resumen . . . 164

Página 9

8. Gestión de paquetes Debian 169
8.1 Introducción a APT . . . 170
8.1.1 Relación entre APT y dpkg . . . 170

8.1.2 Comprensión del archivo sources.list . . . 172
8.1.3 Repositorios Kali . . . 173
El repositorio Kali-Rolling . . . 173
El repositorio de Kali-Dev . . . 174
El repositorio de Kali-Bleeding-Edge . . . 174
Los espejos de Kali Linux . . . 174
8.2 Interacción básica del paquete . . . 175
8.2.1 Inicializando APT . . . 176
8.2.2 Instalación de paquetes . . . 176
Instalación de paquetes con dpkg . . . 176
Instalación de paquetes con APT . . . 177
8.2.3 Actualización de Kali Linux . . . 179
8.2.4 Eliminación y purga de paquetes . . . 180
8.2.5 Inspección de paquetes . . . 181
Consultar la base de datos de dpkg e inspeccionar archivos .deb . . . 181
Consulta de la base de datos de paquetes disponibles con apt-cache y apt . . . 185
8.2.6 Solución de problemas . . . 187
Manejo de problemas después de una actualización . . . 187
El archivo de registro dpkg . . . 188
Reinstalar paquetes con apt --reinstall y aptitude reinstall . . . 189
*Apalancamiento --force- * para reparar dependencias rotas* . . . 189
8.2.7 Frontales: aptitud y sináptica . . . 190
Aptitud . . . 190
Sináptica . . . 194
8.3 Configuración y uso avanzados de APT . . . 194
8.3.1 Configuración de APT . . . 195
8.3.2 Gestión de las prioridades del paquete . . . 196
8.3.3 Trabajar con varias distribuciones . . . 198
8.3.4 Seguimiento de paquetes instalados automáticamente . . . 199
8.3.5 Aprovechar la compatibilidad con múltiples arcos . . . 200
Habilitar Multi-Arch . . . 200
Cambios relacionados con varios arcos . . . 201
8.3.6 Validación de la autenticidad del paquete . . . 202
8.4 Referencia del paquete: Profundizando en el sistema del paquete Debian . . . 204 204
8.4.1 El archivo de control . . . 206
Dependencias: el campo depende . . . 207
Predepende, depende más exigente . . . 207
Recomienda, sugiere y mejora los campos . . . 208

Conflictos: el campo de conflictos . . . 208
Incompatibilidades: el campo Breaks . . . 209
Elementos proporcionados: el campo Proporciona . . . 209
Sustitución de archivos: el campo Sustituye . . . 210
8.4.2 Scripts de configuración . . . 211
Instalación y secuencia de secuencia de comandos de actualización . . . 213
Retiro del paquete . . . 214
8.4.3 Sumas de control, conffiles . . . 214
8.5 Resumen . . . 216
9. Uso avanzado 221
9.1 Modificación de paquetes de Kali . . . 222
9.1.1 Obteniendo las fuentes . . . 223
9.1.2 Instalación de dependencias de compilación . . . 226
9.1.3 Hacer cambios . . . 226
Aplicando un parche . . . 227
Ajustar las opciones de compilación . . . 229
Empaquetar una nueva versión ascendente . . . 229
9.1.4 Inicio de la compilación . . . 231
9.2 Recompilación del kernel de Linux . . . 233
9.2.1 Introducción y requisitos previos . . . 233
9.2.2 Obteniendo las fuentes . . . 234
9.2.3 Configuración del kernel . . . 235
9.2.4 Compilación y construcción del paquete . . . 236
9.3 Creación de imágenes ISO de Kali Live personalizadas . . . 237
9.3.1 Instalación de requisitos previos . . . 237

9.3.2 Creación de imágenes en vivo con diferentes entornos de escritorio . . . 238
9.3.3 Cambio del conjunto de paquetes instalados . . . 238
9.3.4 Uso de ganchos para ajustar el contenido de la imagen . . . 239
9.3.5 Agregar archivos en la imagen ISO o en el sistema de archivos en vivo . . . 240
9.4 Agregar persistencia al Live ISO con una llave USB . . . 240
9.4.1 La característica de persistencia: explicaciones . . . 240
9.4.2 Configuración de la persistencia sin cifrar en una llave USB . . . 242
9.4.3 Configuración de la persistencia cifrada en una llave USB . . . 243
9.4.4 Uso de múltiples almacenes de persistencia . . . 244
9.5 Resumen . . . 246
9.5.1 Sugerencias resumidas para modificar los paquetes de Kali . . . 246
9.5.2 Sugerencias resumidas para recompilar el kernel de Linux . . . 247
9.5.3 Resumen de consejos para crear imágenes ISO Kali Live ISO personalizadas . . . 248
10. Kali Linux en la empresa 251
10.1 Instalación de Kali Linux en la red (arranque PXE) . . . 252

10.2 Aprovechar la gestión de la configuración . . . 255
10.2.1 Configuración de SaltStack . . . 255
10.2.2 Ejecutando comandos en Minions . . . 256
10.2.3 Estados de sal y otras características . . . 258
10.3 Ampliación y personalización de Kali Linux . . . 262
10.3.1 Bifurcación de paquetes Kali . . . 262
10.3.2 Creación de paquetes de configuración . . . 263
10.3.3 Crear un repositorio de paquetes para APT . . . 269
10.4 Resumen . . . 273
11. Introducción a las evaluaciones de seguridad 279
11.1 Kali Linux en una evaluación . . . 281
11.2 Tipos de evaluaciones . . . 283
11.2.1 Evaluación de vulnerabilidad . . . 284
Probabilidad de ocurrencia . . . 287
Impacto . . . 287
Riesgo general . . . 287
En resumen . . . 288
11.2.2 Prueba de penetración de cumplimiento . . . 288
11.2.3 Prueba de penetración tradicional . . . 289
11.2.4 Evaluación de la aplicación . . . 291
11.3 Formalización de la evaluación . . . 293
11.4 Tipos de ataques . . . 294
11.4.1 Denegación de servicio . . . 295
11.4.2 Corrupción de memoria . . . 295
11.4.3 Vulnerabilidades web . . . 296
11.4.4 Ataques de contraseña . . . 296
11.4.5 Ataques del lado del cliente . . . 297
11.5 Resumen . . . 297
12. Conclusión: el camino por delante 301
12.1 Mantenerse al día con los cambios . . . 302
12.2 Mostrando su conocimiento recién adquirido . . . 302
12.3 Ir más allá . . . 302
12.3.1 Hacia la administración del sistema . . . 303
12.3.2 Hacia las pruebas de penetración . . . 303
Índice 304

Prefacio

No tienes idea de lo bueno que lo tienes.

En 1998, era un hacker prometedor, cofundador de uno de los primeros sombreros blancos profesionales.
piratería de equipos. Éramos niños, realmente, con trabajos de ensueño, pagados para entrar en algunos de los lugares más seguros
sistemas informáticos, redes y edificios en el planeta.

Suena bastante sexy, pero en realidad, pasamos la mayor parte del tiempo flotando sobre un teclado, armados
con las herramientas digitales de nuestro comercio. Manejamos una sórdida colección de programas, diseñados para mapear
redes y localizar objetivos; luego escanea, explota y gira a través de ellos. En algunos casos, uno de
nosotros (a menudo Jim Chapple) escribiríamos herramientas personalizadas para hacer cosas malas como escanear una red de Clase A
(algo que ninguna otra herramienta podría hacer en ese momento), pero la mayoría de las veces usamos o modificamos herramientas
escrito por la comunidad hacker. En esos días anteriores a Google, frecuentamos BugTraq, AstaLaVista,
PacketStorm, w00w00, SecurityFocus, X-Force y otros recursos para realizar una investigación y construir
nuestro arsenal

Como teníamos un tiempo limitado en cada concierto, tuvimos que movernos rápidamente. Eso significaba que no podíamos gastar un
mucho tiempo jugueteando con herramientas. Significaba que teníamos que aprender las herramientas básicas por dentro y por fuera, y mantener el
auxiliares de barril, por si acaso. Significaba que teníamos que tener nuestras herramientas bien organizadas, documentadas,
y probado para que haya pocas sorpresas en el campo. Después de todo, si no entramos, perderíamos la cara
con nuestros clientes y tomarían nuestras recomendaciones mucho menos en serio.

Debido a esto, pasé mucho tiempo catalogando herramientas. Cuando se lanzó o actualizó una herramienta, iría
a través de una rutina. Tenía que averiguar si funcionaría en la plataforma de ataque (algunos no), y
si valió la pena (algunos no); Tuve que actualizar cualquier script que dependiera de él, documento
y pruébelo, incluida la transferencia de cualquier cambio realizado a la versión anterior.

Luego, sacudiría todas las herramientas y las pondría en directorios según su propósito durante un
evaluación. Escribiría scripts de envoltura para ciertas herramientas, encadenaría algunas herramientas y correlacionaría
todo eso en un CD separado que podríamos llevar a áreas sensibles, cuando los clientes no nos dejaran
tomar máquinas de ataque o eliminar medios de sus laboratorios.

Este proceso fue doloroso, pero fue necesario. Sabíamos que teníamos la capacidad de entrar en cualquier
red: si aplicamos nuestras habilidades y experiencia, nos mantenemos organizados y trabajamos de manera eficiente.
Aunque permanecer invicto fue un motivador, se trataba de proporcionar un servicio a clientes que
nos *necesitaba* para irrumpir en las redes, para que pudieran tapar las brechas y mover el dinero hacia la situación crítica, pero ...
programas de seguridad de la información descuidados.

Pasamos años afinando nuestras habilidades y experiencia, pero no habríamos tenido éxito sin
organización y eficiencia. Habríamos fallado si no pudiéramos poner la mano en la herramienta adecuada
cuando sea necesario.

Es por eso que pasé tanto tiempo investigando, documentando, probando y catalogando herramientas, y en
A comienzos del siglo XXI, se estaba convirtiendo rápidamente en un trabajo abrumador de tiempo completo. Gracias a
Internet, la superficie de ataque mundial explotó y la variedad y cantidad de herramientas de ataque
aumentó exponencialmente, al igual que la carga de trabajo requerida para mantenerlos.

A partir de 2004, Internet explotó no solo como base para los negocios, sino también como una red social.
plataforma. Las computadoras eran asequibles, más amigables para el consumidor y ubicuas. Tecnología de almacenamiento
ogy se expandió de megabytes a gigabytes. Ethernet saltó de cientos de kilobits a decenas
de megabits por segundo, y las conexiones a Internet eran más rápidas y baratas que nunca. MI-
el comercio estaba en aumento, los sitios de redes sociales como Facebook (2004) y Twitter (2006) entraron en línea
y Google (1998) habían madurado hasta el punto de que cualquier persona (incluidos los criminales) podría encontrar algo acerca de
Cualquier cosa en línea.

La investigación se volvió crítica para equipos como el nuestro porque teníamos que mantenernos al día con nuevos ataques y
conjuntos de herramientas Respondimos a más delitos informáticos, y el trabajo forense exigió que pisáramos
a la ligera mientras revisamos la evidencia potencial. El concepto de un *CD en vivo* significaba que podíamos
realizar análisis forenses en vivo en una máquina comprometida sin comprometer la evidencia.

Ahora nuestro pequeño equipo tenía que administrar herramientas de ataque, herramientas forenses y una distribución de herramientas de área sensible.
ción tuvimos que mantenernos al día con las últimas metodologías de ataque y explotación; y tuvimos que
saben, en realidad hacemos lo que nos pagaron: pruebas de penetración, que tenían una gran demanda. Cosas

estábamos perdiendo el control, y antes de mucho tiempo, estábamos gastando los pesos en batalla y mucho más tiempo investigando, afinando nuestras herramientas y planeando.

No estábamos solos en esta lucha. En 2004, Mati "Muts" Aharoni, un hacker y profesor de seguridad sional lanzó "WHoppiX" (White Hat Knoppix), un CD de Linux en vivo que calificó como "el mejor prueba de lápiz CD en vivo ", incluyó" todos los exploits de SecurityFocus, Packet Storm y k-otik, Metasploit Framework 2.2, y mucho, mucho más ".

Recuerdo que descargarWHoppiXy pensar que era una gran cosa para tener alrededor. Yo descargué otros CD en vivo, pensando que si alguna vez estuviese en apuros reales, los CD en vivo podrían salvar mi tocino en el campo. Pero no estaba dispuesto a confiar en WHoppiX ni en ningún otro CD para un trabajo real. No confiaba en ninguno de ellos para satisfacer la mayoría de mis necesidades; ninguno de ellos se sentía bien para mi flujo de trabajo; no estaban llenos distribuciones instalables; y en el momento en que los descargué no estaban actualizados. Un anciano El juego de herramientas es el beso de la muerte en nuestra industria.

Simplemente agregué estas imágenes de CD, a pesar de su tamaño relativamente masivo, a nuestro arsenal y seguí El doloroso proceso de mantener nuestro juego de herramientas "real".

Pero a pesar de mis opiniones personales en ese momento, y tal vez a pesar de las expectativas de Muts, WHoppiX y sus descendientes tuvieron un impacto sísmico en su vida, nuestra industria y nuestra comunidad.

Página 15

En 2005, WHoppiX evolucionó a WHAX, con un conjunto de herramientas ampliado y actualizado, basado en "cuanto más CD en vivo modular SLAX (Slackware) ". Muts y un equipo cada vez mayor de voluntarios del comité de piratas informáticos la comunidad parecía darse cuenta de que no importaba cuán perspicaces fueran, nunca podrían anticipar todo El crecimiento y la fluctuación de nuestra industria y que los usuarios de su CD tendrían diversas necesidades en el campo. Era obvio que Muts y su equipo estaban usando WHAX en el campo, y ellos Parecía dedicado a hacerlo funcionar. Esto fue alentador para mí.

En 2006, Muts, Max Moser y sus equipos consolidaron Auditor Security Linux y WHAX en una única distribución llamada BackTrack. Todavía basado en SLAX, BackTrack continuó creciendo, agregando más herramientas, más marcos, soporte de idiomas extendido, soporte inalámbrico extenso, un menú estructura que atiende a usuarios principiantes y profesionales, y un núcleo muy modificado. BackTrack se convirtió la distribución de seguridad líder, pero muchos como yo todavía la usaban como respaldo para sus "herramientas reales".

A principios de 2009, Muts y su equipo habían extendido BackTrack significativamente a BackTrack 4. Ahora un completo tiempo de trabajo para Muts, BackTrack ya no era un CD en vivo sino una distribución completa basada en Ubuntu aprovechando los repositorios de software de Ubuntu. El cambio marcó una seria evolución: BackTrack 4 Tenía un mecanismo de actualización. En las propias palabras de Muts: "Al sincronizar con nuestros repositorios BackTrack, regularmente recibirá actualizaciones de herramientas de seguridad poco después de su lanzamiento ".

Este fue un punto de inflexión. El equipo de BackTrack se había sintonizado con las dificultades que enfrentan los probadores de pen, analistas forenses y otros que trabajan en nuestra industria. Sus esfuerzos nos salvarían incontables horas. y proporcionar una base firme, lo que nos permite volver a la lucha y pasar más tiempo haciendo Las cosas importantes (y divertidas). Como resultado, la comunidad respondió acudiendo en masa a los foros. y wiki; y participando en el equipo de desarrollo. BackTrack fue realmente un esfuerzo comunitario, con Muts sigue liderando la carga.

BackTrack4 finalmente se había convertido en una placa de resistencia industrial y yo, y otros como yo, respiraban un suspiro de alivio. Sabíamos de primera mano el "dolor y sufrimiento" que Muts y su equipo estaban soportando, porque habíamos estado allí. Como resultado, muchos de nosotros comenzaron a usar BackTrackasaprimaryfundation por nuestro trabajo Sí, todavía jugamos con herramientas, escribimos nuestro propio código y desarrollamos nuestros propios exploits y técnicas; andweresearchedandexperimented; butwedidnotspendallourtimecollecting, herramientas de actualización, validación y organización.

BackTrack 4 R1 y R2 fueron revisiones adicionales en 2010, lo que condujo a la reconstrucción de Back-Track 5 en 2011. Todavía basado en Ubuntu, y ganando fuerza con cada lanzamiento, BackTrack fue ahora un proyecto masivo que requería un voluntario heroico y un esfuerzo comunitario, pero también fondos. Muts lanzó Offensive Security (en 2006) no solo para proporcionar capacitación y penetración de clase mundial. servicios de prueba de la región, pero también para proporcionar un vehículo para mantener el desarrollo de BackTrack en marcha, y asegúrese de que BackTrack permanezca de código abierto y de uso gratuito.

BackTrack continuó creciendo y mejorando hasta 2012 (con R1, R2 y R3), manteniendo un Ubuntu core y agregar cientos de nuevas herramientas, incluida la explotación física y de hardware herramientas, soporte VMware, innumerables controladores inalámbricos y de hardware, y una multitud de estabilidad de im-comprobaciones y correcciones de errores. Sin embargo, después del lanzamiento de R3, el desarrollo de BackTrack se relaciona cautivadora y algo misteriosamente tranquila.

Hubo algunas especulaciones en la industria. Algunos pensaron que BackTrack estaba siendo "comprado fuera ", vendiendo su alma a un señor corporativo malvado sin rostro por un pago masivo. Seguridad ofensiva Rity se estaba convirtiendo en una de las empresas de formación más respetadas y un líder de pensamiento en nuestro industria, y algunos especularon que su éxito había engullido y marginado la clave BackTrack desarrolladores Sin embargo, nada podría estar más lejos de la verdad.

En 2013, se lanzó Kali Linux 1.0. De las notas de la versión: "Después de un año de desarrollo silencioso, Offensive Security se enorgullece en anunciar el lanzamiento y la disponibilidad pública de Kali Linux, la mayoría Distribución avanzada, robusta y estable de pruebas de penetración hasta la fecha. Kali es un más maduro, segura y una versión empresarial lista para BackTrack ".

Kali Linux no fue un mero cambio de marca de BackTrack. Sporting más de 600 completamente reempaquetado herramientas antiguas, era claramente un conjunto de herramientas increíble, pero aún había más que eso. Kali había estado construido, desde cero, en un núcleo Debian. Para los desinformados, esto podría no parecer un gran acuerdo. Pero los efectos de la ondulación fueron asombrosos. Gracias a un esfuerzo masivo de reempaquetado, los usuarios de Kali podría descargar la fuente de cada herramienta; podrían modificar y reconstruir una herramienta según sea necesario, con solo unas pocas teclas. A diferencia de otros sistemas operativos convencionales de la actualidad, Kali Linux sincronizado con los repositorios de Debian cuatro veces al día, lo que significaba que los usuarios de Kali podían obtener Actualizaciones de paquetes perversamente actuales y correcciones de seguridad. Los desarrolladores de Kali se lanzaron al Deshilachar, empaquetar y mantener versiones anteriores de muchas herramientas para que los usuarios estén constantemente mantenido en el borde sangrante. Gracias a sus raíces de Debian, los usuarios de Kali pudieron arrancar una instalación o ISO directamente desde los repositorios, lo que abrió la puerta para Kali completamente personalizado instalaciones o implementaciones empresariales masivas, que podrían automatizarse y personalizarse aún más con archivos preestablecidos. Para completar la trifecta de personalización, los usuarios de Kali pueden modificar el escritorio entorno, alterar menús, cambiar iconos e incluso reemplazar entornos de ventanas. Un masivo El impulso de desarrollo de ARM abrió la puerta para la instalación de Kali Linux en una amplia gama de hardware plataformas que incluyen puntos de acceso, computadoras de placa única (Raspberry Pi, ODROID, BeagleBone, y CubieBoard, por ejemplo), y computadoras Chromebook basadas en ARM. Y por último pero ciertamente No menos importante, Kali Linux lucía actualizaciones menores y mayores sin problemas, lo que significaba que los devotos tendrían nunca tendrá que reinstalar configuraciones personalizadas de Kali Linux.

La comunidad se dio cuenta. En los primeros cinco días, 90,000 de nosotros descargamos Kali 1.0.

Esto fue solo el comienzo. En 2015, se lanzó Kali 2.0, seguido de los lanzamientos sucesivos de 2016. En resumen, "Si Kali 1.0 se centró en la construcción de una infraestructura sólida, entonces Kali 2.0 se centra en revisando la experiencia del usuario y manteniendo paquetes actualizados y repositorios de herramientas ".

La versión actual de Kali Linux es una distribución continua, que marca el final de la versión discreta. Sions. Ahora, los usuarios están actualizados continuamente y reciben actualizaciones y parches a medida que se crean. Las herramientas principales se actualizan con mayor frecuencia gracias a un sistema de etiquetado de versión ascendente, Se han implementado mejoras de accesibilidad para personas con discapacidad visual, y el Los kernel de Linux se actualizan y se envían para continuar con el soporte de inyección inalámbrica 802.11. SoftwareDefinedRadio (SDR) y herramientas de comunicación de campo cercano (NFC) admiten soporte para nuevos campos de seguridad pruebas. La instalación completa del disco encriptado de Linux y las opciones de autodestrucción de emergencia están disponibles,

Gracias a LVM y LUKS respectivamente, se han agregado opciones de persistencia USB, permitiendo USB-Kali se instala para mantener los cambios entre reinicios, ya sea que la unidad USB esté encriptada o no. Finalmente, las últimas proyecciones de Kalio abrieron la puerta de NetHunter, anopen-sourceworld-class sistema operativo que se ejecuta en dispositivos móviles basados en Kali Linux y Android.

Kali Linux ha evolucionado no solo en la plataforma de elección del profesional de seguridad de la información, pero verdaderamente en un funcionamiento industrial, de clase mundial, maduro, seguro y listo para la empresa distribución del sistema

A través del proceso de desarrollo de una década, Muts y su equipo, junto con el incansable dedicación de innumerables voluntarios de la comunidad hacker, han asumido la carga de la corriente alineando y organizando nuestro ambiente de trabajo, liberándonos de gran parte del trabajo pesado de nuestro trabajo y proporcionar una base segura y confiable, lo que permite concentrarse para conducir la industria adelante con el objetivo final de asegurar nuestro mundo digital.

Y curiosamente, pero no es sorprendente, se ha creado una increíble comunidad en torno a Kali Linux. Cada mes, entre trescientos y cuatrocientos mil de nosotros descargamos una versión de Kali. Venimos juntos en los Kaliforums, unos cuarenta y cinco millones, y una calle de cuatrocientos horas se puede encontrar en el canal Kali IRC. Nos reunimos en conferencias y asistimos a Kali Dojos para aprender cómo para aprovechar mejor a Kali de los propios desarrolladores.

Kali Linux ha cambiado el mundo de la seguridad de la información para mejor, y Muts y su equipo nos ha ahorrado incontables horas de trabajo y frustración, permitiéndonos pasar más tiempo y energía impulsando la industria hacia adelante, juntos.

Pero a pesar de su sorprendente aceptación, apoyo y popularidad, Kali nunca ha lanzado un oficial manual. Bueno, ahora eso ha cambiado. Estoy encantado de haber venido junto con el desarrollo de Kali equipo y específicamente Mati Aharoni, Raphaël Hertzog, Devon Kearns y Jim O'Gorman para ofrecer esta, la primera en quizás una serie de publicaciones oficiales centradas en Kali Linux. En este libro, nosotros se centrará en la plataforma Kali Linux y lo ayudará a comprender y maximizar el uso de Kali desde cero. Todavía no profundizaremos en el arsenal de herramientas contenidas en Kali Linux, pero ya sea un veterano o un n00b absoluto, este es el mejor lugar para comenzar, si está listo para excavar y ponte serio con Kali Linux. Independientemente de cuánto tiempo hayas estado en el juego, tu decisión leer este libro te conecta con la creciente comunidad de Kali Linux, una de las más antiguas, más grandes, más activo y más vibrante en nuestra industria.

En nombre de Muts y el resto del increíble equipo de Kali, felicidades por dar el primer paso. para dominar Kali Linux!

Johnny Long

Febrero de 2017

Prefacio

Las dieciséis computadoras portátiles de gama alta que ordenó para su equipo entusiasta acaban de llegar, y usted ha estado encargado de configurarlos, para el compromiso externo de mañana. Instalas Kali y arrancas uno de los computadoras portátiles solo para descubrir que apenas es utilizable. A pesar del núcleo de última generación de Kali, las tarjetas de red y el mouse no funcionan, y la gran tarjeta gráfica y GPU de NVIDIA lo miran fijamente, porque carecen de controladores instalados correctamente. Tu suspiro

En el *modo* Kali *Live* , escribe rápidamente `lspci` en una consola y luego entrecierra los ojos. Te desplazas por el listado de hardware: “Puente PCI, controlador USB, controlador SATA. ¡Ajá! Ethernet y red de controllers ". Una búsqueda rápida en Google de sus respectivos números de modelo, con referencias cruzadas con el La versión del kernel Kali revela que estos controladores de vanguardia no han llegado al kernel principal todavía.

Pero no todo está perdido. Lentamente se está formulando un plan en su cabeza, y le agradece a los cielos por el Libro *revelado de Kali Linux* que recogiste hace un par de semanas. Podrías usar el Kali Live- Cree un sistema para crear un Kali ISO personalizado, que tendría los controladores necesarios integrados en el medios de instalación Además, puede incluir los controladores de gráficos NVIDIA y el CUDA las bibliotecas necesarias para obtener esa bestia de un GPU completamente étnica para mostrar un gato, y tenerla mientras se agrietan hashes de contraseñas a velocidades vertiginosas. Diablos, incluso podrías lanzar un fondo de pantalla personalizado con un Logotipo de Microsoft en él, para burlarse de su equipo en el trabajo.

Dado que los perfiles de hardware para sus instalaciones son idénticos, ha introducido la opción de arranque en el ISO, por lo tanto, su equipo puede arrancar de un palo de EE. UU. y tener Kali instalado con interacción interna la instalación se cuida sola, encriptación completa del disco y todo.

¡Perfecto! Ahora puede generar una versión actualizada de Kali a pedido, específicamente diseñada y optimizado para su hardware. Salvaste el día. ¡Misión cumplida!

Con el diluvio de hardware que llega al mercado, este escenario se está volviendo más común para aquellos de nosotros que nos aventuramos lejos de los sistemas operativos convencionales, en busca de algo más ágil, más malo o más adecuado para nuestro trabajo y estilo.

Esto es especialmente aplicable a aquellos que se sienten atraídos por el campo de la seguridad, ya sea que se trate de un pasatiempo atractivo, fascinación o línea de trabajo. Como recién llegados, a menudo se encuentran perplejos por el medio ambiente. ment o el sistema operativo. Para muchos recién llegados, Kali es su primera introducción a Linux.

Reconocimos este cambio en nuestra base de usuarios hace un par de años y pensamos que podríamos ayudar nuestra comunidad al crear un libro introductorio estructurado que guíe a los usuarios al mundo

de seguridad, al tiempo que les brinda toda la sofisticación de Linux que necesitarían para comenzar. Y entonces, nació el libro Kali, ahora disponible de forma gratuita a través de Internet para beneficio de cualquier persona interesada en entrar en el campo de la seguridad a través de Kali Linux.

Sin embargo, cuando el libro comenzó a tomar forma, nos dimos cuenta rápidamente de que había un potencial sin explotar. Esta sería una gran oportunidad para ir más allá de un libro introductorio de Kali Linux y explorar Algunas de las características más interesantes y poco conocidas. De ahí el nombre del libro: *Kali Linux Revelada* .

Al final, nos quedamos impresionados con el resultado. El libro respondió a todos nuestros requisitos y estoy Orgulloso de decir que superó nuestras expectativas. Nos dimos cuenta de que habíamos inadvertidamente amplió la base de usuarios potenciales del libro. Ya no estaba destinado solo a los recién llegados al campo de seguridad, pero también incluía gran información para expertos en penetración experimentados para mejorar y pulir su control de Kali Linux, lo que les permite desbloquear todo el potencial de Nuestra distribución. Ya sea que estuvieran colocando una sola máquina o miles en una empresa, haciendo cambios menores de configuración o personalizando completamente el nivel del edificio, construyendo sus propios repositorios, tocando la superficie o profundizando en el sorprendente paquete Debian sistema de gestión, *Kali Linux Revealed* proporciona la hoja de ruta.

Con su mapa en mano, en nombre mío y de todo el equipo de Kali Linux, les deseo un emocionante, viaje divertido, fructífero y "revelador"!

Muts, febrero de 2017

Introducción

KaliLinux es la plataforma de pruebas de penetración más potente y popular del mundo, utilizada por la seguridad profesionales en una amplia gama de especializaciones, que incluyen pruebas de penetración, análisis forense, reversa ingeniería y evaluación de vulnerabilidad. Es la culminación de años de refinamiento y la resultado de una evolución continua de la plataforma, de WHoppiX a WHAX, a BackTrack, y ahora a un completo marco de pruebas de penetración que aprovecha muchas características de Debian GNU / Linux y La vibrante comunidad de código abierto en todo el mundo.

Kali Linux no ha sido creado para ser una simple colección de herramientas, sino más bien un marco flexible que los probadores de penetración profesionales, entusiastas de la seguridad, estudiantes y aficionados pueden personalizar para adaptarse a sus necesidades específicas.

¿Por qué este libro?

Kali Linux no es simplemente una colección de varias herramientas de seguridad de la información que se instalan en un base Debian estándar y preconfigurada para que pueda comenzar a usarlo de inmediato. Sacar el máximo provecho fuera de Kali, es importante tener una comprensión profunda de su poderoso Debian GNU / Linux fundamentos (que admiten todas esas excelentes herramientas) y aprender cómo puede usarlos en su entorno

Aunque Kali es decididamente multipropósito, está diseñado principalmente para ayudar en las pruebas de penetración. El objetivo de este libro no es solo ayudarlo a sentirse como en casa cuando usa Kali Linux, sino también ayudar a mejorar su comprensión y agilizar su experiencia para que cuando esté comprometido en una prueba de penetración y el tiempo es esencial, no tendrá que preocuparse por perder preciosos minutos para instalar un nuevo software o habilitar un nuevo servicio de red. En este libro, presentaremos primero a Linux, luego profundizaremos a medida que le presentemos los matices específicos de Kali Linux para que sepa exactamente lo que sucede debajo del capó.

Este es un conocimiento invaluable, especialmente cuando está tratando de trabajar con poco tiempo. restricciones No es raro requerir esta profundidad de conocimiento cuando se está configurando, solucionar un problema, esforzarse por doblar una herramienta a su voluntad, analizar la salida de una herramienta, o aprovechando Kali en un entorno a mayor escala.

¿Este libro es para ti?

Si está ansioso por sumergirse en el campo de información intelectualmente rico e increíblemente fascinante seguridad, y con razón seleccioné a Kali Linux como plataforma principal, entonces este libro ayudará usted en ese viaje Este libro está escrito para ayudar a los usuarios nuevos de Linux, así como a los actuales Kali usuarios que buscan profundizar su conocimiento sobre los fundamentos de Kali, así como aquellos que han usado Kali durante años, pero que buscan formalizar su aprendizaje, ampliar su uso de Kali, y llenar los vacíos en su conocimiento.

Además, este libro puede servir como hoja de ruta, referencia técnica y guía de estudio para aquellos demandando la certificación Kali Linux Certified Professional.

Enfoque general y estructura del libro

Este libro ha sido diseñado para que pueda tener en sus manos Kali Linux desde el principio. No tiene que leer la mitad del libro para comenzar. Cada tema está cubierto de una manera muy pragmática. manera, y el libro está lleno de muestras y capturas de pantalla para ayudar a hacer las explicaciones más hormigón.

En el capitulo 1 , " Acerca de Kali Linux " [página 2], definimos una terminología básica y explicamos el propósito pose de Kali Linux. En el capítulo 2 , “ Introducción a Kali Linux"[Página 14], te guiamos paso a paso pase de la descarga de la imagen ISO a ejecutar Kali Linux en su computadora. próximo viene el capítulo 3 , "Fundamentos de Linux "[página 48] que proporciona los conocimientos básicos que usted necesita saber sobre cualquier sistema Linux, como su arquitectura, proceso de instalación, sistema de archivos jerarquía, permisos y más.

En este punto, has estado usando Kali Linux como sistema en vivo por un tiempo. Con el capítulo 4 , "Instalando KaliLinux”[Página66] aprenderá a hacer una instalación permanente Kalali Linux (en su disco duro disco) y con el capítulo 5 5, " Configuración de Kali Linux"[Página 104] cómo ajustarlo a su gusto. Como un usuario habitual de Kali, es hora de familiarizarse con los recursos importantes disponibles para los usuarios de Kali: Capítulo 6 , “ Ayudarse a sí mismo y obtener ayuda "[Página 124] le brinda las claves para lidiar con Problemas inesperados que probablemente enfrentará.

Con lo básico bien cubierto, el resto del libro se sumerge en temas más avanzados: capítulo 7 , “ Asegurar y monitorear Kali Linux ” [página 150] le brinda consejos para garantizar que su Kali Linux La instalación cumple con sus requisitos de seguridad. Siguiente, capítulo 8, " Gestión de paquetes Debian "

[página 170] explica cómo aprovechar todo el potencial del ecosistema de empaquetado de Debian. Y en el capítulo 9 , "Uso avanzado"[Página 222], aprende a crear un Kali Linux totalmente personalizado Imagen ISO Todos esos temas son aún más relevantes cuando implementa Kali Linux a escala en un empresa como se documenta en el capítulo 10 , " Kali Linux en la empresa " [página 252].

El ultimo capitulo, capitulo 11, " Introducción a las evaluaciones de seguridad"[Página 280], hace el enlace entre todo lo que has aprendido en este libro y el trabajo diario de los pro-
Profesionales.

Agradecimientos de Raphaël Hertzog

Me gustaría agradecer a Mati Aharoni: en 2012, se puso en contacto conmigo porque yo era uno de docenas de consultores debianos y quería construir un éxito en la parte posterior de la pista que se basaría en Debian Así es como comencé a trabajar en Kali Linux, y desde entonces he disfrutado mi viaje. en el mundo de Kali

Con los años, Kali Linux se acercó a Debian GNU / Linux, especialmente con el cambio a Kali Rolling, basado en las pruebas de Debian. Ahora, la mayor parte de mi trabajo, ya sea en Kali o en Debian, proporciona beneficios a todo el ecosistema de Debian. Y esto es exactamente lo que me mantiene tan motivado para continuar, un día después día, mes tras mes, año tras año.

Trabajar en este libro también es una gran oportunidad que me ofreció Mati. No es del mismo tipo de trabajo pero es igualmente gratificante poder ayudar a las personas y compartir con ellos mi experiencia del sistema operativo Debian / Kali. Aprovechando mi experiencia con el *administrador de Debian Manual* , espero que mis explicaciones te ayuden a iniciarte en el rápido mundo de la seguridad informática.

También me gustaría agradecer a todas las personas de Seguridad Ofensiva que participaron en el libro: Jim O'Gorman (coautor de algunos capítulos), Devon Kearns (revisor), Ron Henry (editor técnico), Joe Steinbach y Tony Cruse (gerentes de proyecto). Y gracias a Johnny Long que se unió a escribí el prefacio pero terminé revisando todo el libro.

Agradecimientos de Jim O'Gorman

Me gustaría agradecer a todos los involucrados en este proyecto por sus contribuciones, de las cuales las mías fueron Solo una pequeña parte. Este libro, al igual que Kali Linux, fue un proyecto colaborativo de muchas manos. haciendo que la luz funcione. Un agradecimiento especial a Raphaël, Devon, Mati, Johnny y Ron por asumir el gran parte del esfuerzo. Sin ellos, este libro no se habría unido.

Agradecimientos de Mati Aharoni

Han pasado algunos años desde que Kali Linux se lanzó por primera vez, y desde el primer día, siempre he soñado de publicar un libro oficial que cubre el sistema operativo Kali en su conjunto. Por lo tanto es Es un gran privilegio para mí ver finalmente un libro de este tipo que se hace público. me gustaría Agradezco sinceramente a todos los involucrados en la creación de este proyecto, incluidos Jim, Devon, Johnny,

y Ron Un agradecimiento muy especial a Raphaël por hacer la mayor parte del trabajo pesado en este libro, y aportando su amplia experiencia a nuestro grupo.

Palabras clave

Distribución de Linux
Derivado de Debian
Propósito
Caracteristicas
Políticas

Capítulo

Sobre Kali Linux 1

Contenido

Un poco de historia 2 Relación con Debian 4 Propósito y casos de uso 5 Características principales de Kali Linux 7
Políticas de Kali Linux 9 Resumen 11

Kali Linux[1] es una distribución de Linux de auditoría de seguridad lista para la empresa basada en Debian GNU / Linux. Kali está dirigido a profesionales de seguridad y administradores de TI, lo que les permite consultar prueba de penetración avanzada de ductos, análisis forense y auditoría de seguridad.

¿Qué es un Linux? ¿Distribución? Aunque se usa comúnmente como un nombre para todo el sistema operativo, Linux es solo el nombre del kernel, un software que maneja las interacciones entre hardware y aplicaciones de usuario final.

La expresión *distribución de Linux* , por otro lado, se refiere a un funcionamiento completo sistema construido sobre el núcleo de Linux, que generalmente incluye un programa de instalación y muchas aplicaciones, que están preinstaladas o empaquetadas en un sistema fácilmente instalable camino.

Debian GNU / Linux[2] es una distribución genérica de Linux líder, conocida por su calidad y estabilidad. Kali Linux se basa en el trabajo del proyecto Debian y agrega más de 300 especiales. paquetes de propósito propios, todos relacionados con la seguridad de la información, particularmente el campo de pruebas de penetración.

Debian es un proyecto de software gratuito que proporciona múltiples versiones de su sistema operativo y a menudo usamos el término *distribución* para referirnos a una versión específica del mismo, para examinar ple las distribuciones Debian Stable o Debian Testing. Lo mismo también se aplica a Kali Linux: con la distribución Kali Rolling, por ejemplo.

1.1. Un poco de historia

El proyecto Kali Linux comenzó silenciosamente en 2012, cuando Offensive Security decidió que querían Reemplace su proyecto venerable Back Track Track Linux, que se mantuvo manualmente, con algo que podría convertirse en un verdadero derivado de Debian[3] , completo con toda la infraestructura requerida y técnicas de embalaje mejoradas. Se tomó la decisión de construir Kali sobre el disco de Debian contribución porque es bien conocido por su calidad, estabilidad y amplia selección de software disponible. Es por eso que yo (Raphaël) me involucré en este proyecto, como consultor de Debian.

La primera versión (versión 1.0) ocurrió un año después, en marzo de 2013, y se basó en Debian 7 "Wheezy", la distribución estable de Debian en ese momento. En ese primer año de desarrollo, empacamos envejeció cientos de aplicaciones relacionadas con pruebas de pen y construyó la infraestructura. A pesar de el número de aplicaciones es significativo, la lista de aplicaciones ha sido meticulosamente seleccionada, drop- Haga ping a las aplicaciones que ya no funcionan o que las características duplicadas ya están disponibles en mejor programas

Durante los dos años posteriores a la versión 1.0, Kali lanzó muchas actualizaciones incrementales, expandiéndose la gama de aplicaciones disponibles y la mejora del soporte de hardware, gracias a la nueva versión del kernel arrendamientos Con cierta inversión en integración continua, nos aseguramos de que todos los paquetes importantes

[1] https://www.kali.org
[2] https://www.debian.org
[3] https://wiki.debian.org/Derivatives/Census

se mantuvieron en un estado instalable y esas imágenes en vivo personalizadas (un sello distintivo de la distribución) siempre se pudo crear.

En 2015, cuando salió Debian 8 "Jessie", trabajamos para cambiar la base de Kali Linux. Mientras Kali Linux 1.x evitó el GNOME Shell (confiando en GNOME Fallback), en esta versión nosotros decidió adoptarlo y mejorarlo: agregamos algunas extensiones de GNOME Shell para adquirir las que faltan características, especialmente el menú de aplicaciones. El resultado de ese trabajo se convirtió en Kali Linux 2.0, publicado en agosto de 2015.

GNOME es Kali Linux's Escritorio predeterminado Medio ambiente

Un entorno de escritorio es una colección de aplicaciones gráficas que comparten un común de herramientas gráficas y que están destinados a usarse juntos en estaciones de trabajo de usuarios. Escritorio- Los mejores entornos generalmente no se utilizan en servidores. Por lo general, proporcionan una aplicación selector de archivos, un administrador de archivos, un navegador web, un cliente de correo electrónico, una suite ofimática, etc.

GNOME[4] es uno de los entornos de escritorio más populares (junto con KDE[5] , Xfce[6] , LXDE[7] , MATE[8]) y se instala en las principales imágenes ISO proporcionadas por Kali Linux. Si no le gusta GNOME, es fácil crear una imagen ISO personalizada con el escritorio ambiente de su elección. Las instrucciones para hacerlo están cubiertas más adelante en este libro en capítulo 9 , "Uso avanzado "[página 222].

Paralelamente, aumentamos nuestros esfuerzos para garantizar que Kali Linux siempre tenga la última versión de todos aplicaciones de prueba de pluma. Desafortunadamente, ese objetivo estaba un poco en desacuerdo con el uso de Debian Stable como base para la distribución, porque nos obligó a respaldar muchos paquetes. Esto es debido a El hecho de que Debian Stable prioriza la estabilidad del software, lo que a menudo causa un largo retraso desde el lanzamiento de una actualización ascendente hasta cuando se integra en la distribución. Dado nuestra inversión en la integración continua, fue un movimiento bastante natural volver a crear Kali Linux en la parte superior de Debian Testing para poder beneficiarnos de la última versión de todos los paquetes de Debian tan pronto como estaban disponibles Debian Testing tiene un ciclo de actualización mucho más agresivo, que es más compatible con la filosofía de Kali Linux.

Este es, en esencia, el concepto de Kali Rolling. Mientras la distribución continua ha estado disponible durante bastante tiempo, Kali 2016.1 fue el primer lanzamiento en adoptar oficialmente la naturaleza rodante de ese distribución: cuando instala la última versión de Kali, su sistema realmente rastrea el Kali Rolling

distribución y *cada día obtienes nuevas actualizaciones* . En el pasado, los lanzamientos de Kali eran instantáneas de la distribución subyacente de Debian con paquetes específicos de Kali inyectados en ella.

Una distribución continua tiene muchos beneficios, pero también conlleva múltiples desafíos, tanto para aquellos de nosotros que estamos construyendo la distribución y para los usuarios que tienen que hacer frente a un interminable flujo de actualizaciones y, a veces, cambios incompatibles con versiones anteriores. Este libro tiene como objetivo darte la conocimiento requerido para lidiar con todo lo que pueda encontrar al administrar su Kali Linux instalación.

4 4 https://www.gnome.org
5 5 https://www.kde.org
6 6 http://www.xfce.org
7 7 http://lxde.org
8 http://mate-desktop.org

1.2. Relación con Debian

La distribución de Kali Linux se basa en Debian Testing 9 . Por lo tanto, la mayoría de los paquetes disponibles en Kali Linux vienen directamente de este repositorio de Debian.

Si bien Kali Linux depende en gran medida de Debian, también es completamente independiente en el sentido de que tenemos nuestra propia infraestructura y conservamos la libertad de realizar los cambios que queramos.

1.2.1 El flujo de paquetes

Del lado de Debian, los contribuyentes están trabajando todos los días para actualizar paquetes y cargarlos. a la distribución inestable de Debian. Desde allí, los paquetes migran a las pruebas de Debian distribución una vez que se han eliminado los errores más problemáticos. El proceso de migración también asegura que no se rompan dependencias en las pruebas de Debian. El objetivo es que las pruebas siempre estén en un estado utilizable (¡o incluso liberable!).

Los objetivos de Debian Testing se alinean bastante bien con los de Kali Linux, por lo que lo elegimos como base. Para agregar En los paquetes específicos de Kali en la distribución, seguimos un proceso de dos pasos.

Primero, tomamos Debian Testing e inyectamos a la fuerza nuestros propios paquetes Kali (ubicados en nuestro *kali-dev-only* repositorio) para construir el repositorio *kali-dev* . Este repositorio se romperá de vez en cuando: por postura, nuestros paquetes específicos de Kali podrían no ser instalables hasta que se hayan vuelto a compilar bibliotecas más nuevas. En otras situaciones, los paquetes que hemos bifurcado también deben actualizarse, ya sea para volver a instalarse o para arreglar la instalabilidad de otro paquete que depende de Una versión más nueva del paquete bifurcado. En cualquier caso, *kali-dev* no es para usuarios finales.

kali-rolling es la distribución que los usuarios de Kali Linux deben rastrear y está construida a partir de *kali-dev* de la misma manera que Debian Testing está construido a partir de Debian Unstable. Los paquetes migran solo cuando Todas las dependencias pueden satisfacerse en la distribución de destino.

1.2.2. Gestionar la diferencia con Debian

Como decisión de diseño, tratamos de minimizar la cantidad de paquetes bifurcados tanto como sea posible. Cómo- Sin embargo, para implementar algunas de las características únicas de Kali, se deben hacer algunos cambios. Limitar Debido al impacto de estos cambios, nos esforzamos por enviarlos en sentido ascendente, ya sea integrando la función di- directamente, o agregando los ganchos necesarios para que sea sencillo habilitar las funciones deseadas sin modificar aún más los paquetes ascendentes.

El Kali Package Tracker 10 nos ayuda a realizar un seguimiento de nuestra divergencia con Debian. En cualquier momento, nosotros puede buscar qué paquete se bifurcó y si está sincronizado con Debian, o si hay una actualización

9 9 https://www.debian.org/releases/testing/
10 http://pkg.kali.org/derivative/kali-dev/

es requerido. Todos nuestros paquetes se mantienen en repositorios Git11 alojando una sucursal de Debian y una Rama de Kali de lado a lado. Gracias a esto, actualizar un paquete bifurcado es un proceso simple de dos pasos: actualizar la rama de Debian y luego fusionarla en la rama de Kali.

Si bien la cantidad de paquetes bifurcados en Kali es relativamente baja, la cantidad de paquetes adicionales es bastante alto: en abril de 2017 había casi 400. La mayoría de estos paquetes son software libre Cumplir con las Directrices de software libre de Debian[12] y nuestro objetivo final sería mantener esos paquetes dentro de Debian siempre que sea posible. Eso es por qué nos esforzamos por cumplir con Debian Política[13] y seguir las buenas prácticas de empaquetado utilizadas en Debian. Lamentablemente, también hay Unas cuantas excepciones donde el empaque adecuado era casi imposible de crear. Como resultado de Por poco tiempo, se han enviado pocos paquetes a Debian.

1.3. Propósito y casos de uso

Mientras que el enfoque de Kali puede ser rápidamente resumido como "prueba de penetración y auditoría de seguridad", hay Hay muchas tareas diferentes involucradas detrás de esas actividades. Kali Linux está construido como un *marco* , be- porque incluye muchas herramientas que cubren casos de uso muy diferentes (aunque ciertamente pueden usarse en combinación durante una prueba de penetración).

Por ejemplo, Kali Linux se puede usar en varios tipos de computadoras: obviamente en las computadoras portátiles de probadores de penetración, pero también en servidores de administradores de sistemas que desean monitorear su red trabajo, en las estaciones de trabajo de analistas forenses y, más inesperadamente, en sigilo incrustado sigiloso vicios, generalmente con CPU ARM, que se pueden colocar en el rango de una red inalámbrica o enchufar en la computadora de los usuarios objetivo. Muchos dispositivos ARM también son máquinas de ataque perfectas debido a su factores de forma pequeños y requisitos de baja potencia. Kali Linux también se puede implementar en la nube para construya rápidamente una granja de máquinas para descifrar contraseñas y en teléfonos móviles y tabletas para permitir para pruebas de penetración verdaderamente portátiles.

Pero eso no es todo; los probadores de penetración también necesitan servidores: para usar software de colaboración dentro de un equipo de evaluadores de pen, para configurar un servidor web para su uso en campañas de phishing, para ejecutar vulnerabilidad herramientas de escaneo y otras actividades relacionadas.

Una vez que haya arrancado Kali, descubrirá rápidamente que el menú principal de Kali Linux está organizado por tema a través de los diversos tipos de tareas y actividades que son relevantes para los evaluadores y otros profesionales de seguridad de la información como se muestra en la Figura 1.1 , " Menú de aplicaciones de Kali Linux " [página 6]

[11] https://gitlab.com/kalilinux/packages
[12] https://www.debian.org/social_contract
[13] https://www.debian.org/doc/debian-policy/

Figura 1.1 *Menú de aplicaciones de Kali Linux*

Estas tareas y actividades incluyen:

- Recopilación de información: Recopilación de datos sobre la red objetivo y su estructura, identificar- ing computadoras, sus sistemas operativos y los servicios que ejecutan. Identificación de potencia partes especialmente sensibles del sistema de información. Extraer todo tipo de listados de la ejecución directorio de Servicios.
- Análisis de vulnerabilidad: prueba rápida de si un sistema local o remoto se ve afectado por cantidad de vulnerabilidades conocidas o configuraciones inseguras. Los escáneres de vulnerabilidad usan bases de datos que contienen miles de firmas para identificar posibles vulnerabilidades.

• Análisis de aplicaciones web: identificación de configuraciones incorrectas y debilidades de seguridad en la web aplicaciones. Es crucial identificar y mitigar estos problemas dado que el público está disponible La capacidad de estas aplicaciones los convierte en objetivos ideales para los atacantes.

• Evaluación de la base de datos: desde la inyección de SQL hasta las credenciales de ataque, los ataques a la base de datos son Vector muy común para los atacantes. Herramientas que prueban los vectores de ataque que van desde SQL en Aquí se puede encontrar la extracción de datos y el análisis.

• Ataques de contraseña: los sistemas de autenticación son siempre un vector de ataque. Muchos útiles Las herramientas se pueden encontrar aquí, desde herramientas de ataque de contraseña en línea hasta ataques fuera de línea contra el cifrado o sistemas de hashing.

• Ataques inalámbricos: la naturaleza dominante de las redes inalámbricas significa que siempre ser un vector comúnmente atacado Con su amplia gama de soporte para múltiples tarjetas inalámbricas, Kali es una opción obvia para ataques contra múltiples tipos de redes inalámbricas.

• Ingeniería inversa: la ingeniería inversa es una actividad con muchos propósitos. En apoyo de actividades ofensivas, es uno de los principales métodos para la identificación de vulnerabilidades y

explotar el desarrollo. En el lado defensivo, se utiliza para analizar el malware empleado en tar- ataques geted. En esta capacidad, el objetivo es identificar las capacidades de una determinada pieza de Tradecraft.

• Herramientas de explotación: explotar o aprovechar una vulnerabilidad (anteriormente identificada), le permite obtener el control de una máquina remota (o dispositivo). Este acceso puede ser utilizado para futuros ataques de escalada de privilegios, ya sea localmente en la máquina comprometida o en otras máquinas accesibles en su red local. Esta categoría contiene varias herramientas. y utilidades que simplifican el proceso de escribir sus propios exploits.

• Sniffing & Spoofing: a menudo se accede a los datos a medida que viajan por la red. ventajoso para un atacante. Aquí puede encontrar herramientas de suplantación de identidad que le permiten suplantar un usuario legítimo, así como herramientas de rastreo que le permiten capturar y analizar datos correctamente fuera del cable. Cuando se usan juntas, estas herramientas pueden ser muy poderosas.

• Explotación posterior: una vez que haya obtenido acceso a un sistema, a menudo querrá mantener ese nivel de acceso o extienda el control moviéndose lateralmente a través de la red. Herramientas que Ayuda en estos objetivos se encuentran aquí.

• Forense: los entornos forenses de arranque en vivo de Linux han sido muy populares durante años. Kali contiene una gran cantidad de herramientas forenses populares basadas en Linux que le permiten realizar desde el triaje inicial hasta la obtención de imágenes de datos, el análisis completo y la gestión de casos.

• Herramientas de informes: una prueba de penetración solo se completa una vez que se han informado los resultados. Esta categoría contiene herramientas para ayudar a recopilar los datos recopilados de la recopilación de información. herramientas, descubrir relaciones no obvias y reunir todo en varios informes.

• Herramientas de ingeniería social: cuando el aspecto técnico está bien asegurado, a menudo existe la posibilidad La habilidad de explotar el comportamiento humano como un vector de ataque. Dada la influencia correcta, las personas con frecuencia puede ser inducido a tomar acciones que comprometan la seguridad del medio ambiente. ¿La llave USB que la secretaria acaba de conectar contiene un PDF inofensivo? ¿O fue también un ¿Caballo de Troya que instaló una puerta trasera? ¿Era el sitio web bancario el contador que acaba de iniciar sesión? en el sitio web esperado o una copia perfecta utilizada para fines de phishing? Esta categoría con- contiene herramientas que ayudan en este tipo de ataques.

• Servicios del sistema: esta categoría contiene herramientas que le permiten iniciar y detener aplicaciones que se ejecutan en segundo plano como servicios del sistema.

1.4. Características principales de Kali Linux

Kali Linux es una distribución de Linux que contiene su propia colección de cientos de herramientas de software. específicamente diseñado para sus usuarios objetivo: probadores de penetración y otros profesionales de seguridad. También viene con un programa de instalación para configurar completamente Kali Linux como el principal operador sistema en cualquier computadora.

Esto es muy parecido a todas las otras distribuciones de Linux existentes, pero hay otras características que diferenciar Kali Linux, muchos de los cuales se adaptan a las necesidades específicas de los probadores de penetración. Echemos un vistazo a algunas de esas características.

1.4.1. Un sistema en vivo

Contrariamente a la mayoría de las distribuciones de Linux, la imagen ISO principal que descarga no es simplemente dedicated para instalar el sistema operativo; También se puede utilizar como un sistema de arranque en vivo. En otra Es decir, puede usar Kali Linux sin instalarlo, simplemente iniciando la imagen ISO (generalmente después de haber copiado la imagen en una llave USB).

El sistema en vivo contiene las herramientas más utilizadas por los probadores de penetración, por lo que incluso si su día- el sistema actual no es Kali Linux, simplemente puede insertar el disco o la llave USB y reiniciar para ejecutar Kali. Sin embargo, tenga en cuenta que la configuración predeterminada no preservará los cambios entre reinicios. Si configura la persistencia con una llave USB (consulte la sección 9.4, " Agregar persistencia a la ISO en vivo con una llave USB "[página 240]), luego puede ajustar el sistema a su gusto (modificar archivos de configuración, guardar informes, actualizar software e instalar paquetes adicionales, por ejemplo) y los cambios será retenido a través de reinicios.

1.4.2. Modo forense

En general, cuando se realiza trabajo forense en un sistema, debe evitar cualquier actividad que pueda alterar los datos en el sistema analizado de cualquier manera. Desafortunadamente, los entornos de escritorio modernos tienden interferir con este objetivo al intentar montar automáticamente cualquier disco que detecten. Para evitar esto comportamiento, Kali Linux tiene un modo forense que se puede habilitar desde el menú de arranque: deshabilitará Todas esas características.

El sistema en vivo es particularmente útil para fines forenses, porque es posible reiniciar cualquier computadora en un sistema Kali Linux sin acceder o modificar sus discos duros.

1.4.3. Un kernel de Linux personalizado

Kali Linux siempre proporciona un kernel Linux reciente personalizado, basado en la versión en Debian Unestable. Esto garantiza un soporte de hardware sólido, especialmente para una amplia gama de dispositivos inalámbricos. los kernel está parcheado para soporte de inyección inalámbrica ya que muchas herramientas de evaluación de seguridad inalámbricas confían en esta característica

Dado que muchos dispositivos de hardware requieren archivos de firmware actualizados (que se encuentran en `/ lib / firmware /`), Kali los instala por defecto, incluido el firmware disponible en la sección no libre de Debian. Aquellos no se instalan por defecto en Debian, porque son de código cerrado y, por lo tanto, no forman parte de Debian apropiado.

1.4.4. Completamente personalizable

Kali Linux está construido por probadores de penetración para probadores de penetración, pero entendemos que no Eryone estará de acuerdo con nuestras decisiones de diseño o elección de herramientas para incluir por defecto. Con esto en Recuerde, siempre nos aseguramos de que Kali Linux sea fácil de personalizar según sus propias necesidades y preferimos ences. Con este fin, publicamos la configuración de construcción en vivo utilizada para construir las imágenes oficiales de Kali, por lo que puedes personalizarlo a tu gusto. Es muy fácil comenzar desde esta configuración publicada y Implemente varios cambios según sus necesidades gracias a la versatilidad de live-build.

Live-build incluye muchas características para modificar el sistema instalado, instalar archivos suplementarios, detener paquetes adicionales, ejecutar comandos arbitrarios y cambiar los valores pre-sembrados a debconf.

1.4.5. Un sistema operativo confiable

Los usuarios de una distribución de seguridad legítimamente quieren saber que se puede confiar y que ha sido desarrollado a simple vista, lo que permite a cualquiera inspeccionar el código fuente. Kali Linux es desarrollado por Un pequeño equipo de desarrolladores expertos que trabajan de forma transparente y siguen la mejor seguridad prácticas: cargan paquetes fuente firmados, que luego se crean en demonios de compilación dedicados. Los paquetes se suman y se distribuyen como parte de un repositorio firmado.

El trabajo realizado en los paquetes se puede revisar completamente a través de los repositorios Git de empaquetado [14] (que contienen etiquetas firmadas) que se utilizan para construir los paquetes fuente de Kali. La evolución de cada

el paquete también se puede seguir a través del rastreador de paquetes Kali[15] .

1.4.6. Utilizable en una amplia gama de dispositivos ARM

Kali Linux proporciona paquetes binarios para las arquitecturas ARM armel, armhf y arm64. Gracias a las imágenes fácilmente instalables proporcionadas por Offensive Security, Kali Linux puede implementarse en muchos dispositivos interesantes, desde teléfonos inteligentes y tabletas hastaWi-Firouters y computadoras de varios formas y tamaños.

1.5. Políticas de Kali Linux

Mientras Kali Linux se esfuerza por seguir la política de Debian cuando sea posible, hay algunos en algún lugar Hicimos elecciones de diseño significativamente diferentes debido a las necesidades particulares de la profesión de seguridad. als.

[14] https://gitlab.com/kalilinux/packages
[15] http://pkg.kali.org

1.5.1. Usuario raíz único por defecto

La mayoría de las distribuciones de Linux fomentan, con bastante sensatez, el uso de una cuenta no privilegiada mientras se ejecuta El sistema y el uso de una utilidad como `sudo` cuando se necesitan privilegios administrativos. Esta es un buen consejo de seguridad, que proporciona una capa adicional de protección entre el usuario y cualquier potencial comandos u operaciones del sistema operativo que son disruptivos o destructivos. Esto es especialmente cierto para sistemas de múltiples usuarios, donde la separación de privilegios de usuario es un requisito: mal comportamiento por parte de uno El usuario puede interrumpir o destruir el trabajo de muchos usuarios.

Dado que muchas herramientas incluidas en Kali Linux solo pueden ejecutarse con privilegios de root, esta es la definición falla en la cuenta de usuario de Kali. A diferencia de otras distribuciones de Linux, no se le pedirá que cree un usuario sin privilegios al instalar Kali. Esta política particular es una desviación importante de la mayoría Los sistemas Linux y tienden a ser muy confusos para los usuarios menos experimentados. Los principiantes deben ser Especialmente cuidadoso al usar Kali, ya que la mayoría de los errores destructivos ocurren cuando se opera con root privilegios

1.5.2. Servicios de red deshabilitados por defecto

A diferencia de Debian, Kali Linux deshabilita cualquier servicio instalado que escuche en una red pública. interfaz de trabajo por defecto, como HTTP y SSH.

La razón detrás de esta decisión es minimizar la exposición durante una prueba de penetración cuando es en detrimento de anunciar su presencia y detección de riesgos debido a la interferencia inesperada de la red comportamiento.

Aún puede habilitar manualmente cualquier servicio de su elección ejecutando `systemctl enable` *servicio* . Volveremos a esto en el capítulo 5 , "Configuración de Kali Linux "[página 104] más adelante en este libro.

1.5.3. Una colección curada de aplicaciones

Debian pretende ser el sistema operativo universal y pone muy pocos límites en lo que se empaqueta, siempre que cada paquete tenga un mantenedor.

Por el contrario, Kali Linux no incluye todas las herramientas de prueba de penetración disponibles. En lugar, nuestro objetivo es proporcionar solo las mejores herramientas con licencia libre que cubran la mayoría de las tareas que un probador de penetración podría querer realizar.

Los desarrolladores de Kali que trabajan como probadores de penetración impulsan el proceso de selección y nosotros aprovechamos sus experiencia y pericia para tomar decisiones inteligentes. En algunos casos esto es una cuestión de hecho, pero Hay otras opciones más difíciles que simplemente se reducen a preferencias personales.

Estos son algunos de los puntos considerados cuando se evalúa una nueva aplicación:

- La utilidad de la aplicación en un contexto de prueba de penetración.

- La funcionalidad única de las características de la aplicación.
- La licencia de la aplicación.
- Los requisitos de recursos de la aplicación.

Mantener un repositorio de herramientas de prueba de penetración actualizado y útil es una tarea difícil. Nosotros Bienvenido sugerencias de herramientas dentro de una categoría dedicada (*NewToolRequests*) en el Kali Bug Tracker[16] . Las nuevas solicitudes de herramientas se reciben mejor cuando la presentación está bien presentada, incluida una explicación. mencione por qué la herramienta es útil, cómo se compara con otras aplicaciones similares, etc.

1.6. Resumen

En este capítulo, le presentamos a Kali Linux, le proporcionamos un poco de historia, repasamos algunos de las características principales, y presentó varios casos de uso. También hemos discutido algunos de los políticas que hemos adoptado al desarrollar Kali Linux.

Consejos resumidos:

- Kali Linux [17] es una distribución de Linux de auditoría de seguridad lista para empresas basada en Debian GNU / Linux. Kali está dirigido a profesionales de seguridad y administradores de TI, lo que les permite para realizar pruebas de penetración avanzadas, análisis forenses y auditorías de seguridad.
- A diferencia de la mayoría de los sistemas de operaciones principales, Kali Linux distribuye la distribución, lo que significa que *recibirás actualizaciones todos los días* .
- La distribución de Kali Linux se basa en las pruebas de Debian [18] . Por lo tanto, la mayoría de los paquetes disponible en Kali Linux viene directamente de este repositorio de Debian.
- Si bien el enfoque de Kali se puede resumir rápidamente con “pruebas de penetración y auditoría de seguridad- ing ", hay varios casos de uso, incluidos los administradores de sistemas que desean monitorear sus redes, análisis forense, instalaciones de dispositivos integrados, monitoreo inalámbrico, instalación ción en plataformas móviles y más.
- Los menús de Kali facilitan el acceso a herramientas para diversas tareas y actividades que incluyen: vulnerabilidades- análisis de capacidad, análisis de aplicaciones web, evaluación de bases de datos, ataques de contraseña, conexión inalámbrica tachuelas, ingeniería inversa, herramientas de explotación, sniffing y spoofing, herramientas de post explotación, medicina forense, herramientas de informes, herramientas de ingeniería social y servicios de sistemas.
- Kali Linux tiene muchas características avanzadas que incluyen: uso como un sistema en vivo (no instalado), un ro- busto y modo forense seguro, un kernel de Linux personalizado, capacidad de personalizar completamente el sistema, un sistema operativo base confiable y seguro, capacidad de instalación ARM, seguridad segura políticas de red de fallas y un conjunto de aplicaciones seleccionadas.

En el próximo capítulo, entraremos y probaremos Kali Linux gracias a su modo en vivo.

dieciséis http://bugs.kali.org
17 https://www.kali.org
18 años https://www.debian.org/releases/testing/

Palabras clave

Descargar
Imagen ISO
Arranque en vivo

Capítulo

2

Empezar con Kali Linux

Contenido

Descargar una imagen ISO de Kali 14
Arranque de una imagen ISO de Kali en modo en vivo 24
Resumen 43

A diferencia de algunos sistemas de operaciones, Kali Linux hace que se inicien las ideas, gracias por el hecho de que sus imágenes de disco son *ISO en vivo* , lo que significa que puede iniciar la imagen descargada sin seguir Cualquier procedimiento de instalación previa. Esto significa que puede usar la misma imagen para probar, para usar como una imagen de arranque de USB o DVD-ROM en un estuche forense, o para instalar como una operación permanente sistema en hardware físico o virtual.

Debido a esta simplicidad, es fácil olvidar que se deben tomar ciertas precauciones. Usuarios de Kali a menudo son el objetivo de aquellos con malas intenciones, ya sean grupos patrocinados por el estado, elementos de organización crímenes identificados o piratas informáticos individuales. La naturaleza de código abierto de Kali Linux lo hace relativamente fácil para construir y distribuir versiones falsas, por lo que es esencial que te acostumbres a descargar de fuentes originales y verificar la integridad y la autenticidad de su descarga. Esto es especialmente relevante para los profesionales de seguridad que a menudo tienen acceso a redes sensibles y son encargado de los datos del cliente.

2.1. Descargar una imagen ISO de Kali

2.1.1 Donde descargar

La única fuente oficial de imágenes ISO de Kali Linux es la sección de Descargas del sitio web de Kali. Debido a su popularidad, los números de sitios ofrecen imágenes de Kali para la descarga, pero no deben considerarse confiable y de hecho puede estar infectado con malware o causar daños irreparables a tu sistema.

[2] https://www.kali.org/downloads/

El sitio web está disponible a través de *HTTPS* , por lo que es difícil suplantar. Ser capaz de llevar a cabo un ataque de hombre en el medio no es suficiente ya que el atacante también necesitaría un cerro www.kali.org certificado firmado por una autoridad de certificación de Seguridad de la capa de transporte (TLS) en la que confía la víctima El navegador de tim. Debido a que las autoridades de certificación existen precisamente para prevenir este tipo de problema, entregar certificados solo a personas cuyas identidades hayan sido verificadas y que hayan proporcionado evidencia de que controlan el sitio web correspondiente.

cdimage.kali.org Los enlaces que se encuentran en la página de descarga apuntan al dominio cdimage.kali.org , que redirige a un espejo cerca de usted, mejorando su velocidad de transferencia mientras reduce carga sobre los servidores centrales de Kali.

Puede encontrar una lista de espejos disponibles aquí:

[2] http://cdimage.kali.org/README.mirrorlist

2.1.2. Qué descargar

La página de descarga oficial muestra una breve lista de imágenes ISO, como se muestra en la Figura 2.1, " Lista de imágenes Ofrecido para descargar "[página 15].

Figura 2.1 *Lista de imágenes ofrecidas para descargar*

Todas las imágenes de disco etiquetadas de 32 o 64 bits se refieren a imágenes adecuadas para CPU, que se encuentran en la mayoría de los escritorios modernos. Computadoras superiores y portátiles. Si está descargando para usar en una máquina bastante moderna, la mayoría probablemente contiene un procesador de 64 bits. Si no está seguro, tenga la seguridad de que todos los procesadores de 64 bits pueden ejecutarse Instrucciones de 32 bits. Siempre puede descargar y ejecutar la imagen de 32 bits. Lo opuesto no es verdad, sin embargo. Consulte la barra lateral para obtener información más detallada.

Si planea instalar Kali en un dispositivo integrado, teléfono inteligente, Chromebook, punto de acceso, o cualquier otro dispositivo con un procesador ARM, debe usar las imágenes *armel* o *armhf de* Linux .

¿Mi CPU es de 32 o 64 bits? En Windows, puede encontrar esta información ejecutando la *Información del sistema* aplicación (que se encuentra en la carpeta Accesorios> Herramientas del sistema). En el resumen del sistema pantalla, puede inspeccionar el campo Tipo de sistema: contendrá "PC basada en x64" para un 64-CPU de bit o “PC basada en x86” para una CPU de 32 bits.

Bajo OS X / macOS, no hay una aplicación estándar que muestre esta información pero aún puede inferirlo de la salida del comando `uname -m` ejecutado en la terminal. Se volverá `x86_64` en un sistema con un núcleo de 64 bits (que sólo puede ejecutarse en un 64 bits CPU) y en sistemas con un núcleo de 32 bits, devolverá `i386` o algo similar (`i486` , `i586` o `i686`). Cualquier kernel de 32 bits puede ejecutarse en una CPU de 64 bits, pero desde Apple controla el hardware y el software, es poco probable que encuentre esta configuración.

En Linux, puede inspeccionar el campo de marcas en el archivo virtual `/ proc / cpuinfo` . Si se contiene el atributo `lm` , entonces su CPU es de 64 bits; de lo contrario, es de 32 bits. los La siguiente línea de comando le dirá qué tipo de CPU tiene:

```
$ grep -qP '^ flags \ s *:. * \ blm \ b' / proc / cpuinfo && echo 64-bit
        ‾ || echo 32 bits
64 bits
```

Ahora que ya sabe si tiene una imagen de 32 bits o 64 bits, solo hay un intervalo: seleccionar El tipo de imagen. La imagen predeterminada de Kali Linux y la variante de Kali Linux Light son ISO en vivo que se puede usar para ejecutar el sistema en vivo o para iniciar el proceso de instalación. Se diferencian solo por el conjunto de aplicaciones preinstaladas. La imagen predeterminada viene con el escritorio GNOME y un gran Colección de paquetes que se consideran apropiados para la mayoría de los probadores de penetración, mientras que la imagen clara viene con el escritorio Xfce (que es mucho menos exigente con los recursos del sistema) y un colección de paquetes, lo que le permite elegir solo las aplicaciones que necesita. Las imágenes restantes usa entornos de escritorio alternativos pero viene con la misma colección de paquetes grandes que la principal imagen.

Una vez que haya decidido que no se aplicará una imagen, puede descargar la imagen haciendo clic en "ISO" en la fila respectiva Alternativamente, puede descargar la imagen de BitTorrent peer-to-peer red haciendo clic en "Torrent", siempre que tenga un cliente BitTorrent asociado con el .torrent extensión.

Mientras se descarga la imagen ISO elegida, debe tomar nota de la suma de comprobación escrita en el columna sha256sum. Una vez que haya descargado su imagen, use esta suma de verificación para verificar que la imagen descargada coincide con la que el equipo de desarrollo de Kali puso en línea (consulte la siguiente sección).

2.1.3. Verificación de integridad y autenticidad

Los profesionales de seguridad deben verificar la integridad de sus herramientas para no solo proteger sus datos y redes pero también las de sus clientes. Mientras que la página de descarga de Kali está protegida por TLS, la actual el enlace de descarga apunta a una URL no encriptada que no ofrece protección contra posibles intrusos los ataques del medio. El hecho de que Kali se base en una red de espejos externos para distribuir el

imagen significa que no debes confiar ciegamente en lo que descargas. El espejo al que fuiste dirigido puede haber sido comprometido, o usted mismo podría ser víctima de un ataque.

Para aliviar esto, el proyecto Kali siempre proporciona sumas de verificación de las imágenes que distribuye. Sino para hacer efectivo dicho control, debe asegurarse de que la suma de control que tomó sea efectivamente suma de comprobación publicada por los desarrolladores de Kali Linux. Tienes diferentes formas de determinar esto.

Confiar en el sitio web protegido por TLS

Cuando recupera la suma de comprobación de la página web de descarga protegida por TLS, su origen es indi- garantizado directamente por el modelo de seguridad del certificado X.509: el contenido que ve proviene de una web sitio que está efectivamente bajo el control de la persona que solicitó el certificado TLS.

Ahora debe generar la suma de comprobación de su imagen descargada y asegurarse de que coincida lo que grabaste del sitio web de Kali:

```
$ sha256sum kali-linux-2017.1-amd64.iso
49b1c5769b909220060dc4c0e11ae09d97a270a80d259e05773101df62e11e9d                    kali-linux-2016.2-amd64.iso
```

Si su suma de comprobación generada coincide con la de la página de descarga de Kali Linux, tiene el archivo rect. Si las sumas de verificación difieren, hay un problema, aunque esto no indica un compromiso o un ataque; las descargas ocasionalmente se corrompen cuando atraviesan Internet. Prueba tu down- cargar de nuevo, desde otro espejo oficial de Kali, si es posible (ver " cdimage.kali.org "[página 14] para más información sobre espejos disponibles).

Confiando en la Web de confianza de PGP

Si no confías en HTTPS para la autenticación, eres un poco paranoico, pero con razón. Existen muchos ejemplos de autoridades certificadoras mal administradas que emitieron certificados falsos, que terminó siendo mal utilizado. También puede ser víctima de un hombre "amigable" en el medio táctica implementada en muchas redes corporativas, utilizando una tienda de confianza personalizada, implantada en el navegador que presenta certificados falsos a sitios web encriptados, lo que permite a los auditores corporativos monitorear tráfico encriptado

Para casos como este, también proporcionamos una clave GnuPG que usamos para firmar las sumas de verificación de las imágenes proporcionamos. Los identificadores de la clave y sus huellas digitales se muestran aquí:

```
pub     rsa4096 / 0xED444FF07D8D0BF6 2012-03-05 [SC] [caduca: 2018-02-02]
        Huella digital clave = 44C6 513A 8E4F B3D3 0875 F758 ED44 4FF0 7D8D 0BF6
uid                          [completo] Kali Linux Repository <devel@kali.org>
sub     rsa4096 / 0xA8373E18FC0D0DCB 2012-03-05 [E] [caduca: 2018-02-02]
```

Esta clave es parte de una *red* global *de confianza* porque al menos la he firmado (Raphaël Hertzog) y soy parte de la red de confianza debido a mi gran uso de GnuPG como desarrollador de Debian.

El modelo de seguridad PGP / GPG es muy exclusivo. Cualquiera puede generar cualquier clave con cualquier identidad, pero solo confiaría en que esa clave si ha sido firmada por otra clave que ya confía. Cuando usted firmar una clave, certifica que conoció al titular de la clave y que sabe que el asociado La identidad es correcta. Y define el conjunto inicial de claves en las que confía, que obviamente incluye tu propia llave

Este modelo tiene sus propias limitaciones, por lo que puede optar por descargar la clave pública de Kali a través de HTTPS (o de un servidor de claves) y simplemente decida que confía en él porque su huella digital coincide con lo que enumerado en varios lugares, incluido el anterior en este libro:

```
$ wget -q -O - https://www.kali.org/archive-key.asc | gpg --import
[o]
$ gpg --keyserver hkp: //keys.gnupg.net --recv-key ED444FF07D8D0BF6
```

```
gpg: clave 0xED444FF07D8D0BF6: clave pública "Kali Linux Repository <devel@kali.org>" importado
gpg: Número total procesado: 1
gpg:                importado: 1 (RSA: 1)
[...]
$ gpg - huella digital 7D8D0BF6
[...]
      Huella digital clave = 44C6 513A 8E4F B3D3 0875 F758 ED44 4FF0 7D8D 0BF6
[...]
```

Después de recuperar la clave, puede usarla para verificar las sumas de verificación de la imagen distribuida. siglos. Descarguemos el archivo con las sumas de verificación (SHA256SUMS) y el archivo de firma asociado (SHA256SUMS.gpg) y verifique la firma:

```
$ wget http://cdimage.kali.org/current/SHA256SUMS
[...]
$ wget http://cdimage.kali.org/current/SHA256SUMS.gpg
[...]
$ gpg --verify SHA256SUMS.gpg SHA256SUMS
gpg: Firma realizada el jue 16 mar 2017 08:55:45 MDT
gpg:                utilizando la clave RSA ED444FF07D8D0BF6
gpg: Buena firma de "Kali Linux Repository <devel@kali.org>"
```

Si recibe el mensaje "Buena firma", puede confiar en el contenido del archivo SHA256SUMS y usar para verificar los archivos que descargaste. De lo contrario, hay un problema. Debes revisar si descargó los archivos de un espejo legítimo de Kali Linux.

Tenga en cuenta que puede usar la siguiente línea de comando para verificar que el archivo descargado tenga el mismo suma de comprobación que figura en SHA256SUMS , siempre que el archivo ISO descargado esté en la misma dirección conservador:

```
$ grep kali-linux-2017.1-amd64.iso SHA256SUMS | sha256sum -c
kali-linux-2017.1-amd64.iso: OK
```

Si no obtiene una respuesta correcta, el archivo que ha descargado es diferente del arrendado por el equipo de Kali. No se puede confiar y no se debe usar.

2.1.4. Copiar la imagen en un DVD-ROM o llave USB

A menos que desee ejecutar Kali Linux en una máquina virtual, la imagen ISO es de uso limitado en y de sí mismo. Debe grabarlo en un DVD-ROM o copiarlo en una llave USB para poder iniciar su máquina en Kali Linux.

No cubriremos cómo grabar la imagen ISO en un DVD-ROM, ya que el proceso varía mucho según la plataforma. forma y entorno, pero en la mayoría de los casos, hacer clic derecho en el archivo .iso presentará un contexto elemento de menú que ejecuta una aplicación de grabación de DVD-ROM. ¡Pruébalo!

Advertencia

En esta sección, aprenderá a sobrescribir un disco arbitrario con un Kali Imagen ISO de Linux. Siempre verifique dos veces el disco de destino antes de iniciar la operación como un solo error probablemente causaría la pérdida completa de datos y posiblemente dañe su configuración sin posibilidad de reparación.

Crear una unidad USB de arranque Kali en Windows

Como requisito previo, debe descargar e instalar *Win32 Disk Imager* :

[2] https://sourceforge.net/projects/win32diskimager/

Conecte su llave USB a su PC con Windows y observe el designador de unidad asociado a ella (para examen-
ple, "E: \").

Inicie *Win32 Disk Imager* y elija el archivo ISO Kali Linux que desea copiar en la llave USB.
Verifique que la letra del dispositivo seleccionado corresponda con la asignada a la llave USB. Una vez
está seguro de haber seleccionado la unidad correcta, haga clic en el botón Escribir y confirme que
desea sobrescribir el contenido de la llave USB como se muestra en la Figura 2.2 , " Win32 Disk Imager en
acción"[Página 20].

Figura 2.2 *Win32 Disk Imager en acción*

Una vez completada la copia, expulse de forma segura la unidad USB del sistema de Windows. Tu puedes ahora
use el dispositivo USB para arrancar Kali Linux.

Crear una unidad USB de arranque Kali en Linux

Crear una llave USB de arranque Kali Linux en un entorno Linux es fácil. El entorno de escritorio GNOME
ronment, que se instala por defecto en muchas distribuciones de Linux, viene con una utilidad *Disks* (en
el paquete *gnome-disk-utility* , que ya está instalado en la imagen estándar de Kali). Ese programa
muestra una lista de discos, que se actualiza dinámicamente cuando conecta o desconecta un disco. Cuando ves
seleccione su llave USB en la lista de discos, aparecerá información detallada y le ayudará a confirmar
que seleccionaste el disco correcto. Tenga en cuenta que puede encontrar el nombre de su dispositivo en la barra de título como se muestra
en la figura 2.3, " Discos de GNOME " [página 21].

Figura 2.3 *Discos de GNOME*

Haga clic en el botón de menú y seleccione Restaurar imagen de disco ... en el menú emergente que se muestra. Seleccione la imagen ISO que descargó anteriormente y haga clic en Iniciar restauración ... como se muestra en la Figura 2.4 , " Cuadro de diálogo Restaurar imagen de disco "[Página 21].

Figura 2.4 Cuadro de *diálogo Restaurar imagen de disco*

Disfrute de una taza de café mientras termina de copiar la imagen en la llave USB (Figura 2.5" Progresión de la restauración de la imagen"[Página 22]).

Figura 2.5 *Progresión de la restauración de imagen*

Crea el USB de arranque Conduce desde el comando Línea

Aunque el proceso gráfico es bastante sencillo, la operación es igual de Fácil para usuarios de línea de comandos.

Cuando inserte su llave USB, el kernel de Linux lo detectará y le asignará un nombre, que se imprime en los registros del núcleo. Puede encontrar su nombre inspeccionando los registros devuelto por dmesg .

```
$ dmesg
[...]
[234743.896134] usb 1-1.2: nuevo dispositivo USB de alta velocidad número 6 usando ehci-pci
[234743.990764] usb 1-1.2: Nuevo dispositivo USB encontrado, idVendor = 08ec, idProduct = 0020
[234743.990771] usb 1-1.2: nuevas cadenas de dispositivos USB: Mfr = 1, Producto = 2,
                Número de serie = 3
[234743.990774] usb 1-1.2: Producto: Store'n'go
[234743.990777] usb 1-1.2: Fabricante: Verbatim
[234743.990780] usb 1-1.2: Número de serie: 0390627052A2F897
[234743.991845] almacenamiento usb 1-1.2: 1.0: dispositivo de almacenamiento masivo USB detectado
[234743.992017] scsi host7: almacenamiento usb 1-1.2: 1.0
[234744.993818] scsi 7: 0: 0: 0: acceso directo                VBTM    Store'n'go       6.51
                PQ: 0 ANSI: 0 CCS
[234744.994425] sd 7: 0: 0: 0: adjunto scsi genérico sg1 tipo 0
[234744.995753] sd 7: 0: 0: 0: [sdb] 3903487 Bloques lógicos de 512 bytes: (2.00 GB
                /1.86 GiB)
[234744.996663] sd 7: 0: 0: 0: [sdb] La protección contra escritura está desactivada
[234744.996669] sd 7: 0: 0: 0: [sdb] Sentido de modo: 45 00 00 08
[234744.997518] sd 7: 0: 0: 0: [sdb] No se encontró la página del modo de almacenamiento en caché
[234744.997524] sd 7: 0: 0: 0: [sdb] Suponiendo caché de unidad: escribir a través
[234745.009375]                 sdb: sdb1
```

```
[234745.015113] sd 7: 0: 0: 0: [sdb ] Disco extraible SCSI adjunto
```

Ahora que sabe que la llave USB está disponible como `/ dev / sdb` , puede proceder a copia la imagen con el comando `dd` :

```
# dd if = kali-linux-light-2017.1-amd64.iso of = / dev / sdb
2070784 + 0 registros en
2070784 + 0 registros
1060241408 bytes (1.1 GB, 1011 MiB) copiados, 334.175 s, 3.2 MB / s
```

Tenga en cuenta que necesita permisos de root para que esta operación tenga éxito y debe también asegúrese de que la llave USB no se use. Es decir, debe asegurarse de que ninguno de sus particiones están montadas. El comando también supone que se ejecuta mientras está en el directorio que aloja la imagen ISO; de lo contrario, se deberá proporcionar la ruta completa.

Como referencia, `si` significa "archivo de entrada" y `de` "archivo de salida". El comando `dd` lee datos del archivo de entrada y los vuelve a escribir en el archivo de salida. No muestra ninguna información sobre el progreso, por lo que debe ser paciente mientras realiza su trabajo (no es inusual para que el comando tome más de media hora!). Mire el LED de actividad de escritura encendido la llave USB si desea verificar que el comando esté funcionando. Las estadísticas que se muestran arriba solo se muestran cuando el comando se ha completado. En OS X / macOS, También puede presionar CTRL + T durante la operación para obtener información estadística sobre la copia incluye cuántos datos se han copiado.

Creación de una unidad USB de arranque Kali en OS X / macOS

OS X / macOS se basa en UNIX, por lo que el proceso de creación de una unidad USB de arranque Kali Linux es similar al procedimiento de Linux. Una vez que haya descargado y verificado su archivo Kali ISO elegido, use `dd` para copiarlo en tu memoria USB.

Para identificar el nombre del dispositivo de la llave USB, ejecute `diskutil list` para enumerar los discos disponibles en tu sistema. Luego, inserte su llave USB y ejecute el comando `diskutil list` nuevamente. El segundo La salida debe incluir un disco adicional. Puede determinar el nombre del dispositivo de la llave USB mediante paring la salida de ambos comandos. Busque una nueva línea que identifique su disco USB y anote el `/ dev / disk X` , donde *X* representa el ID del disco.

Debe asegurarse de que la llave de EE. UU. No esté montada, lo que puede lograrse con un valor no explícito Desmontar comando (suponiendo que `/ dev / disk6` es el nombre del dispositivo de la llave USB):

```
$ diskutil desmontar / dev / disk6
```

Ahora proceda a ejecutar el comando `dd` . Esta vez, agregue un parámetro suplementario - bs para tamaño de bloque. Define el tamaño del bloque que se lee del archivo de entrada y luego se escribe en el archivo de salida.

```
# dd if = kali-linux-light-2017.1-amd64.iso of = / dev / disk6 bs = 1M
1011 + 0 registros en
1011 + 0 registros
1060241408 bytes transferidos en 327.061 segundos (3242328 bytes / segundo)
```

Eso es. Su llave USB ya está lista y puede arrancar desde ella o usarla para instalar Kali Linux.

Arrancar un disco alternativo en OS X / macOS

Para iniciar desde una unidad alternativa en un sistema OS X / macOS, abra el menú de inicio manteniendo presionada la tecla Opción inmediatamente después de encender el dispositivo y seleccionando la unidad que desea utilizar.

Para obtener más información, consulte la base de conocimiento de Apple[1] .

[1] http://support.apple.com/kb/ht1310

2.2. Arranque de una imagen ISO de Kali en modo en vivo

2.2.1. En una computadora real

Como requisito previo, necesita una llave USB preparada (como se detalla en la sección anterior) o un DVD-ROM grabado con una imagen ISO Kali Linux.

El BIOS / UEFI es responsable del proceso de arranque temprano y se puede configurar a través de una pieza de software llamado Setup. En particular, permite a los usuarios elegir qué dispositivo de arranque se prefiere. En en este caso, desea seleccionar la unidad de DVD-ROM o la unidad USB, según el dispositivo usted ha creado

Comenzar la configuración generalmente implica presionar una tecla en particular muy pronto después de que la computadora está encendida en. Esta tecla suele ser Del o Esc, y a veces F2 o F10. La mayoría de las veces, la elección es brevemente parpadeaba en la pantalla cuando la computadora se enciende, antes de que se cargue el sistema operativo.

Una vez que el BIOS / UEFI se ha configurado correctamente para arrancar desde su dispositivo, arranque Kali Linux es simplemente una cuestión de insertar el DVD-ROM o enchufar la unidad USB y encender el computadora.

Deshabilitar el arranque seguro Si bien las imágenes de Kali Linux pueden arrancarse en modo UEFI, no admiten *seguridad de arranque* . Debe deshabilitar esa función en la Configuración.

2.2.2. En una máquina virtual

Las máquinas virtuales tienen múltiples beneficios para KaliLinuxusers. Son especialmente útiles para usar probar Kali Linux pero no está listo para comprometerse a instalarlo permanentemente en su máquina o si Tiene un sistema potente y desea ejecutar varios sistemas operativos simultáneamente. Esto es un Elección popular para muchos probadores de penetración y profesionales de seguridad que necesitan utilizar el amplio gama de herramientas disponibles en Kali Linux pero aún así quieren tener acceso completo a su funcionamiento primario sistema. Esto también les brinda la capacidad de archivar o eliminar de forma segura la máquina virtual y cualquier información del cliente que pueda contener en lugar de reinstalar todo su sistema operativo.

Las características de instantánea del software de virtualización también hacen que sea fácil experimentar con posibles operaciones peligrosas, como el análisis de malware, al tiempo que permite una salida fácil mediante la restauración Una instantánea anterior.

Hay muchas herramientas de virtualización disponibles para todos los sistemas de operaciones principales, incluyendo *VirtualBox*® , *VMware Workstation*® , *Xen* , *KVM* e *Hyper-V,* por nombrar algunos. En última instancia, utilizará el que se adapta mejor a usted, pero cubriremos los dos más utilizados en un contexto de escritorio: *VirtualBox*® y *VMware Workstation Pro*® , ambos ejecutándose en Windows 10. Si no tiene una política corporativa restricciones o preferencias personales, nuestra recomendación es que primero pruebe VirtualBox, ya que es gratuito, funciona bien, es (principalmente) de código abierto y está disponible para la mayoría de los sistemas operativos.

Para las siguientes secciones, supondremos que ya ha instalado la virtualización adecuada herramienta y están familiarizados con su funcionamiento.

Para beneficiarse completamente de la virtualización, debe tener una CPU con la virtualización adecuada características y no deben ser deshabilitados por el BIOS / UEFI. Verifique dos veces cualquier "Intel® Virtual-ization Technology "y / o" Intel® VT-d Feature "opciones en las pantallas de Configuración.

También debe tener un sistema operativo host de 64 bits, como la arquitectura amd64 para Debian Distribuciones de Linux, arquitectura x86_64 para distribuciones Linux basadas en RedHat y Windows ... 64-poco para Windows.

Si no tiene ninguno de los requisitos previos, la herramienta de virtualización no funcionará correctamente o funcionará restringirse a ejecutar solo sistemas operativos invitados de 32 bits.

Dado que las herramientas de virtualización se enganchan en el sistema operativo host y el hardware en un nivel bajo, existe A menudo son incompatibilidades entre ellos. No espere que estas herramientas funcionen bien al mismo tiempo hora. Además, tenga en cuenta que las versiones profesionales de Windows vienen con *Hyper-V* instalado y abled, lo que podría interferir con su herramienta de virtualización de elección. Para desactivarlo, ejecute "Activar funciones de Windows activadas o desactivadas "desde la Configuración de Windows.

VirtualBox

Después de la instalación inicial, la pantalla principal de VirtualBox se parece a la Figura 2.6, " Virtual-Pantalla de inicio de Box "[página 26].

Figura 2.6 *Pantalla de inicio de VirtualBox*

Haga clic en Nuevo (Figura 2.7, " Nombre y sistema operativo "[Página 27]) para iniciar un asistente que lo guiará a través de los múltiples pasos necesarios para ingresar todos los parámetros de la nueva máquina virtual.

Figura 2.7 *Nombre y sistema operativo*

En el primer paso, que se muestra en la Figura 2.7, " Nombre y sistema operativo "[Página 27], debe asignar un nombre a su nueva máquina virtual. Utilice "Kali Linux". También debe indicar qué tipo de operación Se utilizará el sistema ing. Como Kali Linux está basado en Debian GNU / Linux, seleccione Linux para el tipo y Debian (32 bits) o Debian (64 bits) para la versión. Aunque cualquier otra versión de Linux será más probablemente funcione, esto ayudará a distinguir entre las diversas máquinas virtuales que pueda tener instalado

Figura 2.8 *Tamaño de memoria*

En el segundo paso, debe decidir cuánta memoria asignar a la máquina virtual. Mientras
El tamaño recomendado de 768 MB es aceptable para una máquina virtual Debian que actúa como servidor.
definitivamente no es suficiente para ejecutar un sistema de escritorio Kali, especialmente no para un sistema Kali Linux en vivo
ya que el sistema en vivo usa memoria para almacenar los cambios realizados en el sistema de archivos. Nosotros recomendamos
aumentar el valor a 1500 MB (Figura 2.8 , " Tamaño de la memoria "[Página 28]) y recomiendo encarecidamente que
Usted asigna no menos de 2048 MB de RAM.

Figura 2.9 *Disco duro*

En el tercer paso (que se muestra en la Figura 2.9, " Disco duro "[Página 29]), se le solicita que elija un
disco duro virtual o cal para su nueva máquina virtual. Aunque no se requiere un disco duro para ejecutar
Kali Linux como sistema en vivo, agregue uno para cuando demostremos el procedimiento de instalación más tarde, en
Capítulo 4 , " Instalación de Kali Linux "[Página 66].

Figura 2.10 *Tipo de archivo de disco duro*

El contenido del disco duro de la máquina virtual se almacena en la máquina host como un archivo. VirtualBox puede almacenar el contenido del disco duro usando múltiples formatos (como se muestra en la Figura 2.10 , " Tipo de archivo de disco duro "[Página 30]): el valor predeterminado (VDI) corresponde al formato nativo de VirtualBox; VMDK es el formato utilizado por VMware; QCOW es el formato utilizado por QEMU. Mantenga el valor predeterminado porque no tienes ninguna razón para cambiarlo. La capacidad de usar múltiples formatos es interesante principalmente cuando desea mover una máquina virtual de una herramienta de virtualización a otra.

Figura 2.11 *Almacenamiento en disco duro físico*

El texto explicativo en la Figura 2.11 , "Almacenamiento en disco duro físico "[página 31] describe claramente
Las ventajas y desventajas de la asignación dinámica y fija de discos. En este ejemplo, aceptamos
la selección predeterminada (asignada dinámicamente), ya que estamos usando una computadora portátil con discos SSD. Nosotros no
quiere desperdiciar espacio y no necesitará el rendimiento extra ya que la máquina ya está bastante
rápido para empezar.

Figura 2.12 *Ubicación y tamaño del archivo*

El tamaño predeterminado del disco duro de 8 GB se muestra en la Figura 2.12 , "Ubicación y tamaño del archivo"[Página 32] no es
suficiente para una instalación estándar de Kali Linux, así que aumente el tamaño a 20 GB. También puedes ajustar
el nombre y la ubicación de la imagen de disco. Esto puede ser fácil cuando no hay suficiente espacio

en su disco duro, lo que le permite almacenar la imagen del disco en una unidad externa.

Figura 2.13 *La nueva máquina virtual aparece en la lista*

La máquina virtual se ha creado, pero aún no se puede ejecutar, porque no hay operación
Sistema instalado. También tiene algunas configuraciones para ajustar. Haga clic en Configuración en VM Manager
pantalla y repasemos algunas de las configuraciones más útiles.

Figura 2.14 *Configuración de almacenamiento*

En la pantalla de Almacenamiento (Figura 2.14 , " Configuración de almacenamiento " [página 33]), debe asociar el Kali
Imagen ISO de Linux con el lector virtual de CD / DVD-ROM. Primero, seleccione la unidad de CD-ROM en Stor-
Lista de árbol de edad y luego haga clic en el pequeño icono de CD-ROM a la derecha para mostrar un menú contextual
donde puede elegir el archivo de disco óptico virtual ...

Figura 2.15 *Configuración del sistema: placa base*

IntheSystemscreen (Figura 2.15 , “ Configuración del sistema: placa base "[Página34]), usted encontrará a Polilla-pestaña del tablero Asegúrese de que el orden de inicio indica que el sistema primero intentará iniciar desde cualquier dispositivo óptico antes de probar un disco duro. Esta es también la pestaña donde puede modificar la cantidad de memoria asignada a la máquina virtual, si surge la necesidad.

Figura 2.16 *Configuración del sistema: procesador*

En la misma pantalla pero en la pestaña "Procesador" (Figura 2.16 , " Configuración del sistema: procesador "[página 35]), puede ajustar el número de procesadores asignados a la máquina virtual. Más importante, si usa una imagen de 32 bits, habilite PAE / NX o la imagen de Kali no se iniciará desde el núcleo predeterminado La variante utilizada por Kali para i386 (acertadamente llamada "686-pae") se compila de una manera que requiere física Soporte de extensión de dirección (PAE) en la CPU.

Hay muchos otros parámetros que se pueden configurar, como la configuración de la red (que define cómo se maneja el tráfico en la tarjeta de red), pero los cambios anteriores son suficientes para poder arrancar
Un sistema en vivo Kali Linux en funcionamiento. Finalmente, haga clic en Arrancar y la VM debería arrancar correctamente, como se muestra en Figura 2.17 , "Pantalla de arranque de Kali Linux en VirtualBox "[página 36]. Si no, revise cuidadosamente todas las configuraciones e intenta de nuevo.

Figura 2.17 *Pantalla de arranque de Kali Linux en VirtualBox*

VMware

VMware Workstation Pro es muy similar a *VirtualBox* en términos de características e interfaz de usuario, ya que porque ambos están diseñados principalmente para uso de escritorio, pero el proceso de configuración para un nuevo virtual La máquina es un poco diferente.

Figura 2.18 *Pantalla de inicio de VMware*

La pantalla inicial, que se muestra en la Figura 2.18, “ Pantalla de inicio de VMware ” [página 37], muestra un gran Crear un Nuevo botón de máquina virtual que inicia un asistente para guiarlo a través de la creación de su virtual máquina.

Figura 2.19 *Asistente de máquina virtual nueva*

En el primer paso, debe decidir si desea que se le presenten configuraciones avanzadas durante ing el proceso de configuración. En este ejemplo, no hay requisitos especiales, así que elija el típico instalación, como se muestra en la Figura 2.19, " Nuevo asistente de máquina virtual”[Página 37].

Figura 2.20 *Instalación del sistema operativo invitado*

El asistente asume que desea instalar el sistema operativo de inmediato y le pide que lo haga. seleccione la imagen ISO que contiene el programa de instalación (Figura 2.20, " Sistema operativo invitado Instalación ”[página 38]). Seleccione "Archivo de imagen de disco del instalador (iso)" y haga clic en Examinar para seleccionar el archivo de imagen.

Figura 2.21 *Seleccione un sistema operativo invitado*

Cuando el sistema operativo (SO) no se puede detectar desde la imagen ISO seleccionada, el asistente pregunta qué tipo de sistema operativo invitado desea ejecutar. Debe seleccionar "Linux" para el sistema operativo y "Debian 8.x" para la versión, como se muestra en la Figura 2.21 , “ Seleccione un sistema operativo invitado ” [página 38].

Figura 2.22 *Nombre de la máquina virtual*

Elija "Kali Linux" como nombre de la nueva máquina virtual (Figura 2.22, " Nombra el Virtual Malomo "[página 39]). Como con Virtual Box, usted también tiene la opción de guardar los archivos VM alternativos ubicación.

Figura 2.23 *Especifique la capacidad del disco*

El tamaño predeterminado del disco duro de 20 GB (Figura 2.23 , “ Especificar la capacidad del disco ” [página 40]) suele ser suficiente ingenioso, pero puede ajustarlo aquí según sus necesidades esperadas. A diferencia de VirtualBox, que puede usar un solo archivo de diferentes tamaños, VMware tiene la capacidad de almacenar el contenido del disco Múltiples archivos. En ambos casos, el objetivo es conservar el espacio en disco del host.

Figura 2.24 *Listo para crear una máquina virtual*

VMware Workstation ahora está configurado para crear la nueva máquina virtual. Muestra un resumen.
de las elecciones realizadas para que pueda verificar todo antes de crear la máquina. aviso
que el asistente optó por asignar solo 512 MB de RAM a la máquina virtual, lo cual no es suficiente
así que haga clic en Personalizar hardware ... (Figura 2.24 , “ Listo para crear una máquina virtual ” [página 41]) y
modifique la configuración de Memoria, como se muestra en la Figura 2.25 , " Configurar ventana de hardware”[Página 42].

Figura 2.25 *Ventana Configurar hardware*

Después de un último clic en Finalizar (Figura 2.24 , “ Listo para crear máquina virtual "[Página 41]), lo virtual
la máquina ahora está configurada y se puede iniciar haciendo clic en "Encender esta máquina virtual" como
se muestra en la figura 2.26 , “ Kali Linux Virtual Machine Ready ”[Página 43].

Figura 2.26 *Listo para máquina virtual Kali Linux*

2.3. Resumen

En este capítulo, aprendió sobre las diversas imágenes ISO de Kali Linux, aprendió a verificar y descárguelos y aprendió cómo crear discos USB de arranque a partir de ellos en varios sistemas operativos sistemas. También discutimos cómo arrancar los discos USB y revisamos cómo configurar el BIOS y la configuración de inicio en varias plataformas de hardware para que los discos USB se inicien.

Consejos resumidos:

- www.kali.org es el único sitio oficial de descarga de Kali ISO. No los descargue de cualquier otro sitio, porque esas descargas pueden contener malware.
- Siempre valide el sha256sum de sus descargas con el comando `sha256sum` para garantizar La integridad de su descarga ISO. Si no coincide, intente la descarga nuevamente o use un fuente diferente
- Debe escribir la imagen ISO de Kali Linux en un medio de arranque si desea iniciarla en un maquina física. Use *Win32 Disk Imager* en Windows, la utilidad Disks en Linux o `dd` comando en Mac OS X / macOS. Tenga mucho *cuidado* al escribir la imagen. Seleccionar el mal el disco podría dañar permanentemente los datos en su máquina.
- Configure las pantallas de configuración de BIOS / UEFI en una PC o mantenga presionada la tecla Opción en OS X / macOS para permita que la máquina arranque desde la unidad USB.

- Los programas de máquinas virtuales como *VirtualBox* y *VMware Workstation Pro* son especialmente útiles si quieres probar Kali Linux pero no estás listo para comprometerte a instalarlo permanentemente en su máquina o si tiene un sistema potente y desea ejecutar múltiples sistemas operativos simultaneamente.

Ahora que tiene una instalación funcional de Kali Linux, es hora de profundizar en algunas funciones de Linux. datos básicos necesarios para el funcionamiento básico y avanzado de Kali. Si eres de moderado a usuario avanzado de Linux, considere hojear el próximo capítulo.

Palabras clave

Kernel de Linux
Espacio de usuario
Línea de comando
golpetazo
Jerarquía del sistema de archivos
Comandos de Unix

Capítulo

Fundamentos de Linux 3

Contenido

¿Qué es Linux y qué está haciendo? 48
La línea de comando 51
El sistema de archivos 54
Comandos útiles 56
Resumen 62

Antes de que pueda dominar Kali Linux, debe estar cómodo con un sistema Linux genérico. Linux profi-
ciency le servirá bien, porque un gran porcentaje de servicios web, de correo electrónico y otros servicios de Internet
ejecutar en servidores Linux.

En esta sección, nos esforzamos por cubrir los conceptos básicos de Linux, pero asumimos que ya sabe acerca de
sistemas informáticos en general, incluidos componentes como la CPU, RAM, placa base y
disco duro, así como los controladores de dispositivos y sus conectores asociados.

3.1. ¿Qué es Linux y qué está haciendo?

El término "Linux" se usa a menudo para referirse a todo el sistema operativo, pero en realidad, Linux es
el núcleo del sistema operativo, que se inicia mediante el gestor de arranque, que a su vez se inicia mediante
BIOS / UEFI. El núcleo asume una función similar a la de un director de orquesta: garantiza
coordinación entre hardware y software. Este rol incluye la gestión de hardware, procesos,
usuarios, permisos y el sistema de archivos. El núcleo proporciona una base común para todos los demás programas.
en el sistema y normalmente se ejecuta en *anillo cero* , también conocido como *espacio del kernel* .

El espacio de usuario Utilizamos el término *espacio de usuario* para agrupar todo lo que sucede fuera del
núcleo.

Entre los programas que se ejecutan en el espacio de usuario hay muchas utilidades principales de GNU
proyecto ↓ , la mayoría de los cuales están destinados a ejecutarse desde la línea de comandos. Puedes usar
ellos en scripts para automatizar muchas tareas. Consulte la sección 3.4 , " Comandos útiles "

[página 56] para obtener más información sobre los comandos más importantes.

Repasemos rápidamente las diversas tareas manejadas por el kernel de Linux.

3.1.1. Hardware de conducción

El núcleo tiene la tarea, en primer lugar, de controlar los componentes de hardware de la computadora.
Los detecta y configura cuando la computadora se enciende, o cuando se inserta o vuelve a conectar un dispositivo
movido (por ejemplo, un dispositivo USB). También los pone a disposición de software de nivel superior, a través de
Una interfaz de programación simplificada, por lo que las aplicaciones pueden aprovechar los dispositivos sin tener
para abordar detalles como en qué ranura de extensión está conectada una placa opcional. La programación
la interfaz también proporciona una capa de abstracción; esto permite el software de videoconferencia, para examen
ple, usar una cámara web independientemente de su fabricante y modelo. El software puede usar el *Video para Linux*
(V4L) y el kernel traducirán las llamadas de función de la interfaz al hardware real
comandos necesarios para la cámara web específica en uso.

El núcleo exporta datos sobre el hardware detectado a través de `/proc/` y `/sys/` virtual file sys-
Tems. Las aplicaciones a menudo acceden a los dispositivos mediante archivos creados dentro de `/dev/`. Rep. Archivos específicos

[1] http://www.gnu.org

reenviar unidades de disco (por ejemplo, `/dev/sda`), particiones (`/dev/sda1`), ratones (`/dev/input/mouse0`),
teclados (`/dev/input/event0`), tarjetas de sonido (`/dev/snd/*`), puertos serie (`/dev/ttyS*`) y otros
componentes.

Hay dos tipos de archivos de dispositivo: *bloque* y *personaje*. El primero tiene características de un bloque de
datos: tiene un tamaño finito y puede acceder a bytes en cualquier posición del bloque. Este último se comporta
como un flujo de caracteres. Puede leer y escribir caracteres, pero no puede buscar una posición
y cambiar bytes arbitrarios. Para averiguar el tipo de un archivo de dispositivo dado, inspeccione la primera letra en
la salida de `ls -l`. Es b, para dispositivos de bloque, o c, para dispositivos de caracteres:

```
$ ls -l / dev / sda / dev / ttyS0
brw-rw ---- 1 disco raíz 8, 0 mar 21 08:44 / dev / sda
crw-rw ---- 1 marcación raíz 4, 64 mar 30 08:59 / dev / ttyS0
```

Como es de esperar, las unidades de disco y las particiones usan dispositivos de bloque, mientras que el mouse, el teclado y
los puertos seriales usan dispositivos de caracteres. En ambos casos, la interfaz de programación incluye dispositivo-
comandos específicos que se pueden invocar a través de la *llamada al* sistema *ioctl*.

3.1.2. Sistemas de archivos unificadores

Los sistemas de archivos son un aspecto destacado del núcleo. Los sistemas tipo Unix fusionan todos los almacenes de archivos en un
jerarquía única, que permite que los usuarios y las aplicaciones accedan a los datos al conocer su ubicación dentro de
esa jerarquía

El punto de partida de este árbol jerárquico se denomina raíz, representado por el carácter "`/`".
Este directorio puede contener subdirectorios con nombre. Por ejemplo, el subdirectorio de hogares de `/se` llama
`/inicio/`. Este subdirectorio puede, inturn, contener otros subdirectorios, y pronto. Cada directorio puede
También contienen archivos, donde se almacenarán los datos. Por lo tanto, `/home/buxy/Desktop/hello.txt se` refiere
a un archivo llamado hello.txt almacenado en el subdirectorio Desktop del subdirectorio buxy de la página de inicio
directorio, presente en la raíz. El núcleo se traduce entre este sistema de nombres y el almacenamiento.
ubicación en un disco.

A diferencia de otros sistemas, Linux posee una sola jerarquía, y puede integrar datos de
Varios discos. Uno de estos discos se convierte en la raíz, y los otros se *montan* en directorios en
la jerarquía (el comando de Linux se llama `mount`). Estos otros discos están disponibles en
Los *puntos de montaje*. Esto permite almacenar los directorios de inicio de los usuarios (tradicionalmente almacenados en `/home/`)
en un disco duro separado, que contendrá el directorio buxy (junto con los directorios principales de
otros usuarios) Una vez que monte el disco en `/home/`, estos directorios serán accesibles en su
ubicaciones habituales y rutas como `/home/buxy/Desktop/hello.txt` siguen funcionando.

Hay muchos formatos de sistema de archivos, correspondientes a muchas formas de almacenar físicamente datos en
discos Los más conocidos son *ext2*, *ext3* y *ext4*, pero existen otros. Por ejemplo, *VFAT* es el
sistema de archivos utilizado históricamente por los sistemas operativos DOS y Windows. Soporte de Linux para
VFAT permite que los discos duros sean accesibles bajo Kaliaswellas bajo Windows. En cualquier caso, debes
prepare un sistema de archivos en un disco antes de poder montarlo y esta operación se conoce como *formateo*.

Los comandos como mkfs.ext3 (donde mkfs significa *MaKe FileSystem*) manejan el formato. Estas los comandos requieren, como parámetro, un archivo de dispositivo que represente la partición a formatear (para instancia, / dev / sda1 , la primera partición en la primera unidad). Esta operación es destructiva y debe se ejecute solo una vez, a menos que desee borrar un sistema de archivos y comenzar de nuevo.

También hay sistemas de archivos de red como NFS, que no almacenan datos en un disco local. En lugar, los datos se transmiten a través de la red a un servidor que los almacena y los recupera a pedido. Gracias a la abstracción del sistema de archivos, no tiene que preocuparse por cómo está conectado este disco, ya que los archivos permanecen accesibles en su forma jerárquica habitual.

3.1.3. Gestionando Procesos

Un proceso es una instancia en ejecución de un programa, que requiere memoria para almacenar tanto el programa en sí mismo y sus datos operativos. El núcleo se encarga de crear y rastrear procesos. Cuando se ejecuta un programa, el kernel primero reserva algo de memoria, carga el código ejecutable del archivo sistema en él, y luego comienza a ejecutar el código. Mantiene información sobre este proceso, la mayoría visible de los cuales es un número de identificación conocido como el *identificador de proceso* (PID).

Como la mayoría de los sistemas operativos modernos, aquellos con núcleos similares a Unix, incluido Linux, son capaces de multitarea. En otras palabras, permiten que el sistema ejecute muchos procesos al mismo tiempo. En realidad, solo hay un proceso en ejecución a la vez, pero el núcleo divide el tiempo de CPU en pequeños trozos y ejecuciones cada proceso durante la vuelta. Dado que los tiempos pasados son muy cortos (en milisegundos rango), crean la apariencia de procesos que se ejecutan en paralelo, aunque solo están activos durante su intervalo de tiempo e inactivo el resto del tiempo. El trabajo del núcleo es ajustar su programación mecanismos para mantener esa apariencia, mientras se maximiza el rendimiento del sistema global. Si el tiempo los cortes son demasiado largos, la aplicación puede no parecer tan receptiva como se desea. Demasiado corto, y el el sistema pierde tiempo al cambiar de tarea con demasiada frecuencia. Estas decisiones se pueden refinar con el proceso prioridades, donde los procesos de alta prioridad se ejecutarán durante períodos más largos y con un tiempo más frecuente rebanadas que los procesos de baja prioridad.

Sistemas multiprocesador (y variantes)

La limitación descrita anteriormente, de solo un proceso ejecutándose a la vez, no siempre aplicar: la restricción real es que solo puede haber un proceso en ejecución *por pro-núcleo del evaluador* . Los sistemas multiprocesador, multinúcleo o *hiperprocesador* permiten varios procesos para ejecutarse en paralelo. Sin embargo, se utiliza el mismo sistema de división de tiempo para manejar casos donde hay más procesos activos que los núcleos de procesador disponibles. Esto no es inusual: un sistema básico, incluso en su mayoría inactivo, casi siempre tiene decenas de funcionamiento procesos.

El núcleo permite que se ejecuten varias instancias independientes del mismo programa, pero cada una está permitida para acceder solo a sus propios segmentos de tiempo y memoria. Sus datos permanecen así independientes.

3.1.4. Gestión de Derechos

Los sistemas tipo Unix admiten múltiples usuarios y grupos y permiten el control de permisos. La mayoría de En ese momento, el usuario que lo inició identifica un proceso. Ese proceso solo está permitido tomar acciones permitidas para su propietario. Por ejemplo, abrir un archivo requiere que el núcleo verifique la identidad del proceso contra los permisos de acceso (para obtener más detalles sobre este ejemplo en particular, consulte sección 3.4.4 , " Gestión de derechos"[Página 57]).

3.2. La línea de comando

Por "línea de comando", nos referimos a una interfaz basada en texto que le permite ingresar comandos, ejecutar ellos, y ver los resultados. Puede ejecutar un terminal (una pantalla de texto dentro del escritorio gráfico, o la consola de texto en sí fuera de cualquier interfaz gráfica) y un intérprete de comandos dentro de ella (*El caparazón*).

3.2.1. Cómo obtener una línea de comando

Cuando su sistema funciona correctamente, la forma más fácil de acceder a la línea de comando es ejecutar un terminal en su sesión de escritorio gráfico.

Figura 3.1 *Inicio del terminal GNOME*

Por ejemplo, en un sistema Kali Linux predeterminado, GNOME Terminal se puede iniciar desde la lista de aplicaciones vorite. También puede escribir "terminal" mientras está en la pantalla de Actividades (la que obtiene se activa cuando mueve el mouse a la esquina superior izquierda) y hace clic en la aplicación correcta icono que aparece (Figura 3.1 , " Inicio del terminal GNOME " [página 51]).

En el caso de que su interfaz gráfica esté rota, aún puede obtener una línea de comando en virtual consolas (se puede acceder a hasta seis de ellas a través de las seis combinaciones de teclas de CTRL + ALT + F1 a través de CTRL + ALT + F6: la tecla CTRL se puede omitir si ya está en modo de texto, fuera de Xorg o la interfaz gráfica de Wayland). Obtiene una pantalla de inicio de sesión muy básica donde ingresa su inicio de sesión y contraseña antes de obtener acceso a la línea de comando con su shell:

```
Kali GNU / Linux Rolling kali-rolling tty3
inicio de sesión kali-rolling: root
Contraseña:
Último inicio de sesión: Fir Mar 25 12:30:05 EDT 2016 de 192.168.122.1 en pts / 2
Linux kali-rolling 4.4.0-kali1-amd4 # 1 SMP Debian 4.4.6-1kali1 (2016-03-18) x86_64

Los programas incluidos con el sistema Kali GNU / Linux son software libre;
los términos de distribución exactos para cada programa se describen en el
archivos individuales en / usr / share / doc / * / copyright.

Kali GNU / Linux viene ABSOLUTAMENTE SIN GARANTÍA, en la medida
permitido por la ley aplicable.
root @ kali-rolling: ~ #
```

El programa que maneja su entrada y ejecuta sus comandos se llama *shell* (o un comando-intérprete de línea). El shell predeterminado proporcionado en Kali Linux es *Bash* (significa *Bourne Again SHell*). El carácter "$" o "#" final indica que el shell está esperando su entrada. También indica si Bash te reconoce como un usuario normal (el primer caso con el dólar) o como un superusuario (el último caso con el hash).

3.2.2. Conceptos básicos de la línea de comandos: exploración del árbol de directorios y administración de archivos

Esta sección solo proporciona una breve descripción de los comandos cubiertos, todos los cuales tienen muchos opciones no descritas aquí, por lo tanto, consulte la abundante documentación disponible en su informe páginas de manual espectrales. En las pruebas de penetración, con mayor frecuencia recibirá acceso de shell a un sistema después de una explotación exitosa, en lugar de una interfaz gráfica de usuario. Competencia con el comando La línea es esencial para su éxito como profesional de seguridad.

Una vez que se abre una sesión, el comando `pwd` (que significa *directorio de trabajo de impresión*) muestra su ubicación actual en el sistema de archivos. El directorio actual se cambia con el *directorio de* CD Com mand (`cd` es para *cambiar el directorio*). Cuando no especifica el directorio de destino, lo llevan a su directorio de inicio Cuando usa `cd -` , regresa al antiguo directorio de trabajo (el

en uso antes de la última llamada de CD). El directorio padre siempre se llama .. (dos puntos), mientras que el

Página 79

El directorio actual también se conoce como. (un punto). El comando ls permite *enumerar* el contenido de un directorio. Si no proporciona parámetros, ls opera en el directorio actual.

$ **pwd**
/ inicio / buxy
$ **cd Desktop**
$ **pwd**
/ home / buxy / Desktop
$ **cd.**
$ **pwd**
/ home / buxy / Desktop
$ **cd ..**
$ **pwd**
/ inicio / buxy
$ **ls**
Escritorio Descarga plantillas de imágenes
Documentos de música Público Videos

Se puede crear un nuevo directorio con mkdir *directorio* , y quitar un directorio existente (vacío) con el *directorio* rmdir . El comando mv permite *mover* y renombrar archivos y directorios; *re-mover* un archivo se logra con el *archivo* rm , y copiar un archivo se realiza con cp *source-file target-archivo* .

prueba de $ **mkdir**
$ **ls**
Escritorio Descargas Imágenes Plantillas Videos
Documentos de música Público prueba
$ **mv prueba nueva**
$ **ls**
Escritorio Descargas nuevas Público Videos
Documentos de música Plantillas de imágenes
$ **rmdir nuevo**
$ **ls**
Escritorio Descargas Imágenes Plantillas Videos
Documentos de música Público

El shell ejecuta cada comando ejecutando el primer programa del nombre dado que encuentra en un directorio listado en la variable de entorno PATH. Muy a menudo, estos programas están en / bin , / sbin , / usr / bin o / usr / sbin . Por ejemplo, el comando ls se encuentra en / bin / ls ; el cual
El comando informa la ubicación de un ejecutable dado. Algunas veces el comando se maneja directamente por el shell, en cuyo caso, se llama un comando incorporado del shell (cd y pwd se encuentran entre esos); la
El comando type le permite consultar el tipo de cada comando.

$ **echo $ PATH**
/ usr / local / sbin: / usr / local / bin: / usr / sbin: / usr / bin: / sbin: / bin
$ **que es**
/ bin / ls

80

$ **type rm**
rm es / bin / rm
$ **tipo cd**
cd es un shell incorporado

Tenga en cuenta el uso del comando echo , que simplemente muestra una cadena en el terminal. En este caso, se utiliza para imprimir el contenido de las variables de un ambiente en el mismo lugar que sustituye automáticamente variables con sus valores antes de ejecutar la línea de comando.

Variables de entorno Las variables de entorno permiten el almacenamiento de configuraciones globales para el shell u otros programas Son contextuales pero heredables. Por ejemplo, cada proceso tiene su propio conjunto de variables de entorno (son contextuales). Los shells, como los shells de inicio de sesión, pueden declarar variables, que se transmitirán a otros programas que ejecuten (ellos son heredables)

Estas variables se pueden definir en todo el sistema en / etc / profile o por usuario en ~ /

.perfil pero las variables que no son específicas de los intérpretes de línea de comandos son mejores
poner en / etc / environment , ya que esas variables se inyectarán en todas las sesiones de usuario
gracias a un Módulo de autenticación enchufable (PAM), incluso cuando no se ejecuta ningún shell.

3.3. El sistema de archivos

3.3.1 El estándar de jerarquía del sistema de archivos

Al igual que con otras distribuciones de Linux, Kali Linux está organizado para ser coherente con el *sistema de archivos Hi-Erarchy Standard* (FHS), que permite a los usuarios de otras distribuciones de Linux encontrar su camino fácilmente Kali El FHS define el propósito de cada directorio. Los directorios de nivel superior se describen como sigue.

- / bin / : programas básicos
- / boot / : kernel de Kali Linux y otros archivos necesarios para su proceso de arranque temprano
- / dev / : archivos del dispositivo
- / etc / : archivos de configuración
- / home / : archivos personales del usuario
- / lib / : bibliotecas básicas
- / media / * : puntos de montaje para dispositivos extraíbles (CD-ROM, llaves USB, etc.)
- / mnt / : punto de montaje temporal
- / opt / : aplicaciones adicionales proporcionadas por terceros
- / root / : archivos personales del administrador (root)

- / run / : datos de tiempo de ejecución volátiles que no persisten en los reinicios (aún no se incluyen en el FHS)
- / sbin / : programas del sistema
- / srv / : datos utilizados por los servidores alojados en este sistema
- / tmp / : archivos temporales (este directorio a menudo se vacía en el arranque)
- / usr / : aplicaciones (este directorio se subdivide en bin , sbin , lib de acuerdo con la misma lógica que en el directorio raíz) Además, / usr / share / contiene arquitectura-Datos independientes. El directorio / usr / local / debe ser utilizado por el administrador para Instalar aplicaciones manualmente sin sobrescribir archivos manejados por el sistema de empaque (dpkg)
- / var / : variabledatahandledbydaemons. Esto incluye archivos de registro, colas, spools y cachés.
- / proc / y / sys / son específicos del kernel de Linux (y no forman parte del FHS). Son usados por el núcleo para exportar datos al espacio de usuario.

3.3.2. El directorio de inicio del usuario

El contenido del directorio de inicio de un usuario no está estandarizado, pero todavía hay algunos notables convenciones Una es que el directorio de inicio de un usuario a menudo se denomina tilde ("~"). Eso es util saber porque los intérpretes de comandos reemplazan automáticamente una tilde con el directorio correcto (que se almacena en la variable de entorno HOME, y cuyo valor habitual es / home / *user* /).

Tradicionalmente, los archivos de configuración de la aplicación a menudo se almacenan directamente en su directorio de inicio, pero los nombres de los archivos generalmente comienzan con un punto (por ejemplo, el cliente de correo electrónico mutt almacena su configuración) ción en ~ / .muttrc). Tenga en cuenta que los nombres de archivo que comienzan con un punto están ocultos de manera predeterminada; el ls com mand solo los enumera cuando se usa la opción -a y los administradores de archivos gráficos deben ser explícitamente configurado para mostrar archivos ocultos.

Algunos programas también usan múltiples archivos de configuración organizados en un directorio (por ejemplo, ~ / .ssh /). Algunas aplicaciones (como el navegador web Firefox) también usan su directorio para almacenar un caché de datos descargados. Esto significa que esos directorios pueden terminar consumiendo mucho disco espacio.

Estos archivos de configuración se almacenan directamente en su directorio de inicio, a menudo denominados colectivamente *Los archivos de puntos* , han proliferado durante mucho tiempo hasta el punto de que estos directorios pueden estar bastante llenos de ellos. Afortunadamente, un esfuerzo dirigido colectivamente bajo el paraguas de FreeDesktop.org ha resultado en el XDG BaseDirectorySpecification, una convención que pretende limpiar estos archivos y directorios. Esta la especificación establece que los archivos de configuración deben almacenarse en ~ / .config , los archivos de caché en

~ / .cache , y los archivos de datos de la aplicación en ~ / .local (o sus subdirectorios). Esta convención
Está ganando lentamente tracción.

Los escritorios gráficos generalmente tienen accesos directos para mostrar el contenido del directorio ~ / Desktop / (o
cualquiera que sea la traducción apropiada para sistemas no configurados en inglés).

Finalmente, el sistema de correo electrónico a veces almacena correos electrónicos entrantes en un directorio ~ / Mail / .

3.4. Comandos útiles

3.4.1. Mostrar y modificar archivos de texto

El comando de *archivo* cat (destinado a *concatenar* archivos al dispositivo de salida estándar) lee un archivo
y muestra su contenido en el terminal. Si el archivo es demasiado grande para caber en una pantalla, puede usar un localizador
como menos (o más) para mostrarlo página por página.

El comando editor inicia un editor de texto (como Vi o Nano) y permite crear, modificar y
leyendo archivos de texto. Los archivos más simples a veces se pueden crear directamente desde el comando inter-
preter gracias a la redirección: *comando > archivo* crea un archivo llamado *archivo que* contiene la salida del
comando dado *el archivo de comando >>* es similar, excepto que agrega la salida del comando a
el archivo en lugar de sobrescribirlo.

```
$ echo "Kali gobierna!" > kali-rules.txt
$ gato kali-rules.txt
Kali gobierna!
$ echo "Kali es el mejor!" >> kali-rules.txt
$ gato kali-rules.txt
Kali gobierna!
Kali es el mejor!
```

3.4.2. Búsqueda de archivos y dentro de archivos

Las hallazgo *criterios de directorio* comando búsquedas de archivos en la jerarquía bajo el *directorio de* AC-
de acuerdo con varios criterios. El criterio más utilizado es -name *filename* , que permite
buscando un archivo por nombre. También puede usar comodines comunes como "*" en el nombre del archivo
buscar.

```
$ find / etc -name hosts
/ etc / hosts
/ etc / avahi / hosts
$ find / etc -name "hosts *"
/ etc / hosts
/etc/hosts.allow
/etc/hosts.deny
/ etc / avahi / hosts
```

El comando de *archivos de expresión* grep busca el contenido de los archivos y extrae líneas
coincidiendo con la expresión regular. Agregar la opción -r permite una búsqueda recursiva en todos los archivos
contenido en el directorio Esto le permite buscar un archivo cuando solo conoce una parte de su contenido.

3.4.3. Gestionando Procesos

La lista de comandos ps aux procesa los procesos que se ejecutan actualmente y ayuda a identificar el funcionamiento del equipo.
su *PID.* Una vez que conoce el *PID de un* proceso, el comando *pid de señal de* muerte permite que finalice
es una señal (si se detiene el proceso). Varias señales sexistas; mostcommonlyusedareTERM (arequest
terminar con gracia) y MATAR (una muerte forzada).

El intérprete de comandos también puede ejecutar programas en segundo plano si se sigue el comando
por "&". Al usar el signo "y", retoma el control del shell inmediatamente aunque
El comando aún se está ejecutando (oculto a la vista como un proceso en segundo plano). Las listas de comandos de trabajos
los procesos que se ejecutan en segundo plano; ejecutar fg% *job-number* (para *primer plano*) restaura un

trabajo al primer plano. Cuando se ejecuta un comando en primer plano (ya sea porque era comenzó normalmente, o regresó al primer plano con fg), la combinación de teclas Control + Z pausa el proceso y reanuda el control de la línea de comando. El proceso se puede reiniciar. en segundo plano con bg% *número de trabajo* (para *fondo*).

3.4.4 Gestión de derechos

Linux es un sistema multiusuario, por lo que es necesario proporcionar un sistema de permisos para controlar el conjunto de autorizar la operación en archivos y directorios, que incluye todos los recursos y dispositivos del sistema (en un sistema Unix, cualquier dispositivo está representado por un archivo o directorio). Este principio es común a todos los sistemas tipo Unix.

Cada archivo o directorio tiene permisos específicos para tres categorías de usuarios:

- Su propietario (simbolizado por usted, como en el usuario)
- Su grupo propietario (simbolizado por g, como en el grupo), que representa a todos los miembros del grupo.
- Los otros (simbolizados por o, como en otro)

Se pueden combinar tres tipos de derechos:

- lectura (simbolizada por r, como en lectura);
- escritura (o modificación, simbolizada por w, como en escritura);
- ejecución (simbolizado por x, como en eXecute).

En el caso de un archivo, estos derechos se entienden fácilmente: el acceso de lectura permite leer el contenido (incluida la copia), el acceso de escritura permite cambiarlo y el acceso de ejecución permite ejecutarlo (que solo funcionará si es un programa).

setuid y setgid ejecutables

Dos derechos particulares son relevantes para los archivos ejecutables: setuid y setgid (simbolizado con la letra "s"). Tenga en cuenta que con frecuencia hablamos de bit, ya que cada uno de estos booleanos los valores se pueden representar con un 0 o un 1. Estos dos derechos permiten a cualquier usuario ejecutar El programa con los derechos del propietario o del grupo, respectivamente. Este mecanismo Otorga acceso a funciones que requieren permisos de nivel superior a los que tendría usualmente tengo.

Dado que un programa raíz setuid se ejecuta sistemáticamente bajo la identidad de superusuario, es Muy importante para garantizar que sea seguro y confiable. Cualquier usuario que logre subvertir un programa raíz setuid para llamar a un comando de su elección podría suplantar el usuario root y tiene todos los derechos sobre el sistema. Los probadores de penetración buscan regularmente estos tipos de archivos cuando obtienen acceso a un sistema como una forma de aumentar su privilegios

Un directorio se maneja de manera diferente a un archivo. El acceso de lectura da derecho a consultar la lista de sus contenidos (archivos y directorios); el acceso de escritura permite crear o eliminar archivos; y ejecutar el acceso permite cruzar el directorio para acceder a su contenido (por ejemplo, con el comando cd). Poder cruzar un directorio sin poder leerlo le da al usuario permiso para acceder a las entradas que se conocen por su nombre, pero no encontrarlas sin conocer su nombre exacto.

SEGURIDAD

directorio setgid y *adhesivo*

poco

El bit setgid también se aplica a los directorios. Cualquier elemento recién creado en dichos directorios se le asigna automáticamente el grupo propietario del directorio principal, en lugar de heredar ing el grupo principal del creador como de costumbre. Debido a esto, no tiene que cambiar su grupo principal (con el comando newgrp) cuando se trabaja en un árbol de archivos compartido entre varios usuarios del mismo grupo dedicado.

El *bit adhesivo* (simbolizado por la letra "t") es un permiso que solo es útil en directorios. Se utiliza especialmente para directorios temporales donde todos escriben acceso (como / tmp /): restringe la eliminación de archivos para que solo su propietario o el El propietario del directorio principal puede eliminarlos. Al carecer de esto, todos podrían eliminar archivos de otros usuarios en / tmp / .

Tres comandos controlan los permisos asociados con un archivo:

- *el archivo de usuario* chown cambia el propietario del archivo

PROPINAConfrecuencia, desea cambiar el grupo de un archivo al mismo tiempo que

Cambiar el usuario y grupo cambiar el dueño El comando chown tiene una sintaxis especial para eso: chown *usuario* : *archivo de grupo*

- El *archivo de grupo* chgrp altera el grupo propietario
- *archivo de derechos* chmod cambia los permisos para el archivo

Hay dos formas de representar los derechos. Entre ellos, la representación simbólica es probablemente El más fácil de entender y recordar. Involucra los símbolos de letras mencionados anteriormente. usted puede definir derechos para cada categoría de usuarios (u / g / o), configurándolos explícitamente (con =), agregando

(+), o restando (-). Por lo tanto, u = rwx, g + rw o fórmula le da al propietario lectura, escritura y ejecución derechos, agrega derechos de lectura y escritura para el grupo de propietarios y elimina los derechos de lectura para otros usuarios. Los derechos no alterados por la suma o resta en dicho comando no se modifican. los la letra a, para todos, cubre las tres categorías de usuarios, de modo que a = rx otorga a las tres categorías mismos derechos (leer y ejecutar, pero no escribir).

La representación numérica (octal) asocia cada derecho con un valor: 4 para lectura, 2 para escritura y 1 para ejecutar. Asociamos cada combinación de derechos con la suma de las tres figuras, y un El valor se asigna a cada categoría de usuarios, en el orden habitual (propietario, grupo, otros).

Por ejemplo, el comando de *archivo* chmod 754 establecerá los siguientes derechos: leer, escribir y ejecutar para el propietario (ya que 7 = 4 + 2 + 1); leer y ejecutar para el grupo (ya que 5 = 4 + 1); solo lectura para otros. El medio significa noches; así, el *archivo* chmod 600 permite permisos de escritura y escritura para el propietario, y noches para todos. La mayoría de las combinaciones más rectas son 755 por ejecutables archivos y directorios, y 644 para archivos de datos.

Para representar derechos especiales, puede prefijar un cuarto dígito a este número de acuerdo con el mismo principio, donde los bits setuid, setgid y sticky son 4, 2 y 1, respectivamente. El comando chmod 4754 asociará el bit setuid con los derechos descritos anteriormente.

Tenga en cuenta que el uso de la notación octal solo le permite establecer todos los derechos a la vez en un archivo; no se puede úselo para agregar un nuevo derecho, tal como acceso para el propietario del grupo, ya que debe tener en cuenta los derechos existentes y computar el nuevo valor numérico correspondiente.

La representación octal también se usa con el comando umask , que se usa para restringir permisos sions en archivos recién creados. Cuando una aplicación crea un archivo, asigna permisos indicativos, sabiendo que el sistema elimina automáticamente los derechos definidos con umask . Ingrese a umask en un cáscara; verá una máscara como 0022 . Esto es simplemente una representación octal de los derechos a ser eliminado sistemáticamente (en este caso, los derechos de escritura para el grupo y otros usuarios).

Si le da un nuevo valor octal, el comando umask modifica la máscara. Utilizado en un shell inicial ization file (por ejemplo, ~ / .bash_profile), cambiará efectivamente la máscara predeterminada para su sesiones de trabajo

Operación recursiva PROPINA A veces tenemos que cambiar los derechos de un árbol de archivos completo. Todos los comandos anteriores tener una opción -R para operar recursivamente en subdirectorios.

La distinción entre directorios y archivos a veces causa problemas con la repetición operaciones sive. Es por eso que la letra "X" se ha introducido en la representación simbólica. presentación de derechos. Representa un derecho de ejecución que se aplica solo a directorios (y no a los archivos que carecen de este derecho). Por lo tanto, el *directorio* chmod -R a + X solo agregará ejecutar derechos para todas las categorías de usuarios (a) para todos los subdirectorios y archivos para que al menos una categoría de usuario (incluso si su único propietario) ya ha ejecutado derechos.

3.4.5. Obtener información del sistema y registros

El comando libre muestra información en la memoria; informes de *disco libre* (df) sobre el disco disponible espacio en cada uno de los discos montados en el sistema de archivos. Su opción -h (para *lectura humana*) convierte los tamaños en una unidad más legible (generalmente mebibytes o gibibytes). De manera similar, el libre El comando admite las opciones -m y -g, y muestra sus datos en mebibytes o en gibibytes, respectivamente.

```
$ gratis
                total        usado       gratis     beneficio compartido / caché   disponible
Mem:          2052944       661232       621208       10520       770504      1359916
Intercambiar:       0 0          0 0          0 0
$ df
Sistema de archivos     Bloques de 1K  Usado Disponible Uso% Montado en
udev                      1014584       0 0   1014584   0% / dev
tmpfs                      205296      8940    196356   5% / corrida
/ dev / vda1             30830588 11168116 18073328  39% /
tmpfs                     1026472       456   1026016   1% / dev / shm
tmpfs                        5120         0 0      5120   0% / carrera / bloqueo
tmpfs                     1026472         0 0   1026472   0% / sys / fs / cgroup
tmpfs                      205296        36    205260   1% / carrera / usuario / 132
tmpfs                      205296        24    205272   1% / ejecución / usuario / 0
```

El comando `id` muestra la identidad del usuario que ejecuta la sesión junto con la lista de grupos ellos pertenecen. Dado que el acceso a algunos archivos o dispositivos puede estar limitado a los miembros del grupo, verificar la membresía de grupo disponible puede ser útil.

```
$ id
uid = 1000 (buxy) gid = 1000 (buxy) grupos = 1000 (buxy), 27 (sudo)
```

El comando `uname -a` devuelve una línea única que documenta el nombre del kernel (Linux), el nombre del host, la versión del kernel, la versión del kernel, el tipo de máquina (una cadena de arquitectura como x86_64), y el nombre del sistema operativo (GNU / Linux). La salida de este comando generalmente debería se incluirá en los informes de errores, ya que define claramente el núcleo en uso y la plataforma de hardware que están corriendo

```
$ uname -a
Linux kali 4.9.0-kali3-amd64 # 1 SMP Debian 4.9.18-1kali1 (2017-04-04) x86_64 GNU / Linux
```

Todos estos comandos proporcionan información de tiempo de ejecución, pero a menudo es necesario consultar los registros para entender soportar lo que sucedió en su computadora. En particular, el núcleo emite mensajes que almacena en un búfer de anillo cada vez que sucede algo interesante (como un nuevo dispositivo USB que se inserta, una falla en la operación del disco duro o la detección inicial de hardware en el arranque). Puedes recuperar el kernel registra con el comando `dmesg` .

El diario de Systemd también almacena múltiples registros (salida stdout / stderr de demonios, mensajes syslog, kernel logs) y facilita la consulta con `journalctl` . Sin ningún argumento, solo vuelca todos los registros disponibles de forma cronológica. Con la opción `-r` , revertirá el orden que cada mensaje se muestra primero. Con la opción `-f` , imprimirá continuamente nuevas entradas como se adjuntan a su base de datos. La opción `-u` puede limitar los mensajes a los emitidos por un unidad systemd específica (ej .: `journalctl -u ssh.service`).

3.4.6. Descubriendo el hardware

El núcleo exporta muchos detalles sobre el hardware detectado a través de `/ proc /` y `/ sys /` virtual sistemas de archivos. Varias herramientas resumen esos detalles. Entre ellos, `lspci` (en el paquete *pciutils*) enumera los dispositivos PCI, `lsusb` (en el paquete *usbutils*) enumera los dispositivos USB y `lspcmcia` (en los *pcmciautils* paquete) listasPCMCIAcards. Estas herramientas son muy útiles para identificar el modelo exacto del servicio. Esta identificación también permite búsquedas más precisas en la web, que a su vez, conducen a más documentos importantes. Tenga en cuenta que los paquetes *pciutils* y *usbutils* ya están instalados en la base El sistema Kali pero *pcmciautils* debe instalarse con `apt install pcmciautils` . Discutiremos Más información sobre la instalación y gestión de paquetes en un capítulo posterior.

Ejemplo 3.1 *Ejemplo de información proporcionada por* `lspci` *y* `lsusb`

```
$ lspci
[...]
00: 02.1 Controlador de pantalla: Controlador de gráficos Intel Corporation Mobile 915GM / GMS / 910GML Express (rev 03)
00: 1c.0 Puente PCI: Intel Corporation 82801FB / FBM / FR / FW / FRW (Familia ICH6) PCI Express Puerto 1 (rev 03)
00: Controlador USB 1d.0: Intel Corporation 82801FB / FBM / FR / FW / FRW (Familia ICH6) USB UHCI # 1 (rev 03)
[...]
01: 00.0 Controlador Ethernet: Broadcom Corporation NetXtreme BCM5751 Gigabit Ethernet PCI Express (rev 01)
02: 03.0 Controlador de red: Intel Corporation PRO / Wireless 2200BG Network Connection (rev 05)
$ lsusb
```

Bus 005 Dispositivo 004: ID 413c: 8005 Dell Computer Corp.
Bus 005 Dispositivo 008: ID 413c: 8001 Dell Computer Corp.
Bus 005 Dispositivo 007: ID 045e: 00dd Microsoft Corp.
Bus 005 Dispositivo 006: ID 046d: c03d Logitech, Inc.
[...]
Bus 002 Dispositivo 004: ID 413c: 8103 Dell Computer Corp. Inalámbrico 350 Bluetooth

Estos programas tienen una opción -v que enumera información mucho más detallada (pero generalmente innecesaria) ción Finalmente, el comando lsdev (en el paquete *procinfo*) enumera los recursos de comunicación utilizados por dispositivos.

El programa lshw es una combinación de los programas anteriores y muestra una descripción larga del hardware descubierto de manera jerárquica. Debe adjuntar su salida completa a cualquier informe sobre problemas de soporte de hardware.

Page 88

3.5. Resumen

En esta sección, hicimos un recorrido vertiginoso por el paisaje de Linux. Discutimos el kernel y el usuario space, revisó muchos comandos de shell de Linux comunes, discutió procesos y cómo administrar ellos, revisaron los conceptos de seguridad de usuarios y grupos, discutieron el FHS y recorrieron algunos de los más importantes directorios y archivos comunes encontrados en Kali Linux.

Consejos resumidos:

- Linux se usa a menudo para referirse a todo el sistema operativo, pero en realidad Linux es el kernel del sistema operativo iniciado por el gestor de arranque, que a su vez es iniciado por BIOS / UEFI.
- El espacio del usuario se refiere a todo lo que sucede fuera del núcleo. Entre los programas ejecutándose en el espacio del usuario, hay muchas utilidades centrales del proyecto GNU[2] , la mayoría de los cuales están diseñados para ejecutarse desde la línea de comandos (una interfaz basada en texto que le permite ingresar comandos, ejecutarlos y ver los resultados). Un shell ejecuta tus comandos dentro de esa interfaz
- Los comandos comunes incluyen: pwd (imprimir directorio de trabajo), cd (cambiar directorio), ls (lista contenido del archivo o directorio), mkdir (crear directorio), rmdir (eliminar directorio), mv , rm y cp (mover, eliminar o copiar archivos o directorios respectivamente), cat (concatenar o mostrar archivos), menos / más (mostrar archivos página por página), editor (iniciar un editor de texto), buscar (ubicar un archivo o directorio), libre (mostrar información de memoria), df (mostrar espacio libre en disco), id mostrar el identidad del usuario junto con la lista de grupos a los que pertenecen), dmesg (revisar los registros del kernel), y journalctl (muestra todos los registros disponibles).
- Puede inspeccionar el hardware en un sistema Kali con varios comandos: lspci (lista PCI de vices), lsusb (lista de dispositivos USB) y lspcmcia enumera las tarjetas PCMCIA.
- Un proceso es una instancia en ejecución de un programa, que requiere memoria para almacenar tanto el program en sí y sus datos operativos. Puede administrar procesos con comandos como: ps (show procesos), matar (matar procesos), bg (enviar el proceso al fondo), fg (traer el fondo proceso a primer plano) y trabajos (mostrar procesos en segundo plano).
- Los sistemas tipo Unix son multiusuario. Admiten múltiples usuarios y grupos y permiten controlar acciones, en función de los permisos. Puede administrar los derechos de archivo y directorio con varios comandos erales, que incluyen: chmod (cambiar permisos), chown (cambiar propietario) y chgrp (cambio de grupo).
- Al igual que con otras distribuciones profesionales de Linux, Kali Linux está organizado para ser coherente con el *Sistema de archivos* Jerarquía *Estándar* (FHS), que permite a los *usuarios* venir de otras *distribuciones de* Linux para encontrar fácilmente su camino alrededor de Kali.
- Tradicionalmente, los archivos de configuración de la aplicación se almacenan en su directorio de inicio, en oculto. den archivos o directorios que comienzan con un punto (o punto).

[2] http://www.gnu.org

Page 89

Ahora que conoce los fundamentos de Linux, configuremos y ejecute Kali Linux.

Página 90

Palabras clave

Instalación
Desesperado
instalación
Dispositivos ARM
Solución de problemas

Capítulo

4 Instalar Kali Linux

Contenido

Requisitos mínimos de instalación 66
Instalación paso a paso en un disco duro 66
Instalaciones desatendidas 91
Instalaciones ARM 94
Solución de problemas de instalaciones 95
Resumen 100

En este capítulo, nos centraremos en el proceso de instalación de Kali Linux. Primero, discutiremos el mínimo requisitos de instalación de imum (sección 4.1, “ Requisitos mínimos de instalación ” [página 66]) a asegúrese de que su sistema real o virtual esté bien configurado para manejar el tipo de instalación que perseguirás Luego veremos cada paso del proceso de instalación (sección 4.2 4.2, " Paso Instalación paso a paso en un disco duro ”[Página 66]) para una instalación simple, así como para una mayor seguridad Cure la instalación con un sistema de archivos totalmente encriptado. También discutiremos la presentación *previa* , que permite instalaciones desatendidas (sección 4.3 4.3, " Instalaciones desatendidas " [página 91]) al proporcionar Respuestas predeterminadas a las preguntas de instalación. También le mostraremos cómo instalar Kali Linux en varios dispositivos ARM (sección 4.4, " Instalaciones ARM"[Página 94]), que amplía la capacidad de Kali Lazos mucho más allá del escritorio. Finalmente, le mostraremos qué hacer en el raro caso de una instalación falla (sección 4.5, " Solución de problemas de instalaciones " [página 95]), para que pueda resolver el problema y terminar con éxito una instalación difícil.

4.1. Requisitos mínimos de instalación

Los requisitos de instalación para Kali Linux varían según lo que le gustaría instalar. En En el extremo inferior, puede configurar Kali como un servidor Secure Shell (SSH) básico sin escritorio, utilizando tan poco como 128 MB de RAM (se recomiendan 512 MB) y 2 GB de espacio en disco. En el extremo superior, si opta por instale el escritorio predeterminado de GNOME y el *metapaquete kali-linux-full* , realmente debería apuntar a al menos 2048 MB de RAM y 20 GB de espacio en disco.

Además de los requisitos de RAM y disco duro, su computadora debe tener una CPU compatible con al menos una de las arquitecturas amd64, i386, armel, armhf o arm64.

4.2. Instalación paso a paso en un disco duro

En esta sección, asumimos que tiene una unidad USB o DVD de arranque (consulte la sección 2.1.4 , “ Copia la imagen en un DVD-ROM o llave USB ”[página 19] para obtener detalles sobre cómo preparar dicha unidad) y que arrancaste para iniciar el proceso de instalación.

4.2.1 Instalación simple

Primero, veremos una instalación estándar de Kali, con un sistema de archivos sin cifrar.

Arranque e inicio del instalador

Una vez que el BIOS ha comenzado a arrancar desde la unidad USB o DVD-ROM, el menú del gestor de arranque Isolinux aparece, como se muestra en la Figura 4.1, “ Pantalla de inicio ” [página 67]. En esta etapa, el kernel de Linux aún no está cargado; este menú le permite elegir el núcleo para iniciar e ingresar parámetros opcionales para transferido a ella en el proceso.

Para una instalación estándar, solo necesita elegir Instalar o Instalación gráfica (con la flecha teclas), luego presione la tecla Intro para iniciar el resto del proceso de instalación.

Cada entrada de menú oculta una línea de comando de arranque específica, que se puede configurar según sea necesario presionando- Presione la tecla Tab antes de validar la entrada y el arranque.

Figura 4.1 *Pantalla de arranque*

Una vez iniciado, el programa de instalación lo guía paso a paso a través del proceso. Nosotros lo tomaremos
Una mirada a cada uno de estos pasos en detalle. Cubriremos la instalación desde un DVD estándar de Kali Linux.
ROM; Las instalaciones desde un mini.iso pueden verse ligeramente diferentes. También abordaremos gráficas
instalación en modo, pero la única diferencia con la instalación en modo texto clásico es la apariencia.
Las versiones plantean preguntas idénticas y presentan opciones idénticas.

Seleccionando el idioma

Como se muestra en la figura 4.2 , " Selección del idioma"[Página 68], el programa de instalación comienza en
Inglés, pero el primer paso le permite elegir el idioma que se utilizará para el resto del
proceso de instalación. Esta opción de idioma también se utiliza para definir opciones predeterminadas más relevantes en
etapas posteriores (especialmente la distribución del teclado).

Navegando con el Teclado

Algunos pasos en el proceso de instalación requieren que ingrese información. Estas pantallas
tener varias áreas que pueden enfocarse (área de ingreso de texto, casillas de verificación, lista de opciones, OK
y los botones Cancelar), y la tecla Tab le permite moverse de uno a otro.

En el modo de instalación gráfica, puede usar el mouse como lo haría normalmente en un
Escritorio gráfico instalado.

Figura 4.2 *Seleccionar el idioma*

Seleccionando el país

El segundo paso (Figura 4.3 , “ Seleccionar el país ” [página 69]) consiste en elegir su país. En combinación con el idioma, esta información permite que el programa de instalación ofrezca lo mejor diseño de teclado apropiado. Esto también influirá en la configuración de la zona horaria. En el Estados Unidos, se sugiere un teclado QWERTY estándar y el instalador presenta una opción de zonas horarias apropiadas

Figura 4.3 *Selección del país*

Selección de la distribución del teclado

El teclado de inglés americano propuesto corresponde al diseño QWERTY habitual como se muestra en Figura 4.4, " Elección del teclado”[Página 70].

Figura 4.4 *Elección del teclado*

Detección de hardware

En la gran mayoría de los casos, el paso de detección de hardware es completamente automático. El instalador detecta su hardware e intenta identificar el dispositivo de arranque utilizado para acceder a su contenido. Eso carga los módulos correspondientes a los diversos componentes de hardware detectados y luego los monta thebootdeviceinordertoreadit. Los pasos anteriores estaban completamente contenidos en la imagen de arranque incluido en el dispositivo de arranque, un archivo de tamaño limitado y cargado por el cargador de arranque en la memoria cuando Arranque desde el dispositivo de arranque.

Cargando componentes

Con el contenido del dispositivo de arranque ahora disponible, el instalador carga todos los archivos necesarios para Continuar con su trabajo. Esto incluye controladores adicionales para el hardware restante (especialmente la tarjeta de red), así como todos los componentes del programa de instalación.

Detectar hardware de red

En este paso, el instalador intentará identificar automáticamente la tarjeta de red y cargará el módulo de sponding. Si la detección automática falla, puede seleccionar manualmente el módulo para cargar. Me caigo de lo contrario, puede cargar un módulo específico desde un dispositivo extraíble. Esta última solución suele ser solo es necesario si el controlador apropiado no está incluido en el kernel estándar de Linux, pero está disponible en otros lugares, como el sitio web del fabricante.

Esto significa que es totalmente exitoso para las instalaciones de red (como por ejemplo, cuando se inicia desde un mini.iso), ya que los paquetes Debian deben cargarse desde la red.

Configurando la red

Para automatizar el proceso tanto como sea posible, el instalador intenta una red automática configuración de trabajo mediante el protocolo de configuración dinámica de host (DHCP) (para IPv4 e IPv6) y ICMPv6's Neighbor Discovery Protocol (para IPv6), como se muestra en la Figura 4.5, " Configuración automática de red-ración "[página 71].

Figura 4.5 *Configuración automática de red*

Si la configuración automática falla, el instalador ofrece más opciones: intente nuevamente con una configuración normal Configuración de DHCP, intente la configuración de DHCP declarando el nombre de la máquina o configure Una configuración de red estática.

Esta última opción requiere una dirección IP, una máscara de subred, una dirección IP para una posible puerta de enlace, un

nombre de la máquina y un nombre de dominio.

98

Configuración sin DHCP Si la red local está equipada con un servidor DHCP que no desea utilizar porque prefiere definir una dirección IP estática para la máquina durante la instalación, Puede agregar la opción **netcfg / use_dhcp = false** al arrancar. Solo necesitas edite la entrada de menú deseada presionando la tecla Tab y agregando la opción deseada antes de presionar la tecla Enter.

Contraseña de root

El instaladorpromptsforapassword (Figura 4.6, " RootPassword " [página72]) sincerautomáticamente crea una cuenta raíz de superusuario. El instalador también solicita una confirmación de la contraseña para evitar cualquier error de entrada que luego sería difícil de ajustar.

Figura 4.6 *Contraseña raíz*

Page 99

El administrador Contraseña La contraseña del usuario raíz debe ser larga (ocho caracteres o más) e imposible adivinar, ya que los atacantes atacan computadoras y servidores conectados a Internet con herramientas tomadas, intentando iniciar sesión con contraseñas obvias. A veces atacantes aprovechar los ataques del diccionario, utilizando muchas combinaciones de palabras y números como contraseña palabras. Evite usar los nombres de los niños o padres y las fechas de nacimiento, porque estos son fáciles de adivinar

Estas observaciones son igualmente aplicables a otras contraseñas de usuario, pero las consecuencias de una cuenta comprometida son menos drásticas para los usuarios sin derechos administrativos.

Si le falta inspiración, no dude en usar un generador de contraseñas, como pwgen (que se encuentra en el paquete del mismo nombre, que ya está incluido en la base Instalación de Kali).

Configurando el reloj

Si la red está disponible, el reloj interno del sistema se actualizará desde un protocolo de tiempo de red servidor col (NTP). Esto es beneficioso porque garantiza que las marcas de tiempo en los registros sean correctas desde primer arranque.

Si su país abarca varias zonas horarias, se le pedirá que seleccione la zona horaria que desee para usar, como se muestra en la Figura 4.7 , " Selección de zona horaria " [página 73].

Figura 4.7 *Selección de zona horaria*

Página 100

Detección de discos y otros dispositivos

Este paso detecta automáticamente los discos duros en los que se puede instalar Kali, cada uno de los cuales se presentará en el siguiente paso: particionamiento.

Fraccionamiento

El particionamiento es un paso indispensable en la instalación, que consiste en dividir el espacio disponible en los discos duros en secciones discretas (*particiones*) de acuerdo con la función prevista del computadora y esas particiones. Particionar también implica elegir los sistemas de archivos que se utilizarán. Todas de estas decisiones tendrá influencia sobre el rendimiento, la seguridad de los datos y la administración del servidor.

El paso de partición es tradicionalmente difícil para los nuevos usuarios. Sin embargo, los sistemas de archivos Linux y las particiones, incluida la memoria virtual (o particiones de *intercambio*) deben definirse a medida que forman la base dación del sistema. Esta tarea puede complicarse si ya ha instalado otra sistema operativo en la máquina y desea que los dos coexistan. En este caso, debes hacer asegúrese de no alterar sus particiones, o si es necesario, cambie su tamaño sin causar daños.

Para acomodar los esquemas de particiones más comunes (y simples), la mayoría de los usuarios preferirán el *Guiado* modo que recomienda configuraciones de partición y proporciona sugerencias en cada paso del camino. Los usuarios más avanzados apreciarán el modo *Manual* , que permite configuraciones más avanzadas. raciones Cada modo comparte ciertas capacidades.

Figura 4.8 *Elección del modo de partición*

Particionamiento guiado La primera pantalla en la herramienta de **partición** (Figura 4.8, " Elección de partición Modo "[página 74]) presenta puntos de entrada para los modos de particionamiento guiado y manual. "Guiado - usar disco completo "es el esquema de partición más simple y común, que asignará un disco completo disco a Kali Linux.

Las siguientes dos selecciones usan Logical Volume Manager (LVM) para configurar lógico (en lugar de físico), opcionalmente encriptado, particiones. Discutiremos LVM y cifrado más adelante en este capítulo.

Finalmente, la última opción inicia la partición manual, lo que permite una partición más avanzada esquemas, como instalar Kali Linux junto con otros sistemas operativos. Discutiremos manual modo en la siguiente sección.

En este ejemplo, asignaremos un disco duro completo a Kali, por lo que seleccionamos "Guiado: usar todo el disco" para proceder al siguiente paso.

La siguiente pantalla (que se muestra en la Figura 4.9, " Disco para usar para particionamiento guiado "[Página 75]) le permite para elegir el disco donde se instalará Kali seleccionando la entrada correspondiente (para examen- ple, "Disco virtual 1 (vda) - 32.2 GB Virtio Block Device"). Una vez seleccionado, la partición guiada Seguir. Esta opción borrará todos los datos en este disco, así que elija sabiamente.

Figura 4.9 *Disco a utilizar para particionamiento guiado*

A continuación, la herramienta de partición guiada ofrece tres métodos de partición, que corresponden a diferentes usos ent, como se muestra en la Figura 4.10 , “ Asignación guiada de particiones”[Página 76].

Figura 4.10 *Asignación guiada de particiones*

El primer método se llama "Todos los archivos en una partición". Todo el árbol del sistema Linux se almacena en un sistema de archivos único, correspondiente al directorio raíz (" / "). Esta partición simple y robusta El esquema funciona perfectamente bien para sistemas personales o de un solo usuario. A pesar del nombre, dos particiones en realidad se creará: el primero albergará el sistema completo, el segundo la memoria virtual (o "intercambio").

El segundo método, "Separar / inicio / partición", es similar, pero divide la jerarquía de archivos en dos: una partición contiene el sistema Linux (/) y la segunda contiene "directorios homed" datos de usuario, en archivos y subdirectorios disponibles en / home /). Un beneficio de este método es que Es fácil preservar los datos de los usuarios si tiene que reinstalar el sistema.

El último método de particionamiento, denominado "Particiones separadas / home , / var y / tmp ", es apropiado para servidores y sistemas multiusuario. Divide el árbol de archivos en muchas particiones: además de las particiones raíz (/) y cuentas de usuario (/ home /), también tiene particiones para datos de software del servidor (/ var /) y archivos temporales (/ tmp /). Un beneficio de este método es que los usuarios finales no pueden bloquear el servidor al consumir todo el espacio disponible en el disco duro (solo pueden llenar / tmp / y / home /). Al mismo tiempo, los datos del demonio (especialmente los registros) ya no pueden obstruir el resto del sistema.

Después de elegir el tipo de partición, el instalador presenta un resumen de sus selecciones en el pantalla como un mapa de partición (Figura 4.11, " Validación de particionamiento"[Página 77]). Puedes modificar cada particionar individualmente seleccionando una partición. Por ejemplo, podría elegir otro sistema de archivos si el estándar (*ext4*) no es apropiado. En la mayoría de los casos, sin embargo, la partición propuesta es rea sonable y puede aceptarlo seleccionando "Finalizar partición y escribir cambios en el disco". Puede Huelga decirlo, pero elija sabiamente ya que esto borrará el contenido del disco seleccionado.

Figura 4.11 *Validación de particionamiento*

Particionamiento manual Seleccionar Manual en la pantalla principal de "Partition disks" (Figura 4.8, " Elección ofPartitionMode "[página74]) permite una mayor flexibilidad, lo que le permite elegir configuraciones y dictan específicamente el propósito y el tamaño de cada partición. Por ejemplo, esto el modo le permite instalar Kali junto con otros sistemas operativos, habilitar un redunde basado en software conjunto de discos independientes (RAID) para proteger los datos de fallas del disco duro y cambiar el tamaño de forma segura

particiones existentes sin perder datos, entre otras cosas.

Reducir una ventana Dividir

Para instalar Kali Linux junto con un sistema operativo existente (Windows u otro), usted necesitará espacio disponible en el disco duro no utilizado para las particiones dedicadas a Kali. En En la mayoría de los casos, esto significa reducir una partición existente y reutilizar el espacio liberado.

Si está utilizando el modo de partición manual, el instalador puede reducir un Windows partición con bastante facilidad. Solo necesita elegir la partición de Windows e ingresar su nuevo tamaño (esto funciona igual con las particiones FAT y NTFS).

Página 104

Si es un usuario menos experimentado que trabaja en un sistema con datos existentes, tenga mucho cuidado con este método de configuración, ya que es muy fácil cometer errores que podrían conducir a la pérdida de datos.

La primera pantalla en el instalador manual es en realidad la misma que se muestra en la Figura 4.11 , " Vali-Particionamiento de citas "[Página 77], excepto que no incluye particiones nuevas para crear. Le corresponde a ti para agregar esos.

Primero, verá una opción para ingresar a "Particionamiento guiado" seguido de varias opciones de configuración iones A continuación, el instalador mostrará los discos disponibles, sus particiones y cualquier espacio libre posible. que aún no se ha particionado. Puede seleccionar cada elemento mostrado y presionar la tecla Enter para interactuar con él, como siempre.

Si el disco es completamente nuevo, es posible que deba crear una tabla de particiones. Puede hacer esto seleccionando el disco. Una vez hecho esto, debería ver el espacio libre disponible dentro del disco.

Para hacer uso de este espacio libre, debe seleccionarlo y el instalador le ofrecerá dos formas de crear particiones en ese espacio.

Figura 4.12 *Crear particiones en el espacio libre*

La primera entrada creará una única partición con las características (incluido el tamaño) de su elección. La segunda entrada usará todo el espacio libre y creará múltiples particiones con la ayuda del asistente de particionamiento guiado (ver sección 4.2.1.12.1 , " Particionamiento guiado "[página 75]). Esta opción es particularmente interesante cuando desea instalar Kali junto con otro sistema operativo sistema, pero cuando no desea microadministrar el diseño de la partición. La última entrada mostrará los números de cilindro / culata / sector del inicio y del final del espacio libre.

Cuando seleccione "Crear una nueva partición", entrará en la carne de la partición manual secuenciación Después de seleccionar esta opción, se le solicitará un tamaño de partición. Si el disco

Page 105

usa una tabla de partición MSDOS, se le dará la opción de crear una partición primaria o lógica. (Cosas que debemos saber: solo puedes tener cuatro particiones primarias pero muchas particiones más lógicas. la partición que contiene / boot , y por lo tanto el núcleo, debe ser primaria, las particiones lógicas residen en una partición extendida, que consume una de las cuatro particiones primarias.) Entonces debería ver la pantalla de configuración de partición genérica:

Figura 4.13 *Pantalla de configuración de partición*

Para resumir este paso de particionamiento manual, echemos un vistazo a lo que puede hacer con el nuevo dividir. Usted puede:

- Formatee e inclúyalo en el árbol de archivos eligiendo un punto de montaje. El punto de montaje es el directorio que albergará el contenido del sistema de archivos en la partición seleccionada. Así, una partición montada en / home / está tradicionalmente destinada a contener datos de usuario, mientras que " / " es conocida como la *raíz* del árbol de archivos y, por lo tanto, la raíz de la partición que realmente Hospedar el sistema Kali.

- Úselo como una *partición de intercambio* . Cuando el kernel de Linux carece de suficiente memoria libre, almacenará partes inactivas de RAM en una partición de intercambio especial en el disco duro. La memoria virtual sub- El sistema lo hace transparente para las aplicaciones. Para simular la memoria adicional, Win- dows usa un archivo de intercambio (paginación) que está directamente contenido en un sistema de archivos. Por el contrario, Linux usa una partición dedicada a este propósito, de ahí el término partición de intercambio.

- Conviértalo en un "volumen físico para el cifrado" para proteger la confidencialidad de los datos en Ciertas particiones. Este caso está automatizado en la partición guiada. Mira la sección 4.2.2, " En- instalación en un sistema de archivos totalmente encriptado "[Página 85] para más información.

- Conviértalo en un "volumen físico para LVM" (no cubierto en este libro). Tenga en cuenta que esta característica es utilizado por la partición guiada cuando configura particiones cifradas.

- Úselo como un dispositivo RAID (no cubierto en este libro).

- Elija no usar la partición y no la modifique.

Cuando termine, puede salir de la partición manual seleccionando "Deshacer cambios a particiones "o escriba sus cambios en el disco seleccionando" Finalizar partición y escribir cambios al disco "desde la pantalla del instalador manual (Figura 4.11, " Validación de particionamiento " [página 77]).

Copiar la imagen en vivo

El siguiente paso, que no requiere ninguna interacción del usuario, copia el contenido de la imagen en vivo. al sistema de archivos de destino, como se muestra en la Figura 4.14, " Copiando los datos de la imagen en vivo " [página 80].

Figura 4.14 *Copiando los datos de la imagen en vivo*

Page 107

Configurar el Administrador de paquetes (apt)

Para poder instalar el software adicional tradicional, APT necesita configurarse y contarse dónde encontrar Paquetes de Debian En Kali, este paso es en su mayoría no interactivo ya que forzamos al espejo a ser http.kali. org. Solo tiene que confirmar si desea usar este espejo (Figura 4.15, " Usar una red ¿Espejo? "[Página 81]). Si no lo usa, no podrá instalar paquetes complementarios con apt a menos que configure un repositorio de paquetes más tarde.

Figura 4.15 ¿ *Usar un espejo de red?*

Si desea utilizar un espejo local en lugar de http.kali.org, puede pasar su nombre en el núcleo línea de comando (en el momento del arranque) con una sintaxis como esta: mirror / http / hostname = *my.own.mirror* .

108

Finalmente, el programa propone usar un *proxy HTTP* como se muestra en la Figura 4.16 , " Use un proxy HTTP " [página 82]. Un proxy HTTP es un servidor que reenvía solicitudes HTTP para usuarios de la red. A veces ayuda a acelerar las descargas manteniendo una copia de los archivos que se han transferido a través de él (nosotros

luego hablemos de un proxy de almacenamiento en caché). En algunos casos, es el único medio para acceder a una web externa.
servidor; el instalador no podrá descargar el paquete de Debian correctamente
complete este campo durante la instalación. Si no proporciona una dirección proxy, el instalador intentará
para conectarse directamente a Internet.

Figura 4.16 *Usar un proxy HTTP*

A continuación, los archivos Packages.xz y Sources.xz se descargarán automáticamente para actualizar la lista.
de paquetes reconocidos por APT.

Instalación del cargador de arranque GRUB

El gestor de arranque es el primer programa iniciado por el BIOS. Este programa carga el kernel de Linux en
memoria y luego lo ejecuta. El gestor de arranque a menudo ofrece un menú que le permite elegir el
kernel para cargar o el sistema operativo para arrancar.

Debido a su superioridad técnica, GRUB es el gestor de arranque predeterminado instalado por Debian: funciona con
la mayoría de los sistemas de archivos y, por lo tanto, no requieren una actualización después de cada instalación de un nuevo núcleo,
ya que lee su configuración durante el arranque y encuentra la posición exacta del nuevo núcleo.

Debe instalar GRUB en el Master Boot Record (MBR) a menos que ya tenga otro Linux
El sistema se instaló para que sepa cómo arrancar Kali Linux. Como se señala en la Figura 4.17 , "Instale el arranque GRUB
Cargador en un disco duro "[Página 83], modificar el MBR hará que los sistemas operativos no sean reconocidos
que dependen de que no se pueda iniciar hasta que arregle la configuración de GRUB.

Figura 4.17 *Instale el cargador de arranque GRUB en un disco duro*

En este paso (Figura 4.18, " Dispositivo para la instalación del cargador de arranque " [página 84]), debe seleccionar qué Se instalará el dispositivo GRUB. Esta debería ser su unidad de arranque actual.

Figura 4.18 *Dispositivo para la instalación del cargador de arranque*

De manera predeterminada, el menú de inicio propuesto por GRUB muestra todos los núcleos de Linux instalados, así como cualquier otros sistemas operativos que fueron detectados. Es por eso que debes aceptar la oferta para instalarlo en el Master Boot Record. Mantener versiones anteriores del kernel conserva la capacidad de iniciar el sistema si el kernel instalado más recientemente está defectuoso o mal adaptado al hardware. Nosotros asi Le recomendamos que mantenga instaladas algunas versiones anteriores del kernel.

Cuidado: el cargador de arranque y arranque dual

Esta fase del proceso de instalación detecta los sistemas operativos que ya están instalado en la computadora y agregará automáticamente las entradas correspondientes en el menú de arranque. Sin embargo, no todos los programas de instalación hacen esto.

En particular, si instala (o reinstala) Windows posteriormente, el gestor de arranque será borrado. Kali todavía estará en el disco duro, pero ya no será accesible desde el arranque menú. Debería iniciar el instalador de Kali con el **rescate / enable = true** parámetro en la línea de comando del núcleo para reinstalar el cargador de arranque. Esta operación es descrito en detalle en el manual de instalación de Debian.

[2] http://www.debian.org/releases/stable/amd64/ch08s07.html

Finalizando la instalación y reiniciando

Ahora que la instalación se ha completado, el programa le pide que quite el DVD-ROM del lector (o desconecte su unidad USB) para que su computadora pueda iniciarse en su nuevo sistema Kali después de el instalador reinicia el sistema (Figura 4.19, " Instalación completa " [página 85]).

Finalmente, el instalador realizará algunos trabajos de limpieza, como eliminar paquetes que son específicos de creating el ambiente vivo.

Figura 4.19 *Instalación completa*

4.2.2 Instalación en un sistema de archivos totalmente cifrado

Para garantizar la confidencialidad de sus datos, puede configurar particiones cifradas. Esto favorecerá proteja sus datos si pierde o le roban su computadora portátil o disco duro. La herramienta de partición puede ayudarlo a este proceso, tanto en modo guiado como manual.

El modo de particionamiento guiado combinará el uso de dos tecnologías: Configuración de clave unificada de Linux (LUKS) para encriptar particiones y Logical Volume Management (LVM) para administrar el almacenamiento dinamicamente. Ambas funciones también se pueden configurar y configurar mediante el modo de partición manual.

Introducción a LVM

Discutamos primero LVM. Usando la terminología de LVM, una *partición virtual* es un volumen lógico, que es parte de un *grupo de volúmenes* , o una asociación de varios volúmenes físicos. Los volúmenes físicos son reales. particiones (o particiones virtuales exportadas por otras abstracciones, como un dispositivo RAID de software o una partición encriptada).

Con su falta de distinción entre particiones "físicas" y "lógicas", LVM le permite crear Particiones "virtuales" que abarcan varios discos. Los beneficios son dobles: el tamaño de las particiones es ya no está limitado por discos individuales sino por su volumen acumulativo, y puede cambiar el tamaño de los existentes particiones en cualquier momento, como después de agregar un disco adicional.

Esta técnica funciona de una manera muy simple: cada volumen, ya sea físico o lógico, se divide en bloques del mismo tamaño, que LVM correlaciona. La adición de un nuevo disco provocará la creación de un nuevo volumen físico que proporciona nuevos bloques que pueden asociarse a cualquier grupo de volúmenes. Todo Las particiones en el grupo de volúmenes pueden aprovechar al máximo el espacio asignado adicional.

Introducción a LUKS

Para proteger sus datos, puede agregar una capa de cifrado debajo de su sistema de archivos de elección. Linux (y más particularmente el controlador *dm-crypt*) usa el mapeador de dispositivos para crear la partición virtual (cuyo contenido está protegido) basado en una partición subyacente que almacenará los datos en un formulario encriptado (gracias a LUKS). LUKS estandariza el almacenamiento de los datos cifrados, así como metainformación que indica los algoritmos de cifrado utilizados.

Partición de intercambio cifrada Cuando se utiliza una partición cifrada, la clave de cifrado se almacena en la memoria (RAM), y cuando hiberna, una computadora portátil copiará la clave, junto con otros contenidos de RAM, a la partición de intercambio del disco duro. Dado que cualquier persona con acceso al archivo de intercambio (incluido un técnico o un ladrón) podría extraer la clave y descifrar sus datos, el archivo de intercambio debe estar protegido con encriptación

Debido a esto, el instalador le avisará si intenta usar una partición encriptada junto a una partición de intercambio sin cifrar.

Configuración de particiones cifradas

El proceso de instalación para LVM cifrado es el mismo que para una instalación estándar, excepto para paso de partición (Figura 4.20, “ Particionamiento guiado con LVM cifrado ” [página 87]) donde

en su lugar, seleccionará "Guiado: use todo el disco y configure LVM cifrado". El resultado neto será un sistema que no se puede iniciar o acceder hasta que se proporcione la frase de contraseña de cifrado. Esta voluntad cifrar y proteger los datos en su disco.

Figura 4.20 *Particionamiento guiado con LVM cifrado*

El instalador de particionamiento guiado asignará automáticamente una partición física para el almacenamiento de datos cifrados, como se muestra en la Figura 4.21 , " Confirmar cambios en la tabla de particiones ”[página 88]. A En este punto, el instalador confirmará los cambios antes de que se escriban en el disco.

Figura 4.21 *Confirmar cambios en la tabla de particiones*

Esta nueva partición se inicializa con datos aleatorios, como se muestra en la Figura 4.22 , “ Borrado de datos en Partición cifrada ”[página 88]. Esto hace que las áreas que contienen datos no se puedan distinguir del áreas no utilizadas, lo que hace que sea más difícil detectar y posteriormente atacar los datos cifrados.

Figura 4.22 *Borrar datos en una partición cifrada*

A continuación, el instalador le pide que ingrese una frase de contraseña de cifrado (Figura 4.23, " Ingrese su encriptación-Frase de contraseña”[Página 89]). Para ver el contenido de la partición encriptada, deberá necesita ingresar esta frase de contraseña cada vez que reinicie el sistema. Tenga en cuenta la advertencia en el instalador: su sistema encriptado solo será tan fuerte como esta frase de contraseña.

Figura 4.23 *Ingrese su frase de contraseña de cifrado*

La herramienta de particionamiento ahora tiene acceso a una nueva partición virtual cuyo contenido se almacena en-
cifrado en la partición física subyacente. Como LVM usa esta nueva partición como un físico
volumen, puede proteger varias particiones (o volúmenes lógicos LVM) con la misma clave de cifrado,
incluida la partición de intercambio (consulte la barra lateral " Partición de intercambio cifrada"[Página 86]). Aquí, LVM no es
se usa para facilitar la extensión del tamaño de almacenamiento, pero solo por la conveniencia de la indirección
permitiendo dividir una sola partición encriptada en múltiples volúmenes lógicos.

Fin de la partición guiada con LVM cifrado

A continuación, se muestra el esquema de partición resultante (Figura 4.24, " Validación de particionamiento para En-
Instalación de LVM encriptada"[Página 90]) para que pueda ajustar la configuración según sea necesario.

Figura 4.24 *Validación del particionamiento para la instalación de LVM cifrado*

Página 117

Finalmente, después de validar la configuración de la partición, la herramienta solicita confirmación para escribir los cambios en los discos, como se muestra en la Figura 4.25, " Confirmar las particiones que se formatearán " [página 91].

Figura 4.25 *Confirmar particiones para formatear*

Finalmente, el proceso de instalación continúa como se documenta en la sección 4.2.1.14 , " Configuración el administrador de paquetes (apt)"[Página 81].

4.3. Instalaciones desatendidas

Los instaladores de Debian y Kali son muy modulares: en el nivel básico, solo están ejecutando muchos scripts (empaquetados en pequeños paquetes llamados udeb — para µdeb o micro-deb) uno tras otro. Cada el script se basa en debconf (consulte " La herramienta debconf " [página 214]), que interactúa con usted, el usuario, y almacena los parámetros de instalación. Debido a esto, el instalador también se puede automatizar a través de

118

la presentación de informes, la función le permite proporcionar respuestas de un asistente a las solicitudes de instalación iones

4.3.1. Presentando respuestas

Hay varias formas de preseleccionar las respuestas al instalador. Cada método tiene sus propias ventajas. y desventajas Dependiendo de cuándo ocurre la presentación previa, las preguntas que pueden ser pre sembradas varían.

Con parámetros de arranque

Puede preseleccionar cualquier pregunta del instalador con parámetros de arranque que terminen en el comando del núcleo:

línea, accesible a través de / proc / cmdline . Algunos gestores de arranque le permitirán editar estos parámetros interactivamente (lo cual es práctico para fines de prueba), pero si desea hacer que los cambios persistan, carpa, tendrá que modificar la configuración del gestor de arranque.

Puede usar directamente el identificador completo de las preguntas de deb (suchasdebian-installer / language = es) o puede usar abreviaturas para las preguntas más comunes (como idioma = es o nombre de host = duque). Ver la lista completa[1] de alias en el manual de instalación de Debian.

No hay restricciones sobre qué preguntas puede preseleccionar ya que los parámetros de arranque están disponibles desde el inicio del proceso de instalación y se procesan muy temprano. Sin embargo, el número de los parámetros de arranque está limitado a 32 y algunos de ellos ya se usan por defecto. Tambien es Es importante darse cuenta de que cambiar la configuración del cargador de arranque puede no ser trivial a veces.

En la sección 9.3, " Creación de imágenes ISO de Kali Live personalizadas "[Página 237] también aprenderá a modificar la configuración de Isolinux cuando genera su propia imagen ISO de Kali.

Con un archivo presentado en el Initrd

Puede añadir un archivo llamado preseed.cfg en la raíz de la instalación de initrd (esto es, que el initrd se usa para iniciar el instalador). Por lo general, esto requiere reconstruir el paquete fuente del instalador de Debian para generar nuevas versiones de initrd. Sin embargo, live-build ofrece una forma conveniente de hacer esto, que se detalla en la sección 9.3 , " Creación de imágenes ISO de Kali Live personalizadas "[Página 237].

Este método tampoco tiene restricciones en las preguntas que puede preseleccionar como El archivo predeterminado está disponible inmediatamente después del arranque. En Kali, ya utilizamos esta función para personalizar el comportamiento del instalador oficial de Debian.

[1] https://www.debian.org/releases/stable/amd64/apbs02#preseed-aliases

Con un archivo presentado en el medio de arranque

Puede agregar un archivo preestablecido en el medio de arranque (CD o llave USB); la preselección entonces ocurre tan pronto a medida que se montan los medios, lo que significa justo después de las preguntas sobre el idioma y el teclado diseño. El parámetro de inicio de preseed / file se puede usar para indicar la ubicación del archivo de preseeding (por ejemplo, /cdrom/preseed.cfg al instalar desde un CD-ROM, o /hd-media/preseed.cfg cuando se instala desde una llave USB).

Usted no puede ver una respuesta al lenguaje y las opciones de país mientras el archivo de presentación se carga más tarde en el proceso, una vez que se hayan cargado los controladores de hardware. En el lado positivo, live-build facilita poner un archivo suplementario en las imágenes ISO generadas (ver sección 9.3, " Edificio Imágenes ISO de Kali Live personalizadas "[Página 237]).

Con un archivo presentado cargado desde la red

Puede hacer que un archivo preestablecido esté disponible en la red a través de un servidor web y decirle al instalador para descargar ese archivo preseleccionado agregando el parámetro de arranque preseed / url = http: // *server* /preseed.cfg (o usando el alias de url).

Sin embargo, cuando use este método, recuerde que primero debe configurar la red. Esta significa que las preguntas debconf relacionadas con la red (en particular, el nombre de host y el nombre de dominio) y Todas las preguntas anteriores (como el idioma y el país) no pueden preseleccionarse con este método. Este método se usa con mayor frecuencia en combinación con parámetros de arranque que preseleccionan aquellos específicos preguntas

Este método de preselección es el más flexible, ya que puede cambiar la configuración de instalación sin cambiar los medios de instalación.

Retrasar el lenguaje, Country, Keyboard Preguntas	Para superar la limitación de no poder preseleccionar el idioma, el país y preguntas del teclado, puede agregar el parámetro de arranque auto-install / enable = true (o auto = verdadero). Con esta opción, las preguntas se harán más adelante en el proceso, después de configurar la red y, por lo tanto, después de la descarga del archivo preestablecido. La desventaja es que los primeros pasos (especialmente la configuración de la red) siempre sucederán lápiz en inglés y si hay errores, el usuario tendrá que trabajar en inglés pantallas (con un teclado configurado en QWERTY).

4.3.2. Crear un archivo presentado

Un archivo predeterminado es un archivo de texto sin formato en el que cada línea contiene la respuesta a una pregunta de Debconf. Una línea se divide en cuatro campos separados por espacios en blanco (espacios o pestañas). Por ejemplo, di mirror / suite string kali-rolling:

- El primer campo indica el propietario de la pregunta. Por ejemplo, "di" se usa para preguntas relevante para el instalador. También puede ver un nombre de paquete, para preguntas provenientes de De- paquetes bian (como en este ejemplo: atftpd atftpd / use_inetd boolean false).
- El segundo campo es un identificador para la pregunta.
- El tercer campo enumera el tipo de pregunta.
- El cuarto y último campo contiene el valor de la respuesta esperada. Tenga en cuenta que debe ser separado del tercer campo con un solo espacio; los caracteres de espacio adicionales son considerados ered parte del valor.

La forma más sencilla de escribir un archivo preestablecido es instalar un sistema a mano. Entonces el debconf-get-selecciones: el comando de instalación proporcionará las respuestas que proporcionó al instalador. usted puede obtener respuestas dirigidas a otros paquetes con debconf-get-selections . Sin embargo, un Una solución más limpia es escribir el archivo preseleccionado a mano, comenzando con un ejemplo y luego yendo a través de la documentación. Con este enfoque, solo preguntas donde la respuesta predeterminada necesita para ser anulado se puede preestablecer. Proporcione el parámetro de arranque prioridad = crítico para instruir a Deb- conf solo hacer preguntas críticas y usar la respuesta predeterminada para otros.

Guía de instalación Apéndice

La guía de instalación de Debian, disponible en línea, incluye documentación detallada sobre El uso de un archivo preseleccionado en un apéndice. También incluye un detallado y comentado archivo de muestra, que puede servir como base para personalizaciones locales.

[2] https://www.debian.org/releases/stable/amd64/apb.html

[2] https://www.debian.org/releases/stable/example-preseed.txt

Sin embargo, tenga en cuenta que los enlaces anteriores documentan la versión estable de Debian y que Kali usa la versión de prueba, por lo que puede encontrar ligeras diferencias. Tú también puedes consulte el manual de instalación alojado en el sitio web del proyecto del instalador de Debian. Eso puede estar más actualizado.

[2] http://di.alioth.debian.org/manual/en.amd64/apb.html

4.4. Instalaciones ARM

Kali Linux se ejecuta en una amplia variedad de dispositivos basados en ARM (computadoras portátiles, computadoras integradas y dispositivos de desarrollo). tarjetas de operación, por ejemplo) pero no puede usar el instalador tradicional de Kali en estos dispositivos desde a menudo tienen requisitos específicos en términos de configuración del kernel o del gestor de arranque.

Para hacer que esos dispositivos sean más accesibles para los usuarios de Kali, Offensive Security desarrolló scripts para construir imágenes de disco [2] que están listos para usar con varios dispositivos ARM. Proporcionan esas imágenes para descargar en su sitio web:

[2] https://www.offensive-security.com/kali-linux-arm-images/

[2] https://github.com/offensive-security/kali-arm-build-scripts

Como estas imágenes están disponibles, su tarea de instalar Kali en un dispositivo ARM se simplifica enormemente. Aquí están los pasos básicos:

1. Descargue la imagen para su dispositivo ARM y asegúrese de que la suma de verificación coincida con la proporcionado en el sitio web (ver sección 2.1.3, " Verificación de integridad y autenticidad "[Página 16] para explicaciones sobre cómo hacerlo). Tenga en cuenta que las imágenes suelen estar comprimidas xz; hacer Asegúrese de descomprimirlos con unxz .
2. Dependiendo de la ranura de expansión de almacenamiento disponible en su dispositivo ARM específico, adquiera un Tarjeta SD, tarjeta micro SD o módulo eMMC que tiene una capacidad de al menos 8 GB.
3. Copie la imagen descargada al dispositivo de almacenamiento con dd . Esto es similar al proceso de

Copiar una imagen ISO en una memoria USB (ver sección 2.1.4, " Copiando la imagen en un DVD-ROM o llave USB " [página 19]).

```
# dd if = kali-image.img of = / dev / something bs = 512k
```

4. Enchufe la tarjeta SD / eMMC en su dispositivo ARM.
5. Inicie su dispositivo ARM e inicie sesión en él (*usuario "root", contraseña "toor"*). Si no tienes pantalla conectado, entonces tendrá que averiguar la dirección IP que se ha asignado a través de DHCP y conectarse a esa dirección a través de SSH. Algunos servidores DHCP tienen herramientas o interfaces web para mostrar los arrendamientos actuales. Si no tiene nada de eso, use un sniffer para buscar DHCP Arrendamiento de tráfico.
6. Cambie la contraseña de root y genere nuevas claves de host SSH, especialmente si el dispositivo será corriendo permanentemente en una red pública! Los pasos son relativamente sencillos, ver " Generando nuevas claves de host SSH " [página 111].
7. ¡Disfruta de tu nuevo dispositivo ARM con Kali Linux!

Casos especiales y más Documentación detallada

Estas instrucciones son genéricas y, aunque funcionan para la mayoría de los dispositivos, siempre hay excepciones Por ejemplo, los Chromebook requieren el *modo desarrollador* y otros dispositivos. requieren una pulsación de tecla especial para arrancar desde medios externos.

Dado que los dispositivos ARM se agregan con relativa frecuencia y sus especificaciones son tan dinámicas namic, aquí no cubriremos instrucciones de instalación específicas para varios dispositivos ARM. En su lugar, consulte la sección dedicada "Kali en ARM" de la web de documentación de Kali. sitio para obtener información sobre cada dispositivo ARM compatible con Offensive Security:

[2] http://docs.kali.org/category/kali-on-arm

4.5. Solución de problemas de instalaciones

El instalador es bastante confiable, pero puede encontrar errores o enfrentar problemas externos como: net- problemas de trabajo, espejos defectuosos y espacio en disco insuficiente. Debido a esto, es bastante útil ser capaz de solucionar problemas que aparecen en el proceso de instalación.

Cuando el instalador falla, le mostrará una pantalla poco útil, como la que se muestra en la Fig. ure 4.26 , " Error en el paso de instalación "[Página 96].

Figura 4.26 *Error en el paso de instalación*

En este punto, es bueno saber que el instalador utiliza múltiples consolas virtuales:
la pantalla principal que ves se ejecuta en la quinta consola (para el instalador gráfico,
CTRL + Shift + F5) o en la primera consola (para el instalador textual, CTRL + Shift + F1). En ambos casos,
la cuarta consola (CTRL + Shift + F4) muestra registros de lo que está sucediendo y generalmente puede ver un
mensaje de error más útil allí, como el de la Figura 4.27 , " La pantalla de registro del instalador "
[página 97], que revela que el instalador se ha quedado sin espacio en disco.

Figura 4.27 *La pantalla de registro del instalador*

Las consolas segunda y tercera (CTRL + Shift + F2 y CTRL + Shift + F3, respectivamente) alojan shells que
puede usar para investigar la situación actual con más detalle. La mayoría de las herramientas de línea de comando
son proporcionados por BusyBox, por lo que el conjunto de características es bastante limitado, pero es suficiente para descubrir la mayoría de
Los problemas que es probable que encuentre.

¿Qué se puede hacer en el Shell de instalador

Puede inspeccionar y modificar la base de datos debconf con debconf-get y debconf-conjunto . Estos comandos son especialmente convenientes para probar valores de preselección.

Puede inspeccionar cualquier archivo (como el registro de instalación completo disponible en / var / log / syslog) con gato o más . Puede editar cualquier archivo con nano , incluidos todos los archivos ing instalado en el sistema. El sistema de archivos raíz se montará en / target una vez
El paso de partición del proceso de instalación se ha completado.

Una vez que se ha configurado el acceso a la red, puede usar wget y nc (netcat) para recuperar y exportar datos a través de la red.

Una vez que haga clic en Continuar desde la pantalla de falla del instalador principal (Figura 4.26, " Paso de instalación Falló "[página 96]), volverá a una pantalla que normalmente nunca verá (el Principal
Menú que se muestra en la Figura 4.28, " Menú principal del instalador "[Página 98]), que le permite iniciar
Un paso de instalación tras otro. Si logró solucionar el problema a través del acceso de shell
(¡felicidades!), entonces puede volver a intentar el paso que falló.

Figura 4.28 *Menú principal del instalador*

Si no puede resolver el problema, puede presentar un informe de error. El informe debe luego incluya los registros del instalador, que puede recuperar con "Guardar registros de depuración" del menú principal función. Ofrece múltiples formas de exportar los registros, como se muestra en la Figura 4.29, " Guardar registros de depuración (1/2)"[Página 99].

Figura 4.29 *Guardar registros de depuración (1/2)*

Page 126

El método más conveniente, y el que recomendamos, es dejar que el instalador inicie una web
servidor que aloja los archivos de registro (Figura 4.30 , “ Guardar registros de depuración (2/2) ” [página 100]). Luego puedes iniciar
un navegador desde otra computadora en la misma red y descargue todos los archivos de registro y la pantalla
tomas que ha tomado con el botón Captura de pantalla disponible en cada pantalla.

Figura 4.30 *Guardar registros de depuración (2/2)*

4.6. Resumen

En este capítulo, nos centramos en el proceso de instalación de Kali Linux. Discutimos el mini- de Kali Linux
requisitos de instalación de mamá, el proceso de instalación para el sistema de archivos estándar y totalmente cifrado
Tems, preseeding, que permite instalaciones desatendidas, cómo instalar Kali Linux en varios ARM
dispositivos y qué hacer en el raro caso de una falla de instalación.

Consejos resumidos:

Page 127

- Los requisitos de instalación para Kali Linux varían de un servidor SSH básico sin escritorio,
  tan poco como 128 MB de RAM (se recomiendan 512 MB) y 2 GB de espacio en disco, para el *kali- de* gama *alta*
  meta-paquete *linux-full* , con al menos 2048 MB de RAM y 20 GB de espacio en disco. Adicionalmente,

su máquina debe tener una CPU compatible con al menos uno de los amd64, i386, armel, armhf,
o arquitecturas arm64.

- Kali se puede instalar fácilmente como el sistema operativo principal, junto con otros sistemas operativos.
  a través de particionamiento y modificación del cargador de arranque, o como una máquina virtual.
- Para garantizar la confidencialidad de sus datos, puede configurar particiones cifradas. Esta voluntad
  proteja sus datos si pierde o le roban su computadora portátil o disco duro.
- El instalador también se puede automatizar mediante debconf preseeding, una función que le permite
  para proporcionar respuestas desatendidas a las preguntas de instalación.
- Un archivo preestablecido es un archivo de texto sin formato en el que cada línea contiene la respuesta a un Debconf
  pregunta. Una línea se divide en cuatro campos separados por espacios en blanco (espacios o pestañas). Usted puede
  respuestas predeterminadas al instalador con parámetros de arranque, con un archivo predeterminado en initrd, con un
  archivo preestablecido en el medio de arranque o con un archivo preestablecido de la red.
- Kali Linux se ejecuta en una amplia variedad de dispositivos basados en ARM, como computadoras portátiles, computadoras integradas
  ers, y juntas de desarrolladores. La instalación del BRAZO es bastante sencilla. Descargar el apropiado
  imagen, grábelo en una tarjeta SD, unidad USB o mod de controlador multimedia integrado (eMMC)
  ule, conéctelo, inicie el dispositivo ARM, encuentre su dispositivo en la red, inicie sesión y cambie el
  Contraseña SSH y claves de host SSH.
- Puede depurar instalaciones fallidas con consolas virtuales (accesibles con CTRL + Shift y
  teclas de función), debconf-get y debconf-set , leyendo el / var / log / syslog
  archivo de registro, orbysubtingabugreportwithlogfilesrecuperadocon el instalador "Savedebug"
  función de registros ".

Ahora que hemos discutido los fundamentos de Linux y la instalación de Kali Linux, hablemos de la configuración
ración para que pueda comenzar a adaptar Kali para satisfacer sus necesidades.

Palabras clave

Red
Usuarios y grupos
Servicios
apache
PostgreSQL
SSH

Capítulo

5 Configurar Kali Linux

Contenido

Configurar la red 104
Gestión de usuarios de Unix y grupos de Unix 107
Configuración de servicios 109
Gestión de servicios 117
Resumen 119

En este capítulo, veremos varias formas en que puede configurar Kali Linux. Primero, en segundos sección 5.1 , " Configuración de la red "[Página 104], le mostraremos cómo configurar su red configuraciones utilizando un entorno gráfico y la línea de comandos. En la sección 5.2 , " Gestión de Unix Usuarios y grupos de Unix "[Página 107], hablaremos sobre usuarios y grupos, mostrándole cómo crear Comió y modificó cuentas de usuario, estableció contraseñas, deshabilitó cuentas y administró grupos. Finalmente nosotros discutirá los servicios en la sección 5.3, " Configuración de servicios "[Página 109] y explica cómo configurar y mantener servicios genéricos y también centrarse en tres servicios muy importantes y específicos: SSH, PostgreSQL y Apache.

5.1. Configurando la red

5.1.1 En el escritorio con *NetworkManager*

En una instalación de escritorio típica, ya tendrá instalado *NetworkManager* y se puede controlar trolleda y configurada a través del control de GNOME y a través de las menús de arriba a la derecha mostradas en la figura 5.1, " Pantalla de configuración de red "[Página 104].

Figura 5.1 *Pantalla de configuración de red*

La configuración de red predeterminada se basa en DHCP para obtener una dirección IP, un servidor DNS y una puerta de enlace. manera, pero puede usar el icono de engranaje en la esquina inferior derecha para alterar la configuración en muchos formas (por ejemplo: establecer la dirección MAC, cambiar a una configuración estática, habilitar o deshabilitar IPv6 y agregar rutas adicionales). Puede crear perfiles para guardar múltiples configuraciones de red cableadas y cambiar fácilmente entre ellos. Para las redes inalámbricas, sus configuraciones están automáticamente vinculadas a sus Identificador público (SSID).

NetworkManager también maneja conexiones por banda ancha móvil (red inalámbrica de área amplia WWAN) y por módems utilizando el protocolo punto a punto sobre ethernet (PPPoE). Por último, si bien no menos importante, Proporciona integración con muchos tipos de redes privadas virtuales (VPN) a través de plugins dedicados ginebras: SSH, OpenVPN, Cisco's VPNC, PPTP, Strongswan. Echa un vistazo a los paquetes *network-manager-* * ; la mayoría de ellos no están instalados por defecto. Tenga en cuenta que necesita los paquetes con el sufijo -gnome para poder configurarlos a través de la interfaz gráfica de usuario.

5.1.2. En la línea de comando con Ifupdown

Alternativamente, cuando prefiera no usar (o no tenga acceso a) un escritorio gráfico, puede configurar la red con el paquete *ifupdown* ya instalado , que incluye el ifup y herramientas de ifdown . Estas herramientas leen definiciones del archivo de configuración / etc / network / interfaces y están en el corazón del script de inicio /etc/init.d/networking que configura la red en

tiempo de arranque

Cada *dispositivo de red administrado por* ifupdown se *puede* configurar en *cualquier* momento con ifdown network-*dispositivo* . Luego puede modificar / etc / network / interfaces y recuperar la red (con la nueva configuración) con ifup *network-device* .

Analicemos lo que podemos encontrar en el archivo de configuración de Downdown. Hay dos directivas: *dispositivo de red* automático , que indica *ifupdown para* configurar *automáticamente la* interfaz de *red una* vez está disponible e iface *el dispositivo de red inet / inet6* para configurar una interfaz determinada. Por ejemplo, una configuración DHCP simple se ve así:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Tenga en cuenta que la configuración especial para el dispositivo de bucle invertido siempre debe estar presente en este archivo. Para una configuración de dirección IP fija, debe proporcionar más detalles, como la dirección IP, el red y la IP de la puerta de enlace:


```
auto eth0
iface eth0 inet static
    dirección 192.168.0.3
    máscara de red 255.255.255.0
    transmitida 192.168.0.255
    red 192.168.0.0
    Gateway 192.168.0.1
```

Para las interfaces inalámbricas, debe tener el paquete *wpasupplicant* (incluido en Kali por defecto), que proporciona muchas opciones de wpa- * que se pueden usar en / etc / network / interfaces . Echar un vistazo en /usr/share/doc/wpasupplicant/README.Debian.gz para ejemplos y explicaciones. los Las opciones más comunes son wpa-ssid (que define el nombre de la red inalámbrica para unirse) y wpa-psk (que define la frase de contraseña o la clave que protege la red).

```
iface wlan0 inet dhcp
    wpa-ssid MyNetWork
    wpa-psk plaintextsecret
```

5.1.3. En la línea de comando con *systemd-networkd*

Mientras *ifupdown* es la herramienta histórica utilizada por Debian, y mientras sigue siendo el valor predeterminado para el servidor o En otras instalaciones mínimas, hay una herramienta más nueva que vale la pena considerar: *systemd-networkd* . Su inte- La integración con el sistema *systemd* init lo convierte en una opción muy atractiva. No es específico de Debian- distribuciones basadas (al contrario de *ifupdown*) y ha sido diseñado para ser muy pequeño, eficiente y relativamente fácil de configurar si comprende la sintaxis de los archivos de la unidad systemd. Esto es especialmente opción atractiva si considera que *NetworkManager está* hinchado y es difícil de configurar.

Puede configurar systemd-networkd colocando archivos .network en / etc / systemd / network / di- casa del párroco. Alternativamente, puede usar / lib / systemd / network / forpackagedfilesor / run / systemd / red / para archivos generados en tiempo de ejecución. El formato de esos archivos está documentado en systemd. red (5) . La sección Match indica las interfaces de red a las que se aplica la configuración. Puede especificar la interfaz de muchas maneras, incluso por dirección de control de acceso a medios (MAC) o tipo de dispositivo. La sección Red define la configuración de la red.

Ejemplo 5.1 *Configuración basada en DHCP en /etc/systemd/network/80-dhcp.network*

```
[Partido]
Nombre = en *

[Red]
DHCP = sí
```

Ejemplo 5.2 *Configuración estática en* /etc/systemd/network/50-static.network

```
[Partido]
Nombre = enp2s0

[Red]
Dirección = 192.168.0.15 / 24
Gateway = 192.168.0.1
DNS = 8.8.8.8
```

Tenga en cuenta que system-networkd está deshabilitado de forma predeterminada, por lo que si desea usarlo, debe habilitarlo. También depende del sistema resuelto para la integración adecuada de la resolución DNS, que a su vez requiere que reemplace /etc/resolv.conf con un enlace simbólico a / run / systemd / resolve / resolv. conf , que es administrado por systemd-resolve .

```
# systemctl enable systemd-networkd
# systemctl enable systemd-resolve
# systemctl start systemd-networkd
# systemctl start systemd-resolve
# ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

Aunque systemd-networkd adolece de algunas limitaciones, como la falta de soporte integrado para redes inalámbricas, puede confiar en una configuración wpa_supplicant externa preexistente para soporte inalámbrico Sin embargo, es particularmente útil en contenedores y máquinas virtuales y fue desarrollado originalmente para entornos en los que la configuración de la red de un contenedor dependía La configuración de red de su host. En este escenario, systemd-networkd facilita la administración ambos lados de una manera consistente y al mismo tiempo compatible con todo tipo de dispositivos de red virtual que es posible que necesite en este tipo de escenario (consulte systemd.netdev (5)).

5.2. Gestión de usuarios de Unix y grupos de Unix

La base de datos de usuarios y grupos de Unix consta de los archivos de texto / etc / passwd (lista de usuarios), / etc / shadow (contraseñas cifradas de usuarios), / etc / group (lista de grupos) y / etc / gshadow (contraseñas cifradas de grupos). Sus formatos están documentados en passwd (5) , shadow (5) , group (5) y gshadow (5) respectivamente. Si bien estos archivos se pueden editar manualmente con herramientas como vipw y vigr , hay herramientas de nivel superior para realizar las operaciones más comunes.

5.2.1. Crear cuentas de usuario

Aunque Kali se ejecuta con mayor frecuencia mientras está autenticado como usuario root, es posible que deba crear cuentas de usuario no privilegiadas por varias razones, especialmente si está utilizando Kali como principal

sistema operativo. La forma más típica de agregar un usuario es con el comando adduser , que toma Un argumento obligatorio: el nombre de usuario para el nuevo usuario que desea crear.

El comando adduser hace algunas preguntas antes de crear la cuenta, pero su uso es bastante sencillo. Su archivo de configuración, /etc/adduser.conf , incluye muchas configuraciones interesantes. Puede, por ejemplo, definir el rango de identificadores de usuario (UID) que se pueden usar, dictar si o no, los usuarios comparten un grupo común o no, definen shells predeterminados y más.

La creación de una cuenta activa la población del directorio de inicio del usuario con los contenidos. de / etc / skel / template. Esto proporciona al usuario un conjunto de directorios y configuraciones estándar. archivos de uration.

En algunos casos, será útil agregar un usuario a un grupo (que no sea su grupo principal predeterminado) en Para otorgar permisos adicionales. Por ejemplo, un usuario que está incluido en el grupo *sudo* tiene privilegios administrativos completos a través del comando sudo . Esto se puede lograr con un comando como *el grupo de usuarios* adduser .

Usando getent para consultar la base de datos de usuarios El comando getent (obtener entradas) verifica las bases de datos del sistema (incluidas las de usuarios y grupos) usando las funciones de biblioteca apropiadas, que a su vez llaman al nombre módulos de conmutador de servicio (NSS) configurados en el archivo /etc/nsswitch.conf . El COMmand toma uno o dos argumentos: el nombre de la base de datos para verificar y un posible

clave de búsqueda. Por lo tanto, el comando getent passwd kaliuser1 devolverá la información
ción de la base de datos de usuarios con respecto al usuario kaliuser1 .

```
root @ kali: ~ # getent passwd kaliuser1
kaliuser1: x: 1001: 1001: usuario de Kali
        _ , 4444,123-867-5309,321-867-5309: / home / kaliuser1: / bin /
        _ bash
```

5.2.2. Modificar una cuenta o contraseña existente

Los siguientes comandos permiten modificar la información almacenada en campos específicos del usuario.
bases de datos:

- passwd: permite que un usuario normal cambie su contraseña, lo que a su vez actualiza / etc /
  archivo de sombra
- chfn - (CHangeFullName), reservadopara el superusuario (root), modifica el GECOS o "gen-
  campo de información oral ".
- chsh : (CHange SHell) cambia el shell de inicio de sesión del usuario. Sin embargo, las opciones disponibles serán limitadas
  ited a los que figuran en / etc / shells ; el administrador, por otro lado, no está obligado por
  esta restricción y puede configurar el shell para cualquier programa elegido.
- chage - (CHANge AGE) permite al administrador cambiar la configuración de caducidad de la contraseña
  pasando el nombre de usuario como argumento o enumerando la configuración actual utilizando la opción de *usuario* -l .

Alternativamente, también puede forzar la caducidad de una contraseña utilizando el *usuario* passwd -e
comando, que obliga al usuario a cambiar su contraseña la próxima vez que inicie sesión.

5.2.3. Deshabilitar una cuenta

Puede encontrar su necesidad de inhabilitar una cuenta (usuario bloqueado) como medida disciplinaria, por
los propósitos de una investigación, o simplemente en el caso de una ausencia prolongada o definitiva de un
usuario. Una cuenta deshabilitada significa que el usuario no puede iniciar sesión u obtener acceso a la máquina. La cuenta
permanece intacto en la máquina y no se eliminan archivos ni datos; Es simplemente inaccesible. Esto es
logrado mediante el comando passwd -l *usuario* (bloqueo). La reactivación de la cuenta se realiza en
de manera similar, con la opción -u (desbloquear).

5.2.4. Administrar grupos de Unix

Los comandos addgroup y delgroup agregan o eliminan un grupo, respectivamente. El groupmod com-
mand modifica la información de un grupo (su gid o identificador). El comando gpasswd *group* cambia
la contraseña para el grupo, mientras que el comando gpasswd -r *group la* elimina.

Trabajando con varios Grupos

Cada usuario puede ser miembro de muchos grupos. El grupo principal de un usuario es, por defecto,
creado durante la configuración inicial del usuario. Por defecto, cada archivo que crea un usuario
pertenece al usuario, así como al grupo principal del usuario. Esto no siempre es deseable;
por ejemplo, cuando el usuario necesita trabajar en un directorio compartido por otro grupo
que su grupo principal. En este caso, el usuario necesita cambiar grupos usando uno de los
siguientes comandos: newgrp , que inicia un nuevo shell, o sg , que simplemente ejecuta un
comando utilizando el grupo alternativo proporcionado. Estos comandos también permiten al usuario
unirse a un grupo al que no pertenecen actualmente. Si el grupo está protegido con contraseña,
deberán proporcionar la contraseña adecuada antes de ejecutar el comando.

Alternativamente, el usuario puede establecer el bit setgid en el directorio, lo que hace que se creen archivos.
en ese directorio pertenece automáticamente al grupo correcto. Para más detalles,
vea la barra lateral " directorio setgid y *bit fijo* " [página 58].

El comando id muestra el estado actual de un usuario, con su identificador personal
(variable uid), grupo principal actual (variable gid) y la lista de grupos a los que
pertenecer (grupos de variables).

5.3. Configurar servicios

En esta sección veremos los servicios (a veces llamados demonios) o los programas que se ejecutan como
un proceso en segundo plano y realizar diversas funciones para el sistema. Comenzaremos discutiendo
archivos de configuración y procederemos a explicar cómo algunos servicios importantes (como SSH, Post-

greSQL y Apache) y cómo se pueden configurar.

5.3.1. Configurar un programa específico

Cuando desee configurar un paquete desconocido, debe proceder por etapas. Primero deberías lea lo que el mantenedor del paquete ha documentado. El / usr / share / doc / *package* / README.

El archivo Debian es un buen lugar para comenzar. Este archivo a menudo contendrá información sobre el paquete, incluidos punteros que pueden remitirlo a otra documentación. A menudo te ahorrarás un mucho tiempo, y evite mucha frustración, leyendo primero este archivo, ya que a menudo detalla más Errores comunes y soluciones a los problemas más comunes.

A continuación, debe consultar la documentación oficial del software. Consulte la sección 6.1 , " Documen- Fuentes de tation "[Página 124] para obtener consejos sobre cómo encontrar diversas fuentes de documentación. El dpkg -L *El* comando *package* proporciona una lista de archivos incluidos en el paquete; por lo tanto, puede identificar rápidamente la documentación disponible (así como los archivos de configuración, ubicados en / etc /). Además, dpkg -s *el paquete* muestra el *paquete* de datos de datos y muestra cualquier posible *paquete* recomendado sugerido siglos; allí, puede encontrar documentación o quizás una utilidad que facilitará la configuración de El software.

Finalmente, los archivos de configuración a menudo están auto documentados por muchos comentarios explicativos detallados. ing los diversos valores posibles para cada ajuste de configuración. En algunos casos, puede obtener software en funcionamiento descomentando una sola línea en el archivo de configuración. En otros casos, ejemplos de los archivos de configuración se proporcionan en el directorio / usr / share / doc / *package* / examples / . Ellos puede servir como base para su propio archivo de configuración.

5.3.2. Configuración de SSH para inicios de sesión remotos

SSH le permite iniciar sesión de forma remota en una máquina, transferir archivos o ejecutar comandos. Es una industria pruebe la herramienta estándar (ssh) y el servicio (sshd) para conectarse a máquinas de forma remota.

Si bien el paquete *openssh-server* está instalado de manera predeterminada, el servicio *SSH* está deshabilitado de manera predeterminada y por lo tanto no se inicia en el momento del arranque. Puede iniciar manualmente el servicio SSH con systemctl start ssh o configúrelo para que se inicie en el momento del arranque con systemctl enable ssh .

El servicio SSH tiene una configuración predeterminada relativamente sana, pero dadas sus potentes capacidades y naturaleza sensible, es bueno saber qué puede hacer con su archivo de configuración, / etc / ssh / sshd_ config . Todas las opciones están documentadas en sshd_config (5) .

La configuración predeterminada deshabilita los inicios de sesión basados en contraseña para el usuario root, lo que significa que usted primero debe configurar las claves SSH con ssh-keygen . Puede extender esto a todos los usuarios configurando Autenticación de contraseña a no, o puede levantar esta restricción cambiando PermitRootLogin a Sí (en lugar de la contraseña prohibida predeterminada). El servicio SSH escucha por defecto en el puerto 22 pero puede cambiar esto con la directiva Port.

Para aplicar la nueva configuración, debe ejecutar systemctl reload ssh .

Generando nuevo host SSH Llaves

Cada servidor SSH tiene sus propias claves criptográficas; se denominan "claves de host SSH" y se almacenan en / etc / ssh / ssh_host_ * . Deben mantenerse en privado si quieres confidencialidad y no deben ser compartidos por múltiples máquinas.

Cuando instala su sistema copiando una imagen de disco completa (en lugar de usar debian-instalador), la imagen puede contener claves de host SSH pregeneradas que, por lo tanto, debe reemplazar con claves recién generadas. La imagen probablemente también viene con un valor predeterminado contraseña de root que desea restablecer al mismo tiempo. Puedes hacer todo esto con el siguientes comandos:

```
# passwd
[...]
# rm / etc / ssh / ssh_host_ *
# dpkg-reconfigure openssh-server
# service ssh restart
```

5.3.3. Configurar bases de datos PostgreSQL

PostgreSQL es un servidor de base de datos. Raramente es útil por sí solo, pero es utilizado por muchos otros servicios para Almacenamiento de datos. Esos servicios generalmente accederán al servidor de la base de datos a través de la red y generalmente requieren credenciales de autenticación para poder conectarse. Configurar esos servicios requiere creando bases de datos PostgreSQL y cuentas de usuario con los privilegios apropiados en la base de datos. A para poder hacer eso, necesitamos que el servicio se esté ejecutando, así que comencemos con `systemctl start postgresql` .

Múltiples PostgreSQL versiones compatibles

El paquete PostgreSQL permite que múltiples versiones del servidor de bases de datos sean co-instalado También es posible manejar múltiples *clústeres* (un clúster es una colección de bases de datos atendidas por el mismo `postmaster`). Para lograr esto, los archivos de configuración se almacenan en `/etc/postgresql/`*version*`/`*cluster-name*`/` .

Para que los clústeres se ejecuten uno al lado del otro, a cada nuevo clúster se le asigna la próxima disponibilidad. número de puerto capaz (generalmente 5433 para el segundo clúster). El archivo `postgresql.service` es un shell vacío, por lo que es fácil actuar en todos los clústeres juntos ya que cada clúster tiene su unidad propia (`postgresql@`*versión*`-`*cluster*`.service`).

Tipo de conexión y autenticación de cliente

Por defecto, PostgreSQLlistenspara las conexiones entrantes en dos sentidos: en TCPport5432ofthelocal-interfaz de host y en socket basado en archivos `/var/run/postgresql/.s.PGSQL.5432` . Esto puede ser configurado en `postgresql.conf` con varias directivas: listen_addresses para las direcciones para escuchar a, puerto para el puerto TCP y unix_socket_directories para definir el directorio donde se basa el archivo Se crean enchufes.

Dependiendo de cómo se conectan, los clientes se autentican de diferentes maneras. El `pg_hba.conf` El archivo de configuración define quién puede conectarse en cada socket y cómo se autentican atendido De forma predeterminada, las conexiones en el socket basado en archivos utilizan la cuenta de usuario de Unix como nombre de el usuario de PosgreSQL, y supone que no se requiere más autenticación. En la conexión TCP Además, PostgreSQL requiere que el usuario se autentique con un nombre de usuario y una contraseña (aunque no Nombre de usuario / contraseña de Unix, sino más bien uno administrado por PostgreSQL).

El usuario postgres es especial y tiene privilegios administrativos completos sobre todas las bases de datos. Usaremos esta identidad para crear nuevos usuarios y nuevas bases de datos.

Crear usuarios y bases de datos

El comando `createuser` agrega un nuevo usuario y `dropuser` elimina uno. Del mismo modo, el `creadob` El comando agrega una nueva base de datos y `dropdb` elimina una. Cada uno de estos comandos tiene su propio páginas del manual, pero discutiremos algunas de las opciones aquí. Cada comando actúa de manera predeterminada clúster (que se ejecuta en el puerto 5432) pero puede pasar --port = *puerto* para modificar usuarios y bases de datos de un clúster alternativo.

Estos comandos deben conectarse al servidor PostgreSQL para convertir su banda en el símbolo de belleza. clasificado como un usuario con privilegios suficientes para poder ejecutar la operación especificada. Lo más fácil La forma de lograr esto es usar la cuenta de Postgres Unix y conectarse a través del socket basado en archivos:

```
# su - postgres
$ createuser -P king_phisher
Ingrese la contraseña para el nuevo rol:
Ingrese de nuevo:
$ createdb -T template0 -E UTF-8 -O king_phisher king_phisher
$ salida
```

En el ejemplo anterior, la opción -P le pide a `createuser` que `solicite` una contraseña una vez que crea el nuevo usuario de king_phisher. Mirando el `comando createdb` , el -O define al usuario propietario del nueva base de datos (que tendrá todos los derechos para crear tablas y otorgar permisos, etc.). También queremos poder usar cadenas Unicode, por lo que agregamos la opción -E UTF-8 para establecer la codificación, lo que a su vez requiere que usemos la opción -T para elegir otra plantilla de base de datos.

Ahora podemos probar que podemos conectarnos a la base de datos a través del socket escuchando en localhost (-h localhost) como el usuario king_phisher (-U king_phisher):

```
# psql -h localhost -U king_phisher king_phisher
Contraseña para el usuario king_phisher:
psql (9.5.2)
```

```
Conexión SSL (protocolo: TLSv1.2, cifrado: ECDHE-RSA-AES256-GCM-SHA384, bits: 256,
        compresión: apagado)
Escriba "ayuda" para obtener ayuda.

king_phisher =>
```


Como puede ver, la conexión fue exitosa.

Administrar clústeres de PostgreSQL

Primero, vale la pena señalar que el concepto de "clúster PostgreSQL" es una adición específica de Debian y que no encontrará ninguna referencia a este término en la documentación oficial de PostgreSQL. Desde Desde el punto de vista de las herramientas de PostgreSQL, dicho clúster es solo una instancia de un servidor de base de datos corriendo en un puerto específico.

Dicho esto, el paquete *postgresql-common de* Debian proporciona múltiples herramientas para gestionar tales racimos: pg_createcluster , pg_dropcluster , pg_ctlcluster , pg_upgradecluster , pg_renamecluster y pg_lsclusters . No cubriremos todas esas herramientas aquí, pero puedes consulte sus respectivas páginas de manual para obtener más información.

Lo que debe saber es cuando hay una nueva versión de PostgreSQLgets instalado en nuestro sistema, creará un nuevo clúster que se ejecutará en el siguiente puerto (generalmente 5433) y seguirá utilizando la versión anterior hasta que migre sus bases de datos del clúster antiguo al nuevo.

Puede recuperar una lista de todos los clústeres y su estado con pg_lsclusters . Más importante de manera instantánea, puede automatizar la migración de su clúster a la última versión de PostgreSQL con pg_upgradecluster *nombre de clúster de la versión anterior* . Para que esto tenga éxito, es posible que primero tengas que eliminar el clúster (vacío) creado para la nueva versión (con pg_dropcluster *new-version nombre del clúster*). El clúster anterior no se descarta en el proceso, pero tampoco se iniciará Tomaticamente. Puede soltarlo una vez que haya verificado que el clúster actualizado funciona bien.

5.3.4. Configurando Apache

Una instalación típica de Kali Linux incluye el servidor web Apache, proporcionado por el paquete *apache2* . Al ser un servicio de red, está deshabilitado por defecto. Puede iniciar manualmente con systemctl start apache2 .

Con más y más aplicaciones distribuidas como aplicaciones web, es importante tener algún conocimiento de Apache para alojar esas aplicaciones, ya sea para uso local o para haciéndolos disponibles a través de la red.

Apache es un servidor modular y muchas funciones son implementadas por módulos externos que El programa principal se carga durante su inicialización. La configuración predeterminada solo permite la mayoría módulos comunes, pero habilitar nuevos módulos se realiza fácilmente ejecutando un *módulo* a2enmod . Utilizar *Módulo* a2dismod para deshabilitar un módulo. Estos programas en realidad solo crean (o eliminan) símbolos enlaces en / etc / apache2 / mods-enabled / , apuntando a los archivos reales (almacenados en / etc / apache2 / Mods-disponible /).

Hay muchos módulos disponibles, pero vale la pena considerar dos: PHP y SSL. Web ap- Las aplicaciones escritas con PHP son ejecutadas por el servidor web Apache con la ayuda de

módulo proporcionado por el *paquete libapache-mod-php* , y su instalación habilita automáticamente el módulo.

Apache2.4 incluye el módulo SSL requerido para asegurar HTTP (HTTPS) fuera de la caja. Primero necesita para habilitarse con a2enmod ssl , entonces las directivas requeridas deben agregarse a la configuración archivos. Se proporciona un ejemplo de configuración en / etc / apache2 / sites-available / default-ssl. conf . Consulte http://httpd.apache.org/docs/2.4/mod/mod_ssl.html para obtener más información.

ThefulllistofstandardApachemodulescanbefoundonlineat http://httpd.apache.org/docs/ 2.4 / mod / index.html .

Con su configuración predeterminada, el servidor web escucha en el puerto 80 (como está configurado en / etc / apache2 /

ports.conf), y sirve páginas del directorio / var / www / html / de forma predeterminada (como está configurado en /etc/apache2/sites-enabled/000-default.conf).

Configurar hosts virtuales

Un host virtual es una identidad adicional para el servidor web. El mismo proceso de Apache puede servir para múltiples sitios web (por ejemplo, www.kali.org y www.offensive-security.com) porque las solicitudes HTTP se insertan tanto el nombre del sitio web solicitado como la parte local de la URL (esta función se conoce como *basada en el nombre anfitriones virtuales*).

La configuración predeterminada para Apache 2 habilita hosts virtuales basados en nombres. Además, un valor predeterminado el host virtual se define en el archivo /etc/apache2/sites-enabled/000-default.conf; este host virtual lo hará se utilizará si no se encuentra ningún host que coincida con la solicitud enviada por el cliente.

Importante

Las solicitudes relacionadas con hosts virtuales desconocidos siempre serán atendidas por primer host virtual definido, por lo que el paquete incluye un valor predeterminado de 000.

archivo de configuración conf , que clasifica por primera vez entre todos los demás archivos que podría crear.

Luego, cada host virtual adicional se describe mediante un archivo almacenado en / etc / apache2 / sites-available / . El archivo generalmente lleva el nombre del nombre de host del sitio web seguido de un sufijo .conf (por ejemplo: www.example.com.conf). Puede habilitar el nuevo host virtual con un ejemplo de sitio web www.2. com . Aquí hay una configuración mínima de host virtual para un sitio web cuyos archivos se almacenan en / srv / www. example.com/www/ (definido con la opción DocumentRoot):

```
<VirtualHost *: 80>
ServerName www.example.com
ServerAlias example.com
```



```
DocumentRoot /srv/www.example.com/www
</VirtualHost>
```

También puede considerar agregar directivas CustomLog y ErrorLog para configurar Apache para la salida inicia sesión en archivos dedicados al host virtual.

Directivas Comunes

Esta sección revisa brevemente algunas de las directivas de configuración de Apache comúnmente utilizadas.

El archivo de configuración principal generalmente incluye varios bloques de Directorio; permiten especificar comportamientos diferentes para el servidor dependiendo de la ubicación del archivo que se está sirviendo. Tal bloque comúnmente incluye opciones y directivas AllowOverride:

```
<Directorio / var / www>
Las opciones incluyen FollowSymLinks
Permitir anular todo
DirectoryIndex index.php index.html index.htm
</Directory>
```

La directiva DirectoryIndex contiene una lista de archivos para probar cuando la solicitud del cliente coincide con un directorio conservador. El primer archivo existente en la lista se usa y se envía como respuesta.

La directiva Opciones está seguida de una lista de opciones para habilitar. El valor Ninguno deshabilita todas las opciones; correspondientemente, All los habilita a todos excepto a MultiViews. Las opciones disponibles incluyen:

- ExecCGI: indica que se pueden ejecutar scripts CGI.
- FollowSymLinks: le dice al servidor que se pueden seguir los enlaces simbólicos y que la respuesta debe contener el contenido del objetivo de dichos enlaces.
- SymLinksIfOwnerMatch: también le dice al servidor que siga enlaces simbólicos, pero solo cuando link y su objetivo tienen el mismo propietario.
- Incluye: habilita las *inclusiones del lado del servidor* (SSI). Estas son directivas incrustadas en páginas HTML y ejecutado sobre la marcha para cada solicitud.
- Índices: le dice al servidor que enumere el contenido de un directorio si la solicitud HTTP enviada por

el cliente apunta a un directorio sin un archivo de índice (es decir, cuando no hay archivos mencionados por el La directiva DirectoryIndex existe en este directorio).

- MultiViews: permite la negociación de contenido; esto puede ser usado por el servidor para devolver una web página que coincide con el idioma preferido configurado en el navegador.

Requerir autenticación En algunas circunstancias, el acceso a parte de un sitio web debe ser requerido estricto, por lo que solo los usuarios legítimos que proporcionan un nombre de usuario y una contraseña tienen acceso a los contenidos.

Página 142

El archivo .htaccess contiene directivas de configuración de Apache aplicadas cada vez que una solicitud confirma se refiere a un elemento del directorio donde se almacena el archivo .htaccess . Estas directivas son recursiva, ampliando el alcance a todos los subdirectorios.

La mayoría de las directivas que pueden ocurrir en un bloque de Directorio también son legales en un archivo .htaccess . los La directiva AllowOverride enumera todas las opciones que se pueden habilitar o deshabilitar mediante .htaccess . Un uso común de esta opción es restringir ExecCGI, de modo que el administrador elija qué usuarios pueden ejecutar programas bajo la identidad del servidor web (el usuario de www-data).

Ejemplo 5.3 *.htaccess Archivo que requiere autenticación*

```
Requerir usuario válido
AuthName "Directorio privado"
AuthType Basic
AuthUserFile / etc / apache2 / authfiles / htpasswd-private
```

Autenticación Básica No ofrece seguridad El sistema de autenticación utilizado en el ejemplo anterior (Básico) tiene una seguridad mínima ya que la contraseña se envía en texto claro (solo se codifica como *base64* , que es un simple codificación en lugar de un método de cifrado). También debe tenerse en cuenta que el docu- Los elementos protegidos por este mecanismo también pasan por la red de forma clara. Si la seguridad es importante, toda la sesión HTTP debe estar encriptada con Transport Layer Se- Curity (TLS).

El archivo / etc / apache2 / authfiles / htpasswd-private contiene una lista de usuarios y contraseñas; eso comúnmente se manipula con el comando htpasswd . Por ejemplo, el siguiente comando es Se utiliza para agregar un usuario o cambiar su contraseña:

```
# htpasswd / etc / apache2 / authfiles / htpasswd-private user
Nueva contraseña:
Reescriba nueva contraseña:
Agregar contraseña para usuario usuario
```

Restricción de acceso La directiva Requerir controla las restricciones de acceso para un directorio (y su subdirectorios, recursivamente).

Se puede utilizar como acceso restringido basado en muchos criterios; vamos a dejar de describir la restricción de acceso basado en la dirección IP del cliente, pero se puede hacer mucho más potente que eso, especialmente cuando se combinan varias directivas Require dentro de un bloque RequireAll.

Por ejemplo, puede restringir el acceso a la red local con la siguiente directiva:

```
Requiere ip 192.168.0.0/16
```


Page 143

5.4. Servicios de gestion

Kali usa systemd como su sistema de inicio, que no solo es responsable de la secuencia de arranque, sino también actúa permanentemente como un administrador de servicios con todas las funciones, iniciando y monitoreando servicios.

systemd se puede consultar y controlar con systemctl . Sin ningún argumento, ejecuta el El comando systemctl list-units , que genera una lista de las *unidades* activas . Si ejecuta systemctl

estado , la salida muestra una descripción jerárquica de los servicios en ejecución. Comparando ambos
pone, inmediatamente ve que hay multiples tipos de unidades y que los servicios son solo uno
entre ellos.

Cada servicio está representado por una *unidad de servicio* , que se describe mediante un archivo de servicio enviado generalmente en
/ lib / systemd / system / (o / run / systemd / system / , o / etc / systemd / system / ; están listados
aumentando el orden de importancia, y el último gana). Cada uno es posiblemente modificado por otro
nombre-servicio .service.d / *. conf archivos en el mismo conjunto de directorios. Esos archivos unitarios son simples
archivos de texto cuyo formato está inspirado en los conocidos archivos "* .ini" de Microsoft Windows, con *clave*
= pares de *valores* agrupados entre encabezados [*sección*]. Aquí vemos un archivo de servicio de muestra para / lib /
systemd / system / ssh.service :

```
[Unidad]
Descripción = servidor OpenBSD Secure Shell
Después = network.target auditd.service
ConditionPathExists =! / Etc / ssh / sshd_not_to_be_run

[Servicio]
EnvironmentFile = - / etc / default / ssh
ExecStart = / usr / sbin / sshd -D $ SSHD_OPTS
ExecReload = / bin / kill -HUP $ MAINPID
KillMode = proceso
Reinicio = en caso de falla
RestartPreventExitStatus = 255
Tipo = notificar

[Instalar en pc]
WantedBy = multi-user.target
Alias = sshd.service
```

Las unidades objetivo son otra parte del diseño de systemd. Representan un estado deseado que desea
obtenerintermsofunctivatedunits (lo que significa un servicio de configuración en el caso de las unidades de servicio). Ellos
existen principalmente lejos del grupo de dependencias en otras unidades. Cuando el sistema comienza, permite
unidades requeridas para alcanzar el default.target (que se enlaza simbólicamente a graphical.target , y que
a su vez depende de multi-user.target). Entonces todas las dependencias de esos objetivos se activan
durante el arranque

Dichas dependencias se expresan con la directiva wants en la unidad de destino. Pero no tienes
para editar la unidad de destino para agregar nuevas dependencias, también puede crear un enlace simbólico que apunte al

dependienteunidaden el directorio / etc / systemd / system / *target-name* .target.wants / . Y esto es
exactamente lo que hace systemctl enable *foo.service* . Cuando el servicio se puede habilitar, usted cuenta con el sistema
para agregar una dependencia en los destinos enumerados en la entrada WantedBy de la sección [Instalar] de la
archivo de servicio Por el contrario, systemctl deshabilita *foo.service* dropsthesamesymlinkandthus
La dependencia.

Los comandos habilitar y deshabilitar no cambian nada con respecto al estado actual de la
servicios. Solo influyen en lo que sucederá en el próximo arranque. Si quieres ejecutar el servicio
inmediatamente, debe ejecutar systemctl start *foo.service* . Por el contrario, puedes detenerlo
con systemctl stop *foo.service* . También puede inspeccionar el estado actual de un servicio con
systemctl status *foo.service* , que incluye de manera útil las últimas líneas del registro asociado.
Después de haber cambiado la configuración de un servicio, es posible que desee volver a cargarlo o reiniciarlo:
esas operaciones se realizan con systemctl reload *foo.service* y systemctl restart *foo.*
servicio respectivamente.

```
# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Cargado: cargado (/lib/systemd/system/postgresql.service; deshabilitado; proveedor preestablecido:
              ¯ deshabilitado)
     Activo: inactivo (muerto)
# ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service
ls: no se puede acceder a '/etc/systemd/system/multi-user.target.wants/postgresql.service': No
          ¯ tal archivo o directorio
# systemctl enable postgresql
[...]
# ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service
lrwxrwxrwx 1 root root 38 abr 21 16:21 /etc/systemd/system/multi-user.target.wants/
          ¯ postgresql.service -> /lib/systemd/system/postgresql.service
# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Cargado: cargado (/lib/systemd/system/postgresql.service; activado; proveedor preestablecido:
              ¯ deshabilitado)
```

```
     Activo: inactivo (muerto)
# systemctl start postgresql
# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Cargado: cargado (/lib/systemd/system/postgresql.service; activado; proveedor preestablecido:
              deshabilitado)
     Activo: activo (salido) desde jue 2016-04-21 16:22:29 EDT;  Hace 2s
    Proceso: 6355 ExecStart = / bin / true (código = salido, estado = 0 / ÉXITO)
  PID principal: 6355 (código = salido, estado = 0 / ÉXITO)

21 de abril 16:22:29 kali-rolling systemd [1]: Inicio de PostgreSQL RDBMS ...
21 de abril 16:22:29 kali-rolling systemd [1]: Iniciado PostgreSQL RDBMS.
```


Page 145

5.5. Resumen

En este capítulo, aprendimos cómo configurar Kali Linux. Configuramos la configuración de red, hablamos sobre usuarios y grupos, y discutió cómo crear y modificar cuentas de usuario, establecer contraseñas, deshabilitar cuentas y administrar grupos. Finalmente, discutimos los servicios y explicamos cómo configurar y mantener servicios genéricos, específicamente SSH, PostgreSQL y Apache.

Consejos resumidos:

- En una instalación de escritorio típica, ya tendrá instalado *NetworkManager* y puede ser controlado y configurado a través del centro de control de GNOME y a través de la esquina superior derecha menú.
- Puede configurar la red desde la línea de comando con las herramientas `ifup` e `ifdown`, que leen sus instrucciones del archivo de configuración `/ etc / network / interfaces`. Un herramienta aún más nueva, *systemd-networkd* funciona con el sistema *systemd* init.
- Por defecto, la base de datos de usuarios y grupos de Unix consta de los archivos de texto `/ etc / passwd` (listofusers), `/ etc / shadow` (encryptedpasswordsofusers), `/ etc / group` (listofgroups), y `/ etc / gshadow` (contraseñas cifradas de grupos).
- Puede usar el comando `getent` para consultar la base de datos del usuario y otras bases de datos del sistema.
- El comando `adduser` hace algunas preguntas antes de crear la cuenta, pero es un forma de crear una nueva cuenta de usuario.
- Se pueden usar varios comandos para modificar campos específicos en la base de datos del usuario, incluidos: `passwd` (cambiar contraseña), `chfn` (cambiar nombre completo y GECOS, o información general) campo de acción), `chsh` (cambiar el shell de inicio de sesión), `chage` (cambiar la antigüedad de la contraseña) y `passwd -e` *usuario* (obliga al usuario a cambiar su contraseña la próxima vez que inicie sesión).
- Cada usuario puede ser miembro de uno o varios grupos. Se pueden usar varios comandos para modificar la identidad del grupo: `newgrp` cambia la ID del grupo actual, `sg` ejecuta un comando usando En el grupo de suministros alternativo, estos bits pueden ser reemplazados en un directorio, causando archivos creados en ese directorio para pertenecer automáticamente al grupo correcto. Además, el comando `id` muestra el estado actual de un usuario, incluida una lista de miembros de su grupo.
- Puede iniciar SSH manualmente con `systemctl start ssh` o habilitarlo permanentemente con `systemctl habilita ssh`. La configuración predeterminada deshabilita los inicios de sesión basados en contraseña para usuario root, lo que significa que primero debe configurar las claves SSH con `ssh-keygen`.
- PostgreSQL es un servidor de base de datos. Rara vez es útil por sí solo, pero es utilizado por muchos otros servicios para almacenar datos.
- Una instalación típica de Kali Linux incluye el servidor web Apache, proporcionado por *apache2* paquete. Al ser un servicio de red, está deshabilitado de forma predeterminada. Puede comenzarlo manualmente con `systemctl inicia apache2`.

Page 146

- Con su configuración predeterminada, Apache escucha en el puerto 80 (como está configurado en `/ etc / apache2 / ports.conf`), y sirve páginas desde el directorio `/ var / www / html /` por defecto (como configurado en `/etc/apache2/sites-enabled/000-default.conf`).

Ahora que hemos abordado los fundamentos de Linux y la instalación y configuración de Kali Linux, vamos a discuta cómo solucionar problemas de Kali y le enseñe algunas herramientas y trucos para que vuelva a funcionar Ning cuando te encuentras con problemas.

Palabras clave

Documentación
El
Canal IRC
Informe de error

Capítulo

6 Ayudándote a ti mismo y 6 Obteniendo ayuda

Contenido

Fuentes de documentación 124 Comunidades Kali Linux 128 Presentación de un buen informe de error 129 Resumen 146

No importa cuántos años de experiencia tenga, no hay duda de que, tarde o temprano, usted
Encontrará un problema. Resolver ese problema es a menudo una cuestión de entenderlo y
luego aprovechando varios recursos para encontrar una solución o solución alternativa.

En este capítulo, analizaremos las diversas fuentes de información disponibles y analizaremos las mejores
estrategias para encontrar la ayuda que necesita o la solución a un problema que podría estar enfrentando. Lo haremos
también escriba una tecla sobre algunos de los recursos de la comunidad Kali Linux disponibles, incluido el sitio web
foros y canal de Internet Relay Chat (IRC). Por último, presentaremos informes de errores y mostraremos
cómo aprovechar los sistemas de archivo de errores para solucionar problemas y diseñar estrategias
para ayudarlo a presentar su propio informe de errores para que los problemas no documentados puedan manejarse rápidamente y
efectivamente.

6.1. Fuentes de documentación

Antes de que pueda entender lo que realmente está sucediendo cuando hay un problema, necesita saber
papel teórico desempeñado por cada programa involucrado en el problema. Una de las mejores formas de hacer esto.
es revisar la documentación del programa. Comencemos discutiendo dónde, exactamente, puedes encontrar
documentación ya que a menudo se encuentra dispersa.

Cómo evitar RTFM Respuestas

Este acrónimo significa "leer el manual de mierda", pero también se puede ampliar en un variante más amigable, "lea el excelente manual". Esta frase a veces se usa en (conciso) respuestas a preguntas de novatos. Es bastante abrupto y traiciona un cierto molesto por una pregunta hecha por alguien que ni siquiera se ha molestado en leer el documentación. Algunos dicen que esta respuesta clásica es mejor que ninguna respuesta ya que esto al menos insinúa que la respuesta se encuentra dentro de la documentación.

Cuando publique preguntas, no se ofenda necesariamente Respuesta de RTFM, pero haz lo que puedas para al menos demostrar que te has tomado el tiempo investigar un poco antes de publicar la pregunta; menciona las fuentes que tienes consultado y describa los diversos pasos que ha tomado personalmente para encontrar información mation. Esto demostrará que no eres flojo y que realmente estás buscando conocimiento. Seguir las pautas de Eric Raymond es una buena manera de evitar errores comunes y obtener respuestas útiles.

[2] http://catb.org/~esr/faqs/smart-questions.html

6.1.1. Páginas del manual

Las páginas de manual, aunque de estilo relativamente breve, contienen una gran cantidad de información esencial. A ver una página de manual, simplemente escriba `man *manual-page*`. La página del manual generalmente coincide con el nombre del comando Por ejemplo, para conocer las posibles opciones para el comando `cp`, debería escriba `man cp` en el símbolo del sistema.

Las páginas del manual no son solo programas de documentos accesibles desde la línea de comandos, sino también la configuración archivos, llamadas al sistema, funciones de la biblioteca C, etc. A veces los nombres pueden colisionar. Por ejemplo,

El comando de `lectura` del shell tiene el mismo nombre que la llamada al sistema de `lectura`. Por eso las páginas del manual están organizados en las siguientes secciones numeradas:

1. Comandos que se pueden ejecutar desde la línea de comando
2. Llamadas del sistema (funciones proporcionadas por el núcleo)
3. Funciones de la biblioteca (proporcionadas por las bibliotecas del sistema)
4. Dispositivos (en sistemas tipo Unix, estos son archivos especiales, generalmente ubicados en el directorio `/ dev /`)
5. Archivos de configuración (formatos y convenciones)
6. Juegos
7. Conjuntos de macros y estándares.
8. Comandos de administración del sistema
9. rutinas del núcleo

Puede especificar la sección del documento manual que está buscando: para ver la documentación para la llamada al sistema de `lectura`, debe escribir `man 2 read`. Cuando no se especifica explícitamente ninguna sección, el Se mostrará la primera sección que tiene una página de manual con el nombre solicitado. Así, `hombre sombra` devuelve `shadow (5)` porque no hay páginas de manual para *shadow* en las secciones 1–4.

Por supuesto, si no conoce los nombres de los comandos, el manual no será muy útil. utilízalo Ingrese el comando `apropos`, que busca páginas de manual (o más específicamente su descripciones cortas) para cualquier palabra clave que proporcione. El comando `apropiado` luego devuelve un

lista de páginas del manual cuyo resumen menciona las palabras clave solicitadas junto con la línea única resumen de la página del manual. Si elige bien sus palabras clave, encontrará el nombre de comando que necesitas.

Ejemplo 6.1 *Encontrar cp con apropos*

```
$ apropos "copiar archivo"
cp (1)                - copiar archivos y directorios
cpio (1)              - copiar archivos ay desde archivos
gvfs-copy (1)         - Copiar archivos
gvfs-move (1)         - Copiar archivos
hcopy (1)             - copiar archivos desde o hacia un volumen HFS
instalar (1)          - copiar archivos y establecer atributos
ntfscp (8)            - Copie el archivo a un volumen NTFS.
```

Documentación de navegación siguiendo enlaces

Muchas páginas del manual tienen una sección de "Ver también", generalmente cerca del final del documento, que se refiere a otras páginas del manual relevantes para comandos similares, o documentos externos umentación Puede usar esta sección para buscar documentación relevante incluso cuando La primera opción no es óptima.

Además de man , puede usar konqueror (en KDE) y yelp (en GNOME) para buscar páginas de manual como bien.

6.1.2. Documentos informativos

El proyecto GNU tiene manuales escritos para la mayoría de sus programas en formato de *información* ; es por eso que muchos Las páginas del manual se refieren a la documentación de *información* correspondiente . Este formato ofrece algunas ventajas. pero el programa predeterminado para ver estos documentos (también llamado información) es un poco más complejo. usted sería recomendable utilizar pinfo en su lugar (del paquete *pinfo*). Para instalarlo, simplemente ejecute apt actualización seguida de apt install pinfo (ver sección 8.2.2.2, " Instalación de paquetes con APT " [página 177]).

La documentación de *información* tiene una estructura jerárquica y si invoca pinfo sin parámetros, mostrará una lista de los nodos disponibles en el primer nivel. Por lo general, los nodos llevan el nombre de comandos correspondientes.

Puede usar las teclas de flecha para navegar entre los nodos. Alternativamente, también podría usar un gráfico navegador ical (que es mucho más fácil de usar) como konqueror o yelp .

En cuanto a las traducciones de idiomas, el sistema de *información* siempre está en inglés y no es adecuado. capaz de traducción, a diferencia del sistema de páginas man . Sin embargo, cuando le pide al programa pinfo que mostrar una página de *información* no existente , volverá a la página del *manual* con el mismo nombre (si existe), que puede ser traducido

6.1.3. Documentación específica del paquete

Cada paquete incluye su propia documentación e incluso los programas menos documentados en general tener un archivo README que contenga información interesante y / o importante. Este documental se instala en el directorio / usr / share / doc / *package* / (donde *package* representa el nombre del paquete). Si la documentación es particularmente grande, no puede incluirse en el programa paquete principal, pero puede descargarse a un paquete dedicado que generalmente se denomina *paquete* -doc. El paquete principal generalmente recomienda el paquete de documentación para que pueda encontrar fácilmente eso.

El / usr / share / doc / *package* / directoryal también contiene algunos archivos proporcionados por Debian, que complete la documentación especificando las particularidades o mejoras del paquete comparadas a una instalación tradicional del software. El archivo README.Debian también indica todos los adapta- Taciones que se hicieron para cumplir con la Política de Debian. El archivo changelog.Debian.gz permite el usuario debe seguir las modificaciones realizadas al paquete a lo largo del tiempo; es muy útil intentar Comprenda qué ha cambiado entre dos versiones instaladas que no tienen el mismo comportamiento ior. Finalmente, a veces hay un archivo NEWS.Debian.gz que documenta los principales cambios en el programa que puede afectar directamente al administrador.

6.1.4. Sitios web

En muchos casos, puede encontrar sitios web que se utilizan para distribuir programas de software gratuitos y para reunir a la comunidad de sus desarrolladores y usuarios. Estos sitios están cargados con información relevante información en varias formas, como documentación oficial, preguntas frecuentes (FAQ), y archivos de listas de correo. En la mayoría de los casos, las preguntas frecuentes o los archivos de la lista de correo abordan problemas que te has encontrado. Mientras busca información en línea, es inmensamente valioso dominar sintaxis de búsqueda Un consejo rápido: intente restringir una búsqueda a un dominio específico, como el dedicado al programa que te está dando problemas. Si la búsqueda devuelve demasiadas páginas o si los resultados no coincide con lo que busca, puede agregar la palabra clave **kali** o **debian** para limitar los resultados y el objetivo información relevante.

Del error a un Solución	Si el software devuelve un mensaje de error muy específico, ingréselo en un motor de búsqueda (entre comillas dobles " , para buscar la frase completa, en lugar de la palabras clave individuales). En la mayoría de los casos, los primeros enlaces devueltos contendrán la respuesta Que tu necesitas. En otros casos, obtendrá errores muy generales, como "Permiso denegado". En esto caso, es mejor verificar los permisos de los elementos involucrados (archivos, ID de usuario, grupos, etc.) En resumen, no se habitúe a utilizar siempre un motor de búsqueda para encontrar una solución. a tu problema Encontrará que es demasiado fácil olvidar usar el sentido común.

Si no conoce la dirección del sitio web del software, existen varios medios para localizar eso. Primero, busque un campo de página de inicio en la metainformación del paquete (apt show *package*). Alabama- En términos generales, la descripción del paquete puede contener un enlace al sitio web oficial del programa. Si no se indica ninguna URL, el mantenedor del paquete puede haber incluido una URL en / usr / share / doc / *paquete* / archivo de derechos de autor . Finalmente, puede utilizar un motor de búsqueda (como Google, DuckDuckGo, Yahoo, etc.) para encontrar el sitio web del software.

6.1.5. Documentación de Kali en docs.kali.org

El proyecto Kalip mantiene una colección de documentación útil en http://docs.kali.org . Mientras Este libro cubre una gran parte de lo que debe saber sobre Kali Linux, la documentación allí aún puede ser útil, ya que contiene instrucciones paso a paso (muy parecido a cómo hacerlo) sobre muchos temas.

[2] http://docs.kali.org/

Repasemos los diversos temas tratados allí:

- Primeros pasos: una serie de instrucciones, incluidas las instrucciones de descarga, para aquellos nuevos en Kali
- Kali Linux Live: documentación que describe cómo usar Kali Linux como un sistema en vivo
- Instalación de Kali Linux: varios documentos que describen la instalación de Kali Linux, incluido cómo instalarlo en paralelo con otros sistemas operativos

- Kali Linux en ARM: muchas recetas sobre cómo ejecutar Kali Linux en varios dispositivos basados en ARM
- Uso de Kali Linux: múltiples procedimientos que cubren muchas solicitudes comunes
- Personalización de Kali Linux: instrucciones para los seguidores que compiten en el edificio construido en Kalibased en su requisitos propios
- Kali Community Support: sugerencias para las diversas comunidades donde puede obtener apoyo. y explicaciones sobre cómo enviar informes de errores
- Políticas de Kali Linux: explicaciones sobre lo que hace especial a Kali Linux en comparación con otras distribuciones de Linux
- Kali Linux Dojo: videos de talleres Black Hat y DEF CON

6.2. Comunidades Kali Linux

Hay muchas comunidades de Kali Linux en todo el mundo que utilizan muchas herramientas diferentes para comunicarse nicate (foros y redes sociales, por ejemplo). En esta sección, solo presentaremos dos Comunidades Kali Linux.

6.2.1. Foros web en foros.kali.org

Los foros oficiales de la comunidad para el proyecto Kali Linux se encuentran en foros.kali.org [1] . Me gusta en cada foro basado en la web, debe crear una cuenta para poder publicar y el sistema recuerda qué publicaciones ya ha visto, lo que facilita el seguimiento de las conversaciones de forma regular.

Antes de publicar, debe leer las reglas del foro:

[2] http://docs.kali.org/community/kali-linux-community-forums

No los copiaremos aquí, pero vale la pena señalar que no se le permite hablar sobre acusaciones ilegales. actividades como romper en las redes de otras personas. Debe ser respetuoso con la otra comunidad miembros para crear una comunidad acogedora. La publicidad está prohibida y las discusiones fuera de tema deben ser evitados Hay suficientes categorías para cubrir todo lo que le gustaría discutir. sobre Kali Linux.

6.2.2. # kali-linux IRC Channel en Freenode

IRC es un sistema de chat en tiempo real. Las discusiones ocurren en salas de chat que se llaman *canales* y son generalmente se centra en un tema o comunidad en particular. El proyecto Kali Linux usa el # kali- canal de Linux en el Freenode[2] redes (puede usar chat.freenode.net como servidor IRC, en el puerto 6667 para una conexión cifrada con TLS o el puerto 6666 para una conexión de texto sin cifrar).

[1] http://forums.kali.org
[2] http://www.freenode.net

Para unirse a las discusiones sobre IRC, debe usar un cliente IRC como hexchat (en modo gráfico) o irssi (en modo consola). También hay un cliente basado en web disponible en webchat.freenode.net[3] .

Si bien es muy fácil unirse a la conversación, debe tener en cuenta que los canales IRC tienen sus reglas propias y que hay operadores de canal (su apodo tiene el prefijo @) que pueden forzar las reglas: pueden expulsarlo del canal (o incluso prohibirlo si continúa desobedeciendo) las normas). El canal # kali-linux no es una excepción. Las reglas han sido documentadas aquí:

[2] http://docs.kali.org/community/kali-linux-irc-channel

Para resumir las reglas: debe ser amigable, tolerante y razonable. Tú deberías evitar discusiones fuera de tema. En particular, discusiones sobre actividades ilegales, warez / cracks / pirated soft- Las mercancías, la política y las religiones están prohibidas. Tenga en cuenta que su dirección IP estará disponible para otros.

Si desea pedir ayuda, siga las recomendaciones que figuran en " Cómo evitar respuestas RTFM " [página 124]: investigue primero y comparta los resultados. Cuando se le solicite un suplemento información, proporciónela con precisión (si debe proporcionar una salida detallada, no la pegue directamente en el canal, en su lugar use un servicio como Pastebin [4] y publique solo la URL de Pastebin).

No esperes una respuesta inmediata. Aunque IRC es una plataforma de comunicación en tiempo real, los participantes inician sesión desde todo el mundo, por lo que las zonas horarias y los horarios de trabajo varían. Se puede tomar unos minutos u horas para que alguien responda a su pregunta. Sin embargo, cuando otros incluyen su nick en una respuesta, su nick será resaltado y la mayoría de los clientes de IRC le notificarán, entonces deje a su cliente conectado y sea paciente.

6.3. Presentación de un buen informe de error

Si todos sus esfuerzos para resolver un problema fallan, es posible que el problema se deba a un error en el programa. En este caso, el problema puede haber resultado en un informe de error. Puedes buscar un error informes para encontrar una solución a su problema, pero echemos un vistazo al procedimiento para informar un error a Kali, Debian o directamente a los desarrolladores anteriores para que entienda el proceso si necesita enviar su propio informe.

El objetivo de un informe de error es proporcionar suficiente información para que los desarrolladores o mantenedores de el programa (supuestamente) defectuoso puede reproducir el problema, depurar su comportamiento y desarrollar una solución. Esto significa que su informe de error debe contener información adecuada y debe ser dirigido a la persona correcta o el equipo del proyecto. El informe también debe estar bien escrito y completo, asegurando Una respuesta más rápida.

El procedimiento exacto para el informe de error variará dependiendo de dónde lo envíe. (Kali, Debian, desarrolladores anteriores) pero hay algunas recomendaciones genéricas que se aplican a todos los casos. En este capítulo discutiremos esas recomendaciones.

[3] http://webchat.freenode.net

[4] http://pastebin.com

Page 156

6.3.1. Recomendaciones genéricas

Discutamos algunas recomendaciones y guías generales que ayudarán a que la publicación de informes de errores eso es claro, completo y mejora las posibilidades de que el error sea abordado por el desarrolladores de manera oportuna.

Cómo comunicarse

Escriba su informe en inglés La comunidad de software libre es internacional y, a menos que usted conoce a tu interlocutor, deberías estar usando un inglés simple. Si eres hablante nativo de inglés, use oraciones simples y evite construcciones que puedan ser difíciles de entender para las personas con habilidades limitadas de inglés. Aunque la mayoría de los desarrolladores son muy inteligentes, no todos tienen Fuertes habilidades en el idioma inglés. Es mejor nunca asumir.

Sea respetuoso con el trabajo de los desarrolladores Recuerde que la mayoría de los desarrolladores de software libre (incluidos los que están detrás de Kali Linux) son benévolos y pasan su tiempo libre limitado para trabajar El software que está utilizando libremente. Muchos lo hacen por altruismo. Por lo tanto, cuando presenta un informe de error, sea respetuoso (incluso si el error parece un error obvio del desarrollador) y no asumas que te deben una solución. Agradecerles su contribución en su lugar.

Si sabe cómo modificar y recompilar el software, ofrezca ayudar a los desarrolladores a realizar las pruebas. cualquier parche que le envíen. Esto les mostrará que estás dispuesto a invertir tu propio tiempo también.

Sea reactivo y esté listo para proporcionar más información En algunos casos, el desarrollador vendrá volver a usted con solicitudes de más información o solicitudes para que intente recrear el problema quizás usando diferentes opciones o usando un paquete actualizado. Deberías intentar responder a esas consultas lo más rápido posible. Cuanto más rápido envíe su respuesta, mayor será la posibilidad que podrán resolverlo rápidamente mientras el análisis inicial aún está fresco en su mente.

Si bien debe intentar responder rápidamente, tampoco debe hacerlo demasiado rápido: los datos enviados deben ser correcto y debe contener todo lo que los desarrolladores solicitaron. Estarán molestos si Tienen que pedir algo por segunda vez.

Qué poner en el informe de errores

Instrucciones para reproducir el problema Para poder reproducir el problema, los desarrolladores necesitan para saber qué está utilizando, de dónde lo obtuvo y cómo lo instaló.

Debe proporcionar instrucciones precisas, paso a paso, que describan cómo reproducir el problema. Si necesita usar algunos datos para reproducir el problema, adjunte el archivo correspondiente al error reporte. Intenta encontrar el conjunto mínimo de instrucciones necesarias para reproducir el error.

Page 157

Contemple y establezca sus expectativas Explique lo que estaba tratando de hacer y cómo esperaba que el programa se comportara.

En algunos casos, el error solo se activa porque estaba usando el programa de una manera que era no diseñado para operar por los desarrolladores. Al explicar lo que estaba tratando de lograr, usted permitirá a los desarrolladores ver claramente cuándo es este el caso.

En otros casos, el comportamiento que usted describe es un error que puede tener un comportamiento realmente normal. Sea explícito sobre lo que esperaba que hiciera el programa. Esto aclarará la situación para el desarrolladores Pueden mejorar el comportamiento o mejorar la documentación, pero al menos ¡saben que el comportamiento de su programa confunde a algunos usuarios!

Sea específico Incluya los números de versión del software que utiliza, posiblemente con la versión números de sus dependencias. Cuando se refiera a algo que descargó, incluya su URL completa

Cuando reciba un mensaje de error, cítelo exactamente como lo vio. Si es posible, incluya una copia de su

salida de pantalla o una captura de pantalla. Incluya una copia de cualquier archivo de registro relevante, asegurándose de eliminar cualquier dato confidencial primero.

Mencione posibles soluciones o soluciones alternativas Antes de presentar el informe de error, probablemente haya intentado volver a resolver el problema. Explica qué intentaste y qué resultados recibiste. Sea muy claro sobre qué es un hecho y qué fue solo una hipótesis de su parte.

Si realizó una búsqueda en Internet y encontró algunas explicaciones sobre un problema similar, puede mencionelos, en particular cuando encuentre otros informes de errores similares en el rastreador de errores de Debian o en El rastreador de errores aguas arriba.

Si encontró una manera de lograr el resultado deseado sin activar el error, documente eso tambien. Esto ayudará a otros usuarios que se ven afectados por el mismo problema.

Los informes largos de errores **están bien** Un informe de error de dos líneas es insuficiente; proporcionando toda la información generalmente requiere varios párrafos (o, a veces, páginas) de texto.

Proporcione toda la información que pueda. Intente atenerse a lo que es relevante, pero si no está seguro, también mucho es mejor que muy poco.

Si su informe de error es realmente largo, tómese un tiempo para estructurar el contenido y proporcionar un breve resumen al inicio.

Consejos varios

Evite presentar informes de errores **duplicados** En el mundo del software libre, todos los rastreadores de errores son públicos. Abierto los problemas se pueden examinar e incluso tienen una función de búsqueda. Por lo tanto, antes de presentar un nuevo informe de error, intente determinar si su problema ya ha sido reportado por otra persona.

Si encuentra un informe de error existente, suscríbase y posiblemente agregue información complementaria. Hacer no publique comentarios como "Yo también" o "+1"; No sirven para nada. Pero puedes indicar que están disponibles para más pruebas si el remitente original no ofreció esto.

Si no ha encontrado ningún informe de su problema, continúe y archívelo. Si has encontrado relacionados boletos, asegúrese de mencionarlos.

Asegúrese de utilizar la última versión Es muy frustrante para los desarrolladores recibir informes de errores para problemas que ya han resuelto o problemas que no pueden reproducir con la versión que están usando (los desarrolladores casi siempre usan la última versión de su producto). Incluso cuando los desarrolladores mantienen versiones anteriores, el soporte a menudo se limita a correcciones de seguridad y graves problemas. ¿Estás seguro de que tu error es uno de esos?

Es por eso que, antes de presentar un informe de errores, debe asegurarse de que está utilizando la última versión de el sistema problemático y la aplicación y que puede reproducir el problema en esa situación.

Si Kali Linux no ofrece la última versión de la aplicación (ni en kali-rolling ni en kali-sangrado, ver sección 8.1.3.3, " El repositorio de Kali-Bleeding-Edge " [página 174]), usted tiene soluciones naturales: puede probar una instalación manual de la última versión en un virtual descartable máquina, o puede revisar el ChangeLog ascendente (o el historial de confirmación de Git) para ver que hay no ha habido ningún cambio que pueda solucionar el problema que está viendo (y luego archivar el error incluso aunque no probaste la última versión).

No mezcle varios problemas en un solo archivo de informe de errores un informe de error por problema. De esa manera, las discusiones posteriores no se vuelven demasiado desordenadas y cada error se puede solucionar de acuerdo con su propio calendario. Si no lo hace, el error único debe ser reutilizado varias veces y solo se puede cerrar cuando se han solucionado todos los problemas, o los desarrolladores deben presentar el complemento informa que deberías haber creado en primer lugar.

6.3.2. Dónde presentar un informe de error

Para poder decidir dónde presentar el informe de error, debe tener una buena comprensión de problema y debe haber identificado en qué software se encuentra el problema.

Idealmente, puede rastrear el problema hasta un archivo en su sistema y luego puede usar `dpkg` para averiguar qué paquete posee ese archivo y de dónde proviene ese paquete. Asumamos que encontraste un error en una aplicación gráfica. Después de mirar la lista de procesos en ejecución (la salida de `ps auxf`), descubrió que la aplicación se inició con el ejecutable `/ usr / bin / sparta` :

```
$ dpkg -S / usr / bin / sparta
sparta: / usr / bin / sparta
```

```
$ dpkg -s sparta | grep ^ Versión:
Versión: 1.0.1 + git20150729-0kali1
```

Aprende que / usr / bin / sparta es proporcionado por el paquete sparta, que está en la versión 1.0.1 + git 20150729-0kali1. El hecho de que la cadena de versión contenga kali le indica que el paquete

proviene de Kali Linux (o es modificado por Kali Linux). Cualquier paquete que no tenga kali en su La cadena de versión (o en su nombre de paquete) viene directamente de Debian (Pruebas de Debian en general).

Verificación doble antes Archivando errores contra Debian

Si encuentra un error en un paquete importado directamente de Debian, lo ideal sería informado y corregido en el lado de Debian. Sin embargo, antes de hacer esto, asegúrese de que el El problema es reproducible en un sistema Debian simple ya que Kali puede haber causado problema modificando otros paquetes o dependencias.

La forma más fácil de lograr esto es configurar una máquina virtual que ejecute Debian Test- En g. Puede encontrar un ISO de instalación para las pruebas de Debian en el sitio web del instalador de Debian. sitio:

[2] https://www.debian.org/devel/debian-installer/

Si puede confirmar el problema en la máquina virtual, puede enviar el error a Debian ejecutando reportbug dentro de la máquina virtual y siguiendo las instrucciones Opciones proporcionadas.

La mayoría de los informes de errores sobre el comportamiento de las aplicaciones deben dirigirse a sus proyectos anteriores excepto cuando se enfrenta a un problema de integración: en ese caso, el error es un error en la forma en que el software se empaqueta e integra en Debian o Kali. Por ejemplo, si una aplicación ofrece Opciones de tiempo de compilación que el paquete no se puede habilitar o la aplicación no funciona debido a una biblioteca faltante (lo que pone de manifiesto una dependencia faltante en la metainformación del paquete), Puede estar enfrentando un problema de integración. Cuando no sabes qué tipo de problema enfrentas, Por lo general, es mejor presentar el problema en ambos lados y hacer una referencia cruzada.

Identificar el proyecto ascendente y encontrar dónde archivar el informe de error suele ser fácil. Tu solo tiene que navegar por el sitio web anterior, al que se hace referencia en el campo Página de inicio del paquete metadatos:

```
$ dpkg -s sparta | grep ^ Página de inicio:
Página de inicio: https://github.com/SECFORCE/sparta
```

6.3.3. Cómo presentar un informe de error

Presentación de un informe de error en Kali

Kali utiliza un rastreador de errores basado en la web en http://bugs.kali.org donde puede consultar todos los errores informa anónimamente, pero si desea comentar o presentar un nuevo informe de error, deberá registrar una cuenta.

Registrarse para una cuenta de **Bug Tracker** Para comenzar, simplemente haga clic en *Registrarse para una nueva cuenta* en el error sitio web del rastreador, como se muestra en la Figura 6.1 , “ Página de inicio de Kali Bug Tracker ”[Página 134].

Figura 6.1 *Página de inicio de Kali Bug Tracker*

Luego, proporcione un nombre de usuario, una dirección de correo electrónico y una respuesta al desafío CAPTCHA. Luego haga clic el botón Registrarse para continuar (Figura 6.2 , " Página de registro " [página 134]).

Figura 6.2 *Página de registro*

Si tiene éxito, la página siguiente (Figura 6.3, " SignupConfirmationPage " [página135]) le notificará el registro de la cuenta ha sido procesado y el sistema de seguimiento de errores enviará una confirmación correo electrónico a la dirección que proporcionó. Deberá hacer clic en el enlace del correo electrónico para activar su cuenta.

Una vez que su cuenta ha sido activada, haga clic en Continuar para continuar a la página de inicio de sesión del rastreador de errores.

Figura 6.3 *Página de confirmación de registro*

Creación del informe Para comenzar su informe, inicie sesión en su cuenta y haga clic en el enlace Informar problema en la página de inicio. Se le presentará un formulario con muchos campos para completar, como se muestra en la Figura 6.4 , “ Formulario para informar un error ” [página 136].

Figura 6.4 *Formulario para informar un error*

Aquí hay un resumen de todos los campos en el formulario:

Categoría (obligatoria) Este campo describe la categoría del error que está enviando. Informes que puede atribuirse a un paquete específico debe archivarse en Kali Package Bug o Kali Categorías de mejora de paquetes. Otros informes deben usar el error general o la función de recuperación categorías de misiones. Las categorías restantes son para casos de uso específicos: la actualización de herramientas puede ser se utiliza para notificar a los desarrolladores de Kali la disponibilidad de una nueva versión de un paquete de software

en Kali Las nuevas solicitudes de herramientas se pueden utilizar para sugerir nuevas herramientas para empaquetar e integrar en el Distribución de Kali.

Reproducibilidad Este campo documenta si el problema es reproducible de manera predecible o si ocurre solo algo al azar.

Severidad y prioridad Es mejor dejar estos campos sin modificar, ya que son principalmente para los desarrolladores.

Pueden usarlos para ordenar la lista de problemas de acuerdo con la gravedad del problema y La prioridad a la que debe ser manejado.

Versión del producto Este campo debe indicar qué versión de Kali Linux está ejecutando (o la uno que es el más cercano a lo que está ejecutando). Piénselo dos veces antes de informar un problema en una versión anterior que ya no es compatible.

Resumen (obligatorio) Este es esencialmente el título de su informe de error y es lo primero que La gente verá. Asegúrese de que transmite la razón por la que está presentando el informe. Evitar descripciones genéricas como "X no funciona" y optar por "X falla con el error Y bajo condición Z. "

Descripción (obligatorio) Este es el cuerpo de su informe. Aquí debe ingresar todos los formación que recopiló sobre el problema que está experimentando. No olvides todo el recomendaciones dadas en la sección anterior.

Pasos para reproducir En este campo, enumere todas las instrucciones detalladas que explican cómo activar el problema.

Información adicional En esta sección, puede proporcionar cualquier información adicional que crea Es relevante para el tema. Si tiene una solución o solución para el problema, proporciónelo en esta sección.

Cargar archivo No todo se puede explicar con texto sin formato. Este campo le permite adjuntar arbitrario archivos a sus informes: capturas de pantalla para mostrar el error, documentos de muestra que desencadenan el problema lem, archivos de registro, etc.

Ver estado Deje ese campo establecido en "público" para que todos puedan ver su informe de error. Utilice "private "solo para informes relacionados con la seguridad que contienen información sobre seguridad no revelada vulnerabilidades

Archivar un informe de error en Debian

Debian utiliza un sistema de seguimiento de errores (principalmente) basado en correo electrónico conocido como Debbugs. Para abrir un nuevo error informe, usted enviará un correo electrónico (con sintaxis especial) tosubmit@bugs.debian.org. Thiswillallocate un número de error *XXXXXX* e informarle que puede enviar información adicional enviando por correo *XXX XXX* @ bugs.debian.org. Cada error está asociado a un paquete Debian. Puede navegar por todos los errores de

un paquete dado (incluido el error que está pensando informar) en https://bugs.debian.org/ *empaquetar* . Puede consultar el historial de un error determinado en https://bugs.debian.org/ *XXXXXX* .

Configuración de Reportbug Si bien puede abrir un nuevo error con un simple correo electrónico, le recomendamos usando reportbug porque ayudará a redactar un informe de error sólido con toda la información requerida. Idealmente, debe ejecutarlo desde un sistema Debian (por ejemplo, en la máquina virtual donde reproducido el problema).

La primera ejecución de reportbug inicia un script de configuración. Primero, selecciona un nivel de habilidad. Debieras elija Novato o Estándar; Utilizamos este último porque ofrece un control más detallado. Próximo, seleccione una interfaz e ingrese sus datos personales. Finalmente, seleccione una interfaz de usuario. La configuración La secuencia de comandos le permitirá utilizar un agente de transporte de correo local, un servidor SMTP o, como último recurso, un Servidor Debian SMTP.

```
Bienvenido a reportbug! Como parece que es la primera vez que tienes
usado reportbug, estamos configurando su comportamiento. Estas configuraciones serán
guardado en el archivo "/root/.reportbugrc", que podrá editar libremente
más lejos.
Elija el modo operativo predeterminado para reportbug.

1 novato          Ofrezca indicaciones simples, evitando preguntas técnicas.

2 estándar Ofrece indicaciones más amplias, incluida la pregunta sobre cosas
                  que se esperaría que un usuario moderadamente sofisticado
                  saber sobre Debian.

3 avanzado Como estándar, pero supone que sabe un poco más sobre Debian,
           incluyendo "entrante".

4 expertos        Omitir la mayoría de las medidas de sujeción y el triaje preliminar
                  rutinas Este modo no debe ser utilizado por personas desconocidas
                  con las políticas y procedimientos operativos de Debian.
```

Seleccionar modo: **estándar** [novato]
Elija la interfaz predeterminada para reportbug.

1 texto Una interfaz de usuario de consola orientada al texto.

2 gtk2 Una interfaz gráfica de usuario (GTK +).

3 urwid Una interfaz de usuario de consola basada en menús

Seleccionar interfaz: **texto**
¿Reportbug a menudo tendrá acceso directo a Internet? (Deberías responder
Sí a esta pregunta a menos que sepa lo que está haciendo y planea
verifique si se han presentado informes duplicados a través de algún otro canal).

[S | n | q |?]? **Y**
¿Qué nombre real se debe usar para enviar informes de errores?
[raíz]> **Raphaël Hertzog**
¿Cuál de sus direcciones de correo electrónico debe usarse al enviar informes de errores?
(Tenga en cuenta que esta dirección será visible en el sistema de seguimiento de errores, por lo que
puede querer usar una dirección de correo web u otra dirección con buen spam
capacidades de filtrado).
[root@localhost.localdomain]> **buxy@kali.org**
¿Tiene un "agente de transporte de correo" (MTA) como Exim, Postfix o SSMTP
configurado en esta computadora para enviar correo a Internet? [y | N | q |?]? **norte**
Ingrese el nombre de su host SMTP. Por lo general se llama algo
como "mail.example.org" o "smtp.example.org". Si necesita usar un
puerto diferente al predeterminado, use la alternativa <host>: <port>
formato. Simplemente presione ENTER si no tiene uno o no lo sabe, y así
Se utilizará el host Debian SMTP.
>
Por favor ingrese el nombre de su servidor proxy. Solo debería usar esto
parámetro si está detrás de un firewall. El argumento PROXY debería ser
formateado como una URL HTTP válida, que incluye (si es necesario) un número de puerto; para
ejemplo, http://192.168.1.1:3128/. Simplemente presione ENTER si no tiene uno
o no lo se.
>
Archivo de preferencias predeterminado escrito. Para reconfigurar, vuelva a ejecutar reportbug con
la opción "--configurar".

Uso de Reportbug Con la fase de configuración completada, puede comenzar el informe de error real. Tú serás se le solicita un nombre de paquete, aunque también puede proporcionar el nombre del paquete directamente en el línea de comando con el *paquete* reportbug).

¡Ejecutar 'reportbug' como root es probablemente inseguro! Continuar [y | N | q |?]? **y**
Ingrese el nombre del paquete en el que ha encontrado un problema, o
escriba 'otro' para informar un problema más general. Si no sabes que
paquete en el que se encuentra el error, comuníquese con debian-user@lists.debian.org para
asistencia.
> **wireshark**

Contrariamente a los consejos dados anteriormente, si no sabe contra qué paquete presentar el error, usted debería ponerse en contacto con un foro de soporte de Kali (descrito en la sección 6.2, " Comunidades Kali Linux " [página 128]). En el siguiente paso, reportbug descarga la lista de errores archivados en el paquete dado y le permite explorarlos para ver si puede encontrar el suyo.

*** Bienvenido a reportbug. Utilizar ? para ayuda en las indicaciones. ***
Nota: los informes de errores se archivan públicamente (incluida la dirección de correo electrónico de
el remitente).
Conjunto de caracteres detectados: UTF-8

Cambie su configuración regional si esto es incorrecto.

Usando "'Raphaël Hertzog" <buxy@kali.org>' como su dirección de origen.

```
Obteniendo el estado de wireshark ...
Verificación de la integridad del paquete ...
Buscando nuevas versiones en madison ...
Enviará un informe a Debian (por lsb_release).
Consultando Debian BTS para informes sobre wireshark (fuente) ...
35 informes de errores encontrados:

Errores con severidad importantes
    1) # 478200 tshark: parece ignorar los filtros de lectura al escribir en ...
    2) # 776206 mergecap: no se puede crear el archivo de salida> 2 GB
    3) # 780089 wireshark: "En gnome wireshark no tiene barra de título.  Hace…
Errores con gravedad normal
    4) # 151017 etéreo: "Estadísticas de la Jerarquía de Protocolo" dan información engañosa ...
    5) # 275839 no disecciona correctamente la canalización de ESMTP
[...]
   35) # 815122 wireshark: agregar OID 1.3.6.1.4.1.11129.2.4.2
(24-35 / 35) ¿Está el error que encontró en la lista anterior [y | N | b | m | r | q | s | f | e |?]?  ?
y - Problema ya reportado; opcionalmente agregue información adicional.
N - (predeterminado) Problema no mencionado anteriormente; posiblemente verifique más.
b - Abra la lista completa de errores en un navegador web.
m - Obtenga más información sobre un error (también puede ingresar un número
      sin seleccionar "m" primero).
r - Vuelve a mostrar los últimos errores mostrados.
q - estoy aburrido; renunciar por favor
s: omita los problemas restantes; presentar un nuevo informe de inmediato.
f - Filtrar la lista de errores usando un patrón.
e - Abra el informe usando un cliente de correo electrónico.
? - Mostrar esta ayuda.
(24-35 / 35) ¿Está el error que encontró en la lista anterior [y | N | b | m | r | q | s | f | e |?]?  norte
El mantenedor de wireshark es 'Balint Reczey <balint@balintreczey.hu>'.
Buscando dependencias de wireshark ...
```

Si encuentra su error ya archivado, puede optar por enviar información complementaria, de lo contrario, Está invitado a presentar un nuevo informe de error:

```
Describa brevemente el problema (se permiten un máximo de 100 caracteres).  Esto será
el asunto del correo electrónico del error, así que mantenga el resumen lo más conciso posible, para
ejemplo: "no puede enviar correo electrónico" o "no comienza con la opción -q
especificado "(ingrese Ctrl + c para salir de reportbug sin informar un error).
> no disecciona el protocolo foobar
Reescritura sujeta a 'wireshark: no disecciona el protocolo foobar'
```

Después de proporcionar un resumen de una línea de su problema, debe calificar su gravedad a lo largo de un escala:


```
¿Cómo calificaría la gravedad de este problema o informe?

1 crítico              crea software no relacionado en el sistema (o el conjunto
                       sistema) se rompe, o causa una pérdida de datos grave, o
                       introduce un agujero de seguridad en los sistemas donde instala
                       el paquete.
2 tumbas               hace que el paquete en cuestión sea inutilizable por la mayoría o todos
                       usuarios, o causa pérdida de datos, o introduce una seguridad
                       agujero que permite el acceso a las cuentas de los usuarios que usan
                       el paquete.
3 graves               es una violación grave de la política de Debian (es decir, el
                       el problema es una violación de un "deber" o "obligatorio"
                       directiva); puede o no afectar la usabilidad del
                       paquete. Tenga en cuenta que las infracciones de políticas no graves pueden ser
                       errores 'normales', 'menores' o 'lista de deseos'. (Paquete
                       los mantenedores también pueden designar otros errores como "graves" y
                       por lo tanto, de liberación crítica; sin embargo, los usuarios finales no deben hacer
                       entonces.). Para la lista canónica de temas que merecen serios
                       gravedad puede consultar esta página web:
                       http://release.debian.org/testing/rc_policy.txt
4 importantes          un error que tiene un efecto importante en la usabilidad de un
                       paquete, sin dejarlo completamente inutilizable para
                       todos.
5 no genera un error que impide que el paquete se genere desde el origen.
                       (Esta es una 'severidad virtual').
6 normal               un error que no socava la usabilidad del conjunto
                       paquete; por ejemplo, un problema con una opción particular
                       o elemento del menú.
```

7 menores	cosas como errores ortográficos y otros cosméticos menores errores que no afectan la funcionalidad principal de la paquete.
8 lista de deseos	sugerencias y solicitudes de nuevas funciones.

Seleccione un nivel de gravedad: [normal]

Si no está seguro, simplemente mantenga la gravedad predeterminada normal.

También puede etiquetar su informe con algunas palabras clave:

¿Alguno de los siguientes se aplica a este informe?

1 di	Este error es relevante para el desarrollo de debian-installer.
2 ipv6	Este error afecta la compatibilidad con el Protocolo de Internet versión 6.
3 l10n	Este error informa un problema de localización / internacionalización.
4 lfs	Este error afecta la compatibilidad con archivos grandes (más de 2 gigabytes).
5 recién llegado	Este error tiene una solución conocida pero el responsable de mantenimiento solicita a alguien de lo contrario implementarlo.

6 parche	Incluye un parche para solucionar este problema.
7 ascendente	Este error se aplica a la parte ascendente del paquete.
8 ninguno	

Seleccione etiquetas: (una a la vez) [ninguna]

La mayoría de las etiquetas son bastante esotéricas, pero si su informe incluye una solución, debe seleccionar la etiqueta del parche.

Una vez que se completa esto, reportbug abre un editor de texto con una plantilla que debe editar (Ej. ejemplo 6.2 , " Plantilla generada por reportbug " [página 142]). Contiene algunas preguntas que usted debe eliminar y responder, así como cierta información sobre su sistema que ha sido automatizada Cally recogido. Observe cómo se estructuran las primeras líneas. No deben modificarse ya que será analizado por el rastreador de errores para asignar el informe al paquete correcto.

Ejemplo 6.2 *Plantilla generada por reportbug*

```
Asunto: wireshark: no disecciona el protocolo foobar

Paquete: wireshark
Versión: 2.0.2 + ga16e22e-1
Severidad: normal

Estimado mantenedor,

*** Reportero, considere responder estas preguntas, cuando corresponda ***

      * ¿Qué llevó a la situación?
      * ¿Qué hiciste (o no hiciste) exactamente que fue efectivo (o
        ineficaz)?
      * ¿Cuál fue el resultado de esta acción?
      * ¿Qué resultado esperabas en su lugar?

*** Fin de la plantilla: elimine estas líneas de plantilla ***


-- Información del sistema:
Lanzamiento de Debian: stretch / sid
    APT prefiere las pruebas
    Política APT: (500, 'prueba')
Arquitectura: amd64 (x86_64)
Arquitecturas extranjeras: i386

Kernel: Linux 4.4.0-1-amd64 (SMP con 4 núcleos de CPU)
Configuración regional: LANG = fr_FR.utf8, LC_CTYPE = fr_FR.utf8 (charmap = UTF-8)
Shell: / bin / sh vinculado a / bin / dash
Init: systemd (a través de / run / systemd / system)
```

```
Las versiones de los paquetes wireshark dependen de:
ii wireshark-qt 2.0.2 + ga16e22e-1

wireshark recomienda que no haya paquetes.

wireshark sugiere que no haya paquetes.

- no hay información de debconf
```

Una vez que guarde el informe y cierre el editor de texto, volverá a `reportbug` , que proporciona muchos otras opciones y ofertas para enviar el informe resultante.

```
Generando un editor sensible ...
El informe se enviará al "Sistema de seguimiento de errores de Debian" <submit@bugs.debian.org>
¿Enviar este informe sobre wireshark (e para editar) [Y | n | a | c | e | i | l | m | p | q | d | t | s |?]?      ?
Y: (predeterminado) Enviar el informe de error por correo electrónico.
n: no envíe el informe de error;  en su lugar, guárdelo en un archivo temporal (sale de reportbug).
a - Adjunta un archivo.
c - Cambiar editor y reeditar.
e - Vuelva a editar el informe de error.
i - Incluir un archivo de texto.
l - Canaliza el mensaje a través del buscapersonas.
m: elija un anuncio publicitario para editar el informe.
p: imprime el mensaje en stdout.
q: guárdelo en un archivo temporal y salga.
d - Separar un archivo adjunto.
t - Agregar etiquetas.
s - Agregue un destinatario X-Debbugs-CC (un CC pero después del procesamiento BTS).
? - Mostrar esta ayuda.
¿Enviar este informe sobre wireshark (e para editar) [Y | n | a | c | e | i | l | m | p | q | d | t | s |?]?      Y
Guardar una copia de seguridad del informe en / tmp / reportbug-wireshark-backup-20160328-19073-87oJWJ
Conectándose a reportbug.debian.org a través de SMTP ...

Informe de error enviado a: "Sistema de seguimiento de errores de Debian" <submit@bugs.debian.org>
Se enviarán copias después del procesamiento a:
    buxy@kali.org

Si desea proporcionar información adicional, espere para recibir el
número de seguimiento de errores por correo electrónico;  luego puede enviar cualquier información adicional a
n@bugs.debian.org (por ejemplo, 999999@bugs.debian.org), donde n es el error
número. Normalmente recibirá un acuse de recibo por correo electrónico que incluye
el número de informe de error dentro de una hora;  si no has recibido un
confirmación, entonces el proceso de informe de errores falló en algún momento
(informe de error o falla de MTA, mantenimiento de BTS, etc.).
```


Archivar un informe de error en otro proyecto de software libre

Existe una gran diversidad de proyectos de software libre, que utilizan diferentes flujos de trabajo y herramientas. Este di-
La versión también se aplica a los rastreadores de errores en uso. Si bien muchos proyectos están alojados en GitHub y usan
Problemas de GitHub para rastrear sus errores, también hay muchos otros que alojan sus propios rastreadores, basados
en Bugzilla, Trac, Redmine, Flyspray y otros. La mayoría de ellos están basados en la web y requieren que usted
Registre una cuenta para enviar un nuevo ticket.

No cubriremos todos los rastreadores aquí. Depende de usted aprender los detalles de varios rastreadores para
otros proyectos de software libre, pero como GitHub es relativamente popular, lo analizaremos brevemente
aquí. Al igual que con otros rastreadores, primero debe crear una cuenta e iniciar sesión. A continuación, haga clic en Problemas
pestaña, como se muestra en la Figura 6.5, “ Página principal de un proyecto de GitHub ” [página 144].

Figura 6.5 *Página principal de un proyecto GitHub*

Luego puede navegar (y buscar) la lista de problemas abiertos. Una vez que esté seguro de que su error es aún no archivado, puede hacer clic en el botón Nuevo problema (Figura 6.6 , " Página de problemas de un proyecto de GitHub " [página 145]).

Figura 6.6 *Página de problemas de un proyecto GitHub*

Ahora está en una página donde debe describir su problema (Figura 6.7, " Formulario de GitHub para presentar un nueva edición"[Página 145]). Aunque no hay una plantilla como la que se encuentra en reportbug , el error El mecanismo de informes es bastante sencillo, lo que le permite adjuntar archivos, aplicar formato a texto y mucho más. Por supuesto, para obtener los mejores resultados, asegúrese de seguir nuestras pautas para crear un informe detallado y bien descrito.

Figura 6.7 *Formulario de GitHub para presentar un nuevo problema*

6.4. Resumen

En esta sección, discutimos varios métodos para ayudarlo a encontrar documentación e información sobre programas y cómo encontrar ayuda con problemas que pueda encontrar. Echamos un vistazo al hombre y páginas de información y los comandos apropos e info . Hablamos de rastreadores de errores, proporcionamos algunos consejos sobre cómo buscar y enviar buenos informes de errores, y proporcionó algunos consejos para ayudarlo a calcular a quien pertenece el programa o proyecto en cuestión.

Consejos resumidos:

- Antes de que puedas entender lo que realmente está sucediendo cuando hay un problema, debes Conocer el papel teórico desempeñado por cada programa involucrado en el problema. Uno de los mejores La forma de hacerlo es revisar la documentación del programa.
- Para ver una página de manual, simplemente escriba man *manual-page* , completando el nombre del comando después de un número de sección opcional.
- El comando apropos devuelve una lista de páginas del manual cuyo resumen menciona el informe palabras clave solicitadas, junto con el resumen de una línea de la página del manual.
- El proyecto GNU tiene manuales escritos para la mayoría de sus programas en formato de *información* . Esto es por qué muchas páginas del manual hacen referencia a la documentación de *información* correspondiente .
- Cada paquete incluye su propia documentación e incluso los programas menos documentados generalmente tienen un archivo README que contiene información interesante y / o importante. Esta documentación se instala en el directorio / usr / share / doc / *package* / .
- En la mayoría de los casos, las preguntas frecuentes o los archivos de la lista de correo del sitio web oficial de un programa pueden abordar problemas que ha encontrado
- El proyecto Kali mantiene una colección de documentación útil en http://docs.kali.org.
- El proyecto Kali Linux utiliza el canal # kali-linux en la red IRC Freenode [5] . Usted puede use chat.freenode.net como servidor IRC, en el puerto 6667 para una conexión o puerto cifrado con TLS 6666 para una conexión de texto claro. Para unirse a las discusiones sobre IRC, debe usar un IRC cliente como hexchat (en modo gráfico) o irssi (en modo consola). También hay una web cliente basado disponible en webchat.freenode.net [6] .
- Los foros oficiales de la comunidad para el proyecto Kali Linux se encuentran en foros.kali.org[7] .
- Si descubre un error en un programa, puede buscar informes de errores o archivar los suyos. Estar seguro seguir las pautas que hemos esbozado para garantizar que su informe sea claro y comprensivo sive, y mejora las posibilidades de que los desarrolladores aborden el error de manera oportuna Moda.

[5] [5] https://www.freenode.net
[6] [6] https://webchat.freenode.net
[7] [7] https://forums.kali.org

- Algunos informes de errores deben presentarse a Kali, mientras que otros pueden presentarse en el lado de Debian. UNA comando como **dpkg -s *nombre-paquete* | grep ^ Versión:** revelará el número de versión y se etiquetará como "kali" si se trata de un paquete modificado por Kali.
- Identificar un proyecto de alcance y encontrar un lugar en el archivo del informe de errores es generalmente fácil. Sim- navegue por el sitio web ascendente al que se hace referencia en el campo Página de inicio del paquete metadatos.
- Kaliusesaweb-basedbugtrackerat https://bugs.kali.org donde puede consultar informes de errores de forma anónima, pero si desea comentar o presentar un nuevo informe de error, usted necesitará registrar una cuenta.
- Debian utiliza un sistema de seguimiento de errores basado en correo electrónico (principalmente) conocido como Debbugs. Para abrir un nuevo informe de error, puede enviar un correo electrónico (con una sintaxis especial) a submit@bugs.debian.org o usted puede usar el comando reportbug , que lo guiará a través del proceso.
- Si bien muchos proyectos están alojados en GitHub y utilizan problemas de GitHub para rastrear sus errores, hay También hay muchos otros que alojan sus propios rastreadores. Puede que tenga que investigar los conceptos básicos de rastreadores de errores de terceros si necesita publicar en ellos.

Ahora que tiene las herramientas básicas para navegar por Linux, instalar y configurar Kali y solucionar problemas

Al solucionar problemas de su sistema y obtener ayuda, es hora de analizar el bloqueo de Kali para que pueda proteja su instalación y los datos de su cliente.

Palabras clave

Politica de seguridad
Cortafuegos
iptables
Supervisión
Inicio sesión

Capítulo

7 Asegurando y Supervisión de Kali Linux

Contenido

Definición de una política de seguridad 150
Posibles medidas de seguridad 152
Asegurar los servicios de red 153
Cortafuegos o filtrado de paquetes 153
Monitoreo y registro 161
Resumen 164

A medida que comience a usar Kali Linux para un trabajo cada vez más sensible y de mayor perfil, es probable que necesita tomar la seguridad de su instalación más en serio. En este capítulo, primero discutiremos políticas de seguridad, destacando varios puntos a considerar al definir dicha política, y resumiendo Algunas de las amenazas para su sistema y para usted como profesional de seguridad. También discutiremos medidas de seguridad para computadoras portátiles y sistemas de escritorio y enfoque en firewalls y filtrado de paquetes. Fi- Finalmente, discutiremos las herramientas y estrategias de monitoreo y le mostraremos cómo implementarlas mejor para detectar posibles amenazas a su sistema.

7.1. Definiendo una Política de Seguridad

No es práctico discutir la seguridad a grandes rasgos ya que la idea representa una amplia gama de problemas. conceptos, herramientas y procedimientos, ninguno de los cuales se aplica universalmente. Elegir entre ellos requiere un Se precisan ideas precisas sobre sus objetivos. Asegurar un sistema que comienza con una respuesta a algunas preguntas. Prisa-

Invertir de lleno en la implementación de un conjunto arbitrario de herramientas corre el riesgo de centrarse en lo incorrecto aspectos de seguridad.

Por lo general, es mejor determinar un objetivo específico. Un buen enfoque para ayudar con esa determinación comienza con las siguientes preguntas:

- *¿Qué* estás tratando de proteger? La política de seguridad será diferente dependiendo de si desea proteger computadoras o datos. En el último caso, también necesita saber qué datos.
- ¿Qué está tratando de proteger *contra* ? ¿Es una fuga de datos confidenciales? Datos accidentales ¿pérdida? ¿Pérdida de ingresos causada por la interrupción del servicio?
- Además, ¿contra *quién* estás tratando de proteger? Las medidas de seguridad serán bastante diferentes para protegerse contra un error tipográfico por parte de un usuario habitual del sistema frente a protegerse contra un error grupo de atacante externo minado.

El término "riesgo" se usa habitualmente para referirse colectivamente a estos tres factores: qué proteger, qué debe evitarse y quién podría hacer que esto suceda. Modelar el riesgo requiere respuestas a estas tres preguntas. A partir de este modelo de riesgo, se puede construir una política de seguridad y la política Se puede implementar con acciones concretas.

Preguntas permanentes Bruce Schneier, un experto mundial en asuntos de seguridad (no solo seguridad informática), intenta para contrarrestar uno de los mitos más importantes de la seguridad con un lema: "La seguridad es un proceso, no es un producto ". Los activos a proteger cambian con el tiempo y también lo hacen las amenazas y medios disponibles para posibles atacantes. Incluso si una política de seguridad ha sido inicialmente perfectamente diseñado e implementado, nunca debe descansar en sus laureles. El riesgo los componentes evolucionan y la respuesta a ese riesgo debe evolucionar en consecuencia.

También vale la pena tener en cuenta las restricciones adicionales, ya que pueden restringir el rango de políticas ¿Hasta dónde está dispuesto a llegar para asegurar un sistema? Esta pregunta tiene un gran impacto en qué política implementar. Con demasiada frecuencia, la respuesta solo se define en términos de costos monetarios,

pero también se deben considerar otros elementos, como la cantidad de inconvenientes impuestos a usuarios del sistema o degradación del rendimiento.

Una vez que se ha modelado el riesgo, puede comenzar a pensar en diseñar una política de seguridad real.

Hay extremos que pueden entrar en juego al decidir el nivel de protección de seguridad para adoptar. Por un lado, puede ser extremadamente simple proporcionar seguridad básica del sistema.

Por ejemplo, si el sistema a proteger solo comprende una computadora de segunda mano, el uso exclusivo de que es agregar algunos números al final del día, decidiendo no hacer nada especial para proteger Sería bastante razonable. El valor intrínseco del sistema es bajo y el valor de los datos. son cero ya que no están almacenados en la computadora. Un atacante potencial que se infiltra en este sistema solo ganaría una calculadora. El costo de asegurar un sistema de este tipo probablemente sería mayor que El costo de una violación.

En el otro extremo del espectro, es posible que desee proteger la confidencialidad de los datos secretos en de la manera más completa posible, superando cualquier otra consideración. En este caso, un apro- Una respuesta importante sería la destrucción total de los datos (borrar de forma segura los archivos, destruir los discos duros, los bits, la disolución de estos bits ácidos y pronto). Si existe un requisito adicional adicional mencionar que los datos deben mantenerse almacenados para su uso futuro (aunque no necesariamente disponibles), y si el costo aún no es un factor, entonces un punto de partida sería almacenar los datos en iridio-platino placas de aleación almacenadas en búnkeres a prueba de bombas debajo de varias montañas del mundo, cada una de las cuales siendo (por supuesto) completamente secreto y custodiado por ejércitos enteros.

Aunque estos ejemplos pueden parecer extremos, sin embargo, serían una respuesta adecuada a ciertos riesgos definidos, en la medida en que son el resultado de un proceso de pensamiento que tiene en cuenta los objetivos para alcanzar y las restricciones para cumplir. Cuando viene de una decisión razonada, seguridad de la nariz La política es más o menos respetable que cualquier otra.

Volviendo a un caso más típico, un sistema de información puede segmentarse en coherente y en su mayoría subsistemas independientes. Cada subsistema tendrá sus propios requisitos y restricciones, por lo que la evaluación de riesgos y el diseño de la política de seguridad deben realizarse por separado para cada. Un buen principio a tener en cuenta es que una pequeña superficie de ataque es más fácil de defender que un el Grande. La organización de la red también debe diseñarse en consecuencia: los servicios sensibles debe concentrarse en un pequeño número de máquinas, y estas máquinas solo deben ser Accesible a través de un número mínimo de rutas o puntos de control. La lógica es sencilla: es más fácil asegurar estos puntos de control que asegurar todas las máquinas sensibles contra la totalidad de mundo exterior. Es en este punto que la utilidad del filtrado de red (incluso por firewalls) se hace evidente. Este filtrado puede implementarse con hardware dedicado pero de una manera más simple y Una solución más flexible es utilizar un firewall de software como el integrado en el kernel de Linux.

Page 178

7.2. Posibles medidas de seguridad

Como se explicó en la sección anterior, no hay una respuesta única a la pregunta de cómo asegurar Kali Linux Todo depende de cómo lo use y de lo que esté tratando de proteger.

7.2.1 En un servidor

Si ejecuta Kali Linux en un servidor de acceso público, lo más probable es que desee proteger el servidor de red vicios cambiando las contraseñas predeterminadas que puedan estar configuradas (ver sección 7.3, " Asegurando la red-Servicios de trabajo "[página 153]) y posiblemente también restringiendo su acceso con un cortafuegos (consulte la sección sección 7.4 , " Firewall o filtrado de paquetes "[Página 153]).

Si distribuye cuentas de usuario directamente en el servidor o en uno de los servicios, desea asegúrese de establecer contraseñas seguras (deben resistir los ataques de fuerza bruta). Al mismo tiempo, es posible que desee configurar *fail2ban* , lo que hará que sea mucho más difícil usar contraseñas de fuerza bruta la red (al filtrar las direcciones IP que exceden el límite de intentos fallidos de inicio de sesión). Instalar en pc *fail2ban* con `apt update` seguido de `apt install fail2ban` .

Si ejecuta servicios web, es probable que desee alojarlos a través de HTTPS para evitar la interconexión de red. diarios para detectar su tráfico (que puede incluir cookies de autenticación).

7.2.2 En una computadora portátil

La computadora portátil de un probador de penetración no está sujeta a los mismos riesgos que un servidor público: por ejemplo, es menos probable que estés sujeto a escaneos aleatorios de kiddies de script e incluso cuando lo estás, probablemente no tendrá ningún servicio de red habilitado.

El riesgo real a menudo surge cuando viaja de un cliente a otro. Por ejemplo, tu laptop podría ser robado mientras viaja o incautado por la aduana. Es por eso que lo más probable es que quieras usar full cifrado de disco (consulte la sección 4.2.2 , " Instalación en un sistema de archivos completamente cifrado "[Página 85]) y posiblemente también configure la función "arma nuclear" (consulte " Agregar una contraseña nuclear para mayor seguridad "[Página 246]): la fecha que ha recogido durante su compromiso es confidente y requiere la mayor parte proteccion.

También es posible que necesite reglas de firewall (consulte la sección 7.4 , "Cortafuegos o filtrado de paquetes"[Página 153]) pero no para el mismo propósito que en el servidor. Es posible que desee prohibir todo el tráfico saliente, excepto el tráfico generado por su acceso VPN. Esto se entiende como una red de seguridad, de modo que cuando la VPN está inactiva, inmediatamente lo notas (en lugar de recurrir al acceso a la red local). De esa manera, tu no divulgue las direcciones IP de sus clientes cuando navega por la web o realiza otras actividades en línea ocupaciones. Además, si está realizando un compromiso interno local, es mejor permanecer en control de toda su actividad para reducir el ruido que crea en la red, que puede alertar al cliente y sus sistemas de defensa.

Page 179

7.3. Asegurando los servicios de red

En general, es una buena idea deshabilitar los servicios que no utiliza. Kali hace que sea fácil hacer esto ya que la mayoría de los servicios de red están deshabilitados por defecto.

Mientras los servicios permanezcan deshabilitados, no representan ninguna amenaza de seguridad. Sin embargo, debes ser cuidado cuando los habilitas porque:

- no hay un firewall por defecto, por lo que si escuchan en todas las interfaces de red, son efectivamente disponible públicamente.
- algunos servicios no tienen credenciales de autenticación y le permiten configurarlos en el primer uso; otros

tener credenciales predeterminadas (y por lo tanto ampliamente conocidas) preestablecidas. Asegúrese de (re) establecer cualquier contraseña a algo que solo tú sabes.

- muchos servicios se ejecutan como root con privilegios de administrador completos, por lo que las consecuencias de una Por lo tanto, el acceso restringido o una violación de la seguridad suelen ser graves.

Credenciales predeterminadas No enumeraremos aquí todas las herramientas que vienen con credenciales predeterminadas, en su lugar, debe consulte el archivo README.Debian de los paquetes respectivos, así como docs.kali.org [1] y tools.kali.org [2] para ver si el servicio necesita un cuidado especial para garantizarlo.

Si ejecuta en modo en vivo, la contraseña de la cuenta raíz es " *toor* ". Así deberías no habilite SSH antes de cambiar la contraseña de la cuenta raíz, o antes de tener modificó su configuración para no permitir inicios de sesión basados en contraseña.

También tenga en cuenta que el proyecto BeEF (del paquete ya instalado *beef-xss*) también es se sabe que tiene credenciales predeterminadas de usuario "beef", contraseña "beef") codificadas en su archivo de configuración de falla.

7.4. Cortafuegos o filtrado de paquetes

Un *firewall* es un equipo informático con hardware, software o ambos que analiza el paquetes de red entrantes o salientes (entrando o saliendo de una red local) y solo permite a través de aquellos que coinciden con ciertas condiciones predefinidas.

Una puerta de enlace de red de filtrado es un tipo de firewall que protege una red completa. Es usual instalado en una máquina dedicada configurada como puerta de enlace para la red para que pueda analizar todo paquetes que pasan y salen de la red. Alternativamente, un servidor local de cortafuegos ofrece un servicio que se ejecuta en una máquina en particular para filtrar o limitar el acceso a algunos servicios en esa máquina, o posiblemente para evitar conexiones salientes por software malicioso que un usuario podría, voluntariamente o no, han instalado

[1] https://docs.kali.org
[2] https://tools.kali.org

El kernel de Linux incorpora el firewall de *netfilter* . No hay una solución llave en mano para configurar cualquier firewall ya que los requisitos de red y de usuario difieren. Sin embargo, puede controlar *netfilter* desde el usuario espacio con los comandos iptables e ip6tables . La diferencia entre estos dos comandos es que el primero funciona para redes IPv4, mientras que el segundo funciona en IPv6. Ya que ambas redes las pilas de protocolos probablemente existirán durante muchos años, ambas herramientas deberán usarse en paralelo. También puede usar la excelente herramienta fwbuilder basada en GUI , que proporciona una representación gráfica ción de las reglas de filtrado.

Independientemente de cómo decida configurarlo, *netfilter* es la implementación de firewall de Linux, así que tomemos un mira de cerca cómo funciona.

7.4.1. Comportamiento de Netfilter

Netfilter utiliza cuatro tablas independientes, que almacenan reglas que regulan tres tipos de operaciones en paquetes:

- el filtro se refiere a las reglas de filtrado (aceptar, rechazar o ignorar un paquete);
- nat (Network Address Translation) se refiere a la traducción de las direcciones de origen o destino y puertos de paquetes;
- mangle se refiere a otros cambios en los paquetes IP (incluido el campo ToS — *Tipo de servicio* — y opciones);
- raw permite otras modificaciones manuales en los paquetes antes de que lleguen a la ruta de conexión sistema de ing.

Cada tabla contiene listas de reglas llamadas *cadenas* . El firewall usa cadenas estándar para manejar paquetes basado en circunstancias predefinidas. El administrador puede crear otras cadenas, que solo ser utilizado cuando se refiere por una de las cadenas estándar (ya sea directa o indirectamente).

La tabla de filtros tiene tres cadenas estándar:

- ENTRADA: se refiere a los paquetes cuyo destino es el firewall en sí;
- SALIDA: se refiere a los paquetes emitidos por el firewall;
- ADELANTE: se refiere a los paquetes que pasan a través del firewall (que no es su origen

ni su destino).

La tabla nat también tiene tres cadenas estándar:

- PREROUTING: para modificar paquetes tan pronto como lleguen;
- POSTROUTING: para modificar paquetes cuando están listos para seguir su camino;
- SALIDA: para modificar los paquetes generados por el firewall en sí.

Estas cadenas se ilustran en la Figura 7.1, " Cómo se *llaman las* cadenas de *Netfilter* " [página 155].

Figura 7.1 *Cómo se* llaman las *cadenas de* Netfilter

Cada cadena es una lista de reglas; cada regla es un conjunto de condiciones y una acción a realizar cuando el Se cumplen las condiciones. Al procesar un paquete, el firewall escanea la cadena apropiada, una regla después de otro, y cuando se cumplen las condiciones para una regla, salta (de ahí la opción -j en el comandos) a la acción especificada para continuar el procesamiento. Los comportamientos más comunes son stan-Dardizedanddedicatedactionsexistforthemhem. Tomar una de las acciones estándar interrumpe la procesamiento de la cadena, ya que el destino de los paquetes ya está sellado (salvo una excepción mencionada abajo). A continuación se enumeran las acciones de *Netfilter* .

- ACEPTAR: permite que el paquete siga su camino.
- RECHAZAR: rechazar el paquete con un paquete de error de protocolo de mensajes de control de Internet (ICMP) (la opción --reject-with *type* de iptables determina el tipo de error a enviar).
- DROP: borra (ignora) el paquete.
- LOG: registra (a través de syslogd) un mensaje con una descripción del paquete. Tenga en cuenta que esta acción no interrumpe el procesamiento y la ejecución de la cadena continúa en la siguiente regla, que es por qué registrar paquetes rechazados requiere BLOG y REJECT / DROPrule. Común Los parámetros asociados con el registro incluyen:
  - - nivel de registro, con advertencia de valor predeterminado, indica el nivel de gravedad de syslog .
  - --log-prefix permite especificar un prefijo de texto para diferenciar entre mensajes registrados.
  - --log-tcp-secuencia, --log-tcp-options y --log-ip-options indican datos adicionales que deben incluirse integrado en el mensaje: respectivamente, el número de secuencia TCP, las opciones TCP y Opciones de IP.
- ULOG: registre un mensaje a través de ulogd , que puede adaptarse mejor y ser más eficiente que syslogd para manejar grandes cantidades de mensajes; tenga en cuenta que esta acción, como LOG, también convierte el procesamiento a la siguiente regla en la cadena de llamada.
- *nombre_cadena* : salta a la cadena dada y evalúa sus reglas.

- RETURN: interrumpe el procesamiento de la cadena actual y vuelve a la cadena de llamada; en caso la cadena actual es estándar, no hay una cadena de llamada, por lo que la acción predeterminada (definida con la opción -P para iptables) se ejecuta en su lugar.

- SNAT (solo en la tabla nat): aplica la *traducción de direcciones de red de origen* (SNAT). Opciones extra describa los cambios exactos que se aplicarán, incluida la opción --to-source *address* : *port* , que define la nueva dirección IP y / o puerto de origen.

• DNAT (solo en la tabla nat): aplica la *traducción de direcciones de red de destino* (DNAT). Op op-
las opciones describen los cambios exactos para aplicar, incluida la *dirección de* destino : opción de *puerto* ,
que define la nueva dirección IP y / o puerto de destino.

• MASQUERADE (solo en la tabla nat): aplique el *enmascaramiento* (un caso especial de *Source NAT*).

• REDIRECT (solo en la tabla nat): redirige de forma transparente un paquete a un puerto determinado del
cortafuegos en sí; esto se puede usar para configurar un proxy web transparente que funcione sin problemas
figuración en el lado del cliente, ya que el cliente piensa que se conecta con el destinatario, mientras que el
Las comunicaciones en realidad pasan por el proxy. La opción --to-ports *port (s)* indica el
puerto, o rango de puertos, donde los paquetes deben ser redirigidos.

Otras acciones, particularmente aquellas relacionadas con la tabla de cambios, están fuera del alcance de este texto.
Las páginas de comando man iptables (8) e ip6tables (8) tienen una lista completa.

¿Qué es ICMP? *El Protocolo de mensajes de control de Internet* (ICMP) es el protocolo utilizado para transmitir datos auxiliares.
información sobre comunicaciones. Prueba la conectividad de red con el comando ping
mand, que envía un mensaje de *solicitud de eco* ICMP , que el destinatario debe enviar
responda con un mensaje de *respuesta de eco* ICMP . Señala un cortafuegos que rechaza un paquete, indi-
detecta un desbordamiento en un búfer de recepción, propone una ruta mejor para los siguientes paquetes en el
conexión, y así sucesivamente. Este protocolo está definido por varios documentos RFC. RFC777
y RFC792 fueron los primeros, pero muchos otros ampliaron y / o revisaron el protocolo.

[2] http://www.faqs.org/rfcs/rfc777.html

[2] http://www.faqs.org/rfcs/rfc792.html

Como referencia, un búfer de recepción es una pequeña zona de memoria que almacena datos entre el tiempo
llega desde la red y el tiempo que el kernel lo maneja. Si esta zona está llena, nueva
no se pueden recibir datos e ICMP señala el problema para que el emisor pueda reducir la velocidad
reducir su velocidad de transferencia (que idealmente debería alcanzar un equilibrio después de un tiempo).

Tenga en cuenta que aunque una red IPv4 puede funcionar sin ICMP, ICMPv6 es estrictamente re
requerido para una red IPv6, ya que combina varias funciones que estaban, en el IPv4
mundo, extendido a través de ICMPv4, *Protocolo de Membresía de Grupo de Internet* (IGMP) y *Ad-
Protocolo de resolución de vestimenta* (ARP). ICMPv6 se define en RFC4443.

[2] http://www.faqs.org/rfcs/rfc4443.html

7.4.2. Sintaxis de iptables y ip6tables

Los comandos iptables e ip6tables se usan para manipular tablas, cadenas y reglas. Su
-t opción de *tabla* indica en qué tabla operar (de forma predeterminada, filtro).

Comandos

Las principales opciones para interactuar con las cadenas se enumeran a continuación:

• -L *cadena* enumera las reglas de la cadena. Esto se usa comúnmente con la opción -n para deshabilitar
resolución de nombre (por ejemplo, iptables -n -L INPUT mostrará las reglas relacionadas con
próximos paquetes).

• -N *cadena* crea *una* nueva *cadena* . Puede crear nuevas cadenas para un número de propósitos, incluidos
probar un nuevo servicio de red o defenderse de un ataque de red.

• -X *chain* elimina una *cadena* vacía y sin usar (por ejemplo, iptables -X ddos-attack).

• -Una *regla de cadena* agrega una regla al final de la cadena dada. Recuerda que las reglas son procesadas
de arriba a abajo, así que asegúrese de tener esto en cuenta al agregar reglas.

• -I *encadenar regla_num regla* inserta una *regla* antes de *otro* número *número_regla* . Aswiththe-Aoption,
tenga en cuenta el orden de procesamiento al insertar nuevas reglas en una cadena.

• -D *chain rule_num* (o -D *chain rule*) elimina una regla en una cadena; la primera sintaxis identifica el
regla que se eliminará por su número (iptables -L --line-numbers mostrará estos números-
bers), mientras que este último lo identifica por su contenido.

• -F *cadena* enjuaga una cadena (elimina todas sus reglas). Por ejemplo, para eliminar todas las reglas relacionadas
a los paquetes salientes, ejecutarías iptables -F OUTPUT . Si no se menciona ninguna cadena, todos los
Se eliminan las reglas de la tabla.

• La *acción de cadena* -P define la acción por defecto, o "política" para una cadena dada; tenga en cuenta que solo stan-

Las cadenas Dard pueden tener esa política. Para eliminar todo el tráfico entrante de forma predeterminada, debe ejecutar iptables -P INPUT DROP .

Reglas

Cada regla se expresa como *condiciones* -j *action action_options* . Si se describen varias condiciones en la misma regla, entonces el criterio es la conjunción (*AND* lógico) de las condiciones, que está en menos restrictivo que cada condición individual.

La condición del *protocolo* -p coincide con el campo de protocolo del paquete IP. Los valores mas comunes son tcp, udp, icmp e icmpv6. Esta condición puede complementarse con condiciones en el TCP puertos, con cláusulas como --source-port *port* y --destination-port *port* .

Page 184

Negar condiciones Prefijar una condición con un signo de exclamación niega la condición. Por ejemplo, negar una condición en la opción -p coincide con "cualquier paquete con un protocolo diferente que el especificado ". Este mecanismo de negación se puede aplicar a todas las demás condiciones. también.

La condición -s *dirección* o -s *red / máscara* coincide con la dirección de origen del paquete. Corre- espontáneamente, -d *dirección* o -d *red / máscara* coincide con la dirección de destino.

La condición de *interfaz* -i selecciona los paquetes que provienen de la interfaz de red dada. -o *interfaz* selecciona los paquetes que salen en una interfaz específica.

La condición de *estado* --state coincide con el estado de un paquete en una conexión (esto requiere ipt_ módulo kernel conntrack , para el seguimiento de la conexión). El estado NUEVO describe un paquete que comienza una nueva conexión, ESTABLECIDA coincide con paquetes que pertenecen a una conexión ya existente, y RELATED hace coincidir los paquetes que inician una nueva conexión relacionada con una existente (que es útil para las conexiones de datos ftp en el modo "activo" del protocolo FTP).

Hay muchas opciones disponibles para iptables e ip6tables y dominarlas todas requiere Una gran cantidad de estudio y experiencia. Sin embargo, una de las opciones que usará con mayor frecuencia es el uno para bloquear el tráfico de red malicioso de un host o rango de hosts. Por ejemplo, para bloquear silenciosamente Tráfico entrante desde la dirección IP 10.0.1.5 y la subred 31.13.74.0/24 clase C:

```
# iptables -A INPUT -s 10.0.1.5 -j DROP
# iptables -A INPUT -s 31.13.74.0/24 -j DROP
# iptables -n -L INPUT
ENTRADA de cadena (política ACEPTAR)
objetivo     fuente de opt prot                destino
SOLTAR       todos - 10.0.1.5                  0.0.0.0/0
SOLTAR       todos - 31.13.74.0/24             0.0.0.0/0
```

Otro comando de uso común de iptables es permitir el tráfico de red para un servicio específico o Puerto. Para permitir que los usuarios se conecten a SSH, HTTP e IMAP, puede ejecutar los siguientes comandos:

```
# iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
# iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
# iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT
# iptables -n -L INPUT
ENTRADA de cadena (política ACEPTAR)
objetivo     fuente de opt prot                destino
SOLTAR       todos - 10.0.1.5                  0.0.0.0/0
SOLTAR       todos - 31.13.74.0/24             0.0.0.0/0
ACEPTAR      tcp - 0.0.0.0/0                   0.0.0.0/0          estado NUEVO tcp dpt: 22
ACEPTAR      tcp - 0.0.0.0/0                   0.0.0.0/0          estado NUEVO tcp dpt: 80
ACEPTAR      tcp - 0.0.0.0/0                   0.0.0.0/0          estado NUEVO tcp dpt: 143
```

Se considera una buena *higiene de la* computadora limpiar las reglas viejas e innecesarias. Lo más fácil La forma de eliminar las reglas de iptables es hacer referencia a las reglas por número de línea, que puede recuperar con

Page 185

la opción --line-numbers. Sin embargo, tenga cuidado: al soltar una regla, se volverán a numerar todas las reglas que aparezcan más abajo en la cadena.

```
# iptables -n -L INPUT --line-numbers
```

```
ENTRADA de cadena (política ACEPTAR)
objetivo numérico        fuente de opt prot                    destino
1        SOLTAR          todos - 10.0.1.5                      0.0.0.0/0
2        SOLTAR          todos - 31.13.74.0/24                 0.0.0.0/0
3        ACEPTAR         tcp - 0.0.0.0/0                       0.0.0.0/0          estado NUEVO tcp dpt: 22
4 4      ACEPTAR         tcp - 0.0.0.0/0                       0.0.0.0/0          estado NUEVO tcp dpt: 80
5 5      ACEPTAR         tcp - 0.0.0.0/0                       0.0.0.0/0          estado NUEVO tcp dpt: 143
# iptables -D INPUT 2
# iptables -D INPUT 1
# iptables -n -L INPUT --line-numbers
ENTRADA de cadena (política ACEPTAR)
objetivo numérico        fuente de opt prot                    destino
1        ACEPTAR         tcp - 0.0.0.0/0                       0.0.0.0/0          estado NUEVO tcp dpt: 22
2        ACEPTAR         tcp - 0.0.0.0/0                       0.0.0.0/0          estado NUEVO tcp dpt: 80
3        ACEPTAR         tcp - 0.0.0.0/0                       0.0.0.0/0          estado NUEVO tcp dpt: 143
```

Existen condiciones más específicas, dependiendo de las condiciones genéricas descritas anteriormente. por
Para obtener más información, consulte iptables (8) e ip6tables (8)

7.4.3. Crear reglas

Cada creación de regla requiere una invocación de iptables o ip6tables . Escribiendo estos comandos
manualmente puede ser tedioso, por lo que las llamadas generalmente se almacenan en un script para que el sistema se automatice
configurado de la misma manera cada vez que la máquina arranca. Este script puede ser escrito a mano.
pero también puede ser interesante prepararlo con una herramienta de alto nivel como fwbuilder .

```
# apt install fwbuilder
```

El principio es simple. En el primer paso, describa todos los elementos que estarán involucrados en el
reglas reales:

- El firewall en sí, con sus interfaces de red.
- Las redes, con sus rangos de IP correspondientes.
- Los servidores
- Los puertos que pertenecen a los servicios alojados en los servidores.

Luego, cree las reglas con simples acciones de arrastrar y soltar en los objetos como se muestra en la Figura 7.2 ,
" Ventana principal de Fwbuilder " [página 160]. Algunos menús contextuales pueden cambiar la condición (negativo-
ing, por ejemplo). Entonces la acción debe ser elegida y configurada.

En lo que respecta a IPv6, puede crear dos conjuntos de reglas distintos para IPv4 e IPv6, o crear
solo uno y deje que fwbuilder traduzca las reglas de acuerdo con las direcciones asignadas a los objetos.

Figura 7.2 *Ventana principal de Fwbuilder*

fwbuilder generará un script que configurará el firewall de acuerdo con las reglas que tenga
definido. Su arquitectura modular da la capacidad de generar sistemas de escritura de guiones diferentes sistemas

incluyendo iptables para Linux, ipf para FreeBSD y pf para OpenBSD.

7.4.4. Instalar las reglas en cada arranque

Para implementar las reglas del firewall cada vez que se inicia la máquina, deberá registrarse el script de configuración en una directiva ascendente del archivo / etc / network / interfaces . En el siguiente Por ejemplo, el script se almacena en /usr/local/etc/arrakis.fw .

```
auto eth0
iface eth0 inet static
        dirección 192.168.0.1
        red 192.168.0.0
        máscara de red 255.255.255.0
        transmitida 192.168.0.255
        arriba /usr/local/etc/arrakis.fw
```


Este ejemplo supone que está usando *ifupdown* para configurar las interfaces de red. Si tu están usando otra cosa (como *NetworkManager* o *systemd-networkd*), luego consulte sus respectivos documentación para descubrir formas de ejecutar una secuencia de comandos después de que aparezca la interfaz.

7.5. Monitoreo y registro

La confidencialidad y protección de los datos es un aspecto importante de la seguridad, pero es igualmente importante. para garantizar la disponibilidad de los servicios. Como administrador y profesional de seguridad, debe asegurarse que todo funciona como se espera, y es su responsabilidad detectar comportamientos anómalos y degradación del servicio de manera oportuna. El software de monitoreo y registro juega un papel clave en este aspecto de seguridad, que proporciona información sobre lo que está sucediendo en el sistema y la red.

En esta sección, revisaremos algunas herramientas que pueden usarse para monitorear varios aspectos de un Kali sistema.

7.5.1. Supervisión de registros con logcheck

El programa logcheck monitorea los archivos de registro cada hora de manera predeterminada y envía mensajes de registro inusuales en correos electrónicos al administrador para su posterior análisis.

La lista de archivos monitoreados se almacena en /etc/logcheck/logcheck.logfiles . Los valores por defecto funciona bien si el archivo /etc/rsyslog.conf no se ha revisado por completo.

Logcheck puede informar en varios niveles de detalle: *paranoico* , *servidor* y *estación de trabajo* . *paranoico* es *muy* detallado y probablemente debería restringirse a servidores específicos como firewalls. *el servidor* es el predeterminado modo y se recomienda para la mayoría de los servidores. *la estación de trabajo* obviamente está diseñada para estaciones de trabajo y es extremadamente conciso, ya que filtra más mensajes que las otras opciones.

En los tres casos, logcheck probablemente debería personalizarse para excluir algunos mensajes adicionales (pendiente de los servicios instalados), a menos que realmente desee recibir lotes por hora de largos correos electrónicos interesantes Dado que el mecanismo de selección de mensajes es bastante complejo, / usr / share / doc / logcheck-database / README.logcheck-database.gz es una lectura obligatoria, si es desafiante.

Las reglas aplicadas se pueden dividir en varios tipos:

- aquellos que califican un mensaje como un intento de craqueo (almacenado en un archivo en / etc / logcheck / cracking.d / directorio);
- intentos de craqueo ignorados (/etc/logcheck/cracking.ignore.d/);
- aquellos que clasifican un mensaje como alerta de seguridad (/etc/logcheck/violations.d/);
- alertas de seguridad ignoradas (/etc/logcheck/violations.ignore.d/);
- finalmente, los que se aplican a los mensajes restantes (considerados como *eventos del sistema*).

Los archivos *ignore.d* se usan para (obviamente) ignorar los mensajes. Por ejemplo, un mensaje etiquetado como craqueo intento o una alerta de seguridad (siguiendo una regla almacenada en /etc/logcheck/violations.d/myfile archivo) solo puede ser ignorado por una regla en /etc/logcheck/violations.ignore.d/myfile o / etc / logcheck / violaciones.ignore.d / myfile- archivo de *extensión* .

Un evento del sistema siempre se señala a menos que haya una regla en /etc/logcheck/ignore.d. {paranoid, server, workstation} / directorios indica que el evento debe ignorarse. Por supuesto, el solo los directorios tomados en cuenta son los correspondientes a niveles de verbosidad iguales o mayores que el modo de operación seleccionado.

7.5.2. Monitoreo de actividad en tiempo real

top es una herramienta interactiva que muestra una lista de los procesos actualmente en ejecución. La ordenación predeterminada se basa en la cantidad actual de uso del procesador y se puede obtener con la tecla P. Otro tipo los pedidos incluyen una clasificación por memoria ocupada (tecla M), por tiempo total de procesador (tecla T) y por proceso identificador (tecla N). La tecla k mata un proceso al ingresar su identificador de proceso. La tecla r cambia La prioridad de un proceso.

Cuando el sistema parece estar sobrecargado, top es una gran herramienta para ver qué procesos son competitivos. ing para tiempo de procesador o consumir demasiada memoria. En particular, a menudo es interesante comprobar si los procesos que consumen recursos coinciden con los servicios reales que conoce la máquina anfitrión. Un proceso desconocido que se ejecuta como el usuario "www-data" realmente debería sobresalir y ser investigador. tigado ya que es probablemente una instancia de software instalado y ejecutado en el sistema a través de Una vulnerabilidad en una aplicación web.

top es una herramienta muy flexible y su página de manual brinda detalles sobre cómo personalizar su pantalla y adaptarlo a tus necesidades y hábitos personales.

La herramienta gráfica gnome-system-monitor es similar a top y proporciona aproximadamente la misma función. Tures.

7.5.3. Detectando cambios

Una vez que se instala y configura un sistema, la mayoría de los archivos del sistema deben permanecer relativamente estáticos hasta El sistema está actualizado. Por lo tanto, es una buena idea monitorear los cambios en los archivos del sistema ya que Un cambio inesperado puede ser motivo de alarma y debe investigarse. Esta sección presenta un Algunas de las herramientas más comunes utilizadas para monitorear archivos del sistema, detectar cambios y, opcionalmente, notificar usted como administrador del sistema.

Auditoría de paquetes con dpkg --verify

dpkg --verify (o dpkg -V) es una herramienta interesante ya que muestra los archivos del sistema que tienen modificado (potencialmente por un atacante), pero esta salida debe tomarse con un grano de sal. A

hacer su trabajo, dpkg se basa en sumas de verificación almacenadas en su propia base de datos que se almacena en el disco duro (se encuentra en / var / lib / dpkg / info / *package* .md5sums). Por lo tanto, un atacante completo modificará estos archivos para que contengan las nuevas sumas de comprobación para los archivos subvertidos o un atacante avanzado comprometerá el paquete en su espejo Debian. Para protegerse contra esta clase de ataque, use Sistema de verificación de firma digital de APT (consulte la sección 8.3.6 , " Validación de la autenticidad del paquete " [página 202]) para verificar adecuadamente los paquetes.

¿Qué es un archivo? ¿Huella dactilar? Como recordatorio: una huella digital es un valor, a menudo un número (aunque en hexadecimal notation), que contiene una especie de firma para el contenido de un archivo. Esta firma es calculado con un algoritmo (MD5 o SHA1 son ejemplos bien conocidos) que más o menos garantiza que incluso el más mínimo cambio en el contenido del archivo dará como resultado un cambio de huella digital; Esto se conoce como el "efecto avalancha". Un simple numérico la huella digital sirve como prueba de fuego para verificar si el contenido de un archivo tiene ha sido alterado Estos algoritmos no son reversibles; en otras palabras, para la mayoría de ellos, saber una huella digital no permite encontrar los contenidos correspondientes. Matemáticas recientes Los avances matemáticos parecen debilitar el carácter absoluto de estos principios, pero su uso no se pone en tela de juicio hasta ahora, ya que la creación de diferentes contenidos produce el mismo La huella dactilar todavía parece ser una tarea bastante difícil.

La ejecución de dpkg -V verificará todos los paquetes instalados e imprimirá una línea para cada archivo que falla verificación. Cada personaje denota una prueba en algunos metadatos específicos. Desafortunadamente, dpkg hace no almacena los metadatos necesarios para la mayoría de las pruebas y, por lo tanto, generará signos de interrogación para ellos. Canalla- De manera reciente, solo la prueba de suma de comprobación puede arrojar un 5 en el tercer carácter (cuando falla).

```
# dpkg -V
??5?????? /lib/systemd/system/ssh.service
??5?????? c /etc/libvirt/qemu/networks/default.xml
??5?????? c /etc/lvm/lvm.conf
??5?????? c / etc / sal / lista
```

En el ejemplo anterior, dpkg informa un cambio en el archivo de servicio de SSH que el administrador realizó a el archivo empaquetado en lugar de usar un `/etc/systemd/system/ssh.service` override apropiado (que se almacenaría debajo de `/ etc` como debería ser cualquier cambio de configuración). También enumera múltiples archivos de configuración (identificados por la letra "c" en el segundo campo) que habían sido legítimamente modificado.

Monitoreo de archivos: AIDE

La herramienta Advanced Intrusion Detection Environment (AIDE) verifica la integridad del archivo y detecta cualquier cambiar contra una imagen previamente grabada del sistema válido. La imagen se almacena como una base de datos. (`/var/lib/aide/aide.db`) que contiene la información relevante sobre todos los archivos del sistema (finger- impresiones, permisos, marcas de tiempo, etc.).

Puede instalar AIDE ejecutando `apt update` seguido de `apt install aide` . Primero iniciará ize la base de datos con `aideinit` ; luego se ejecutará diariamente (a través del script `/etc/cron.daily/aide`) para

Verifique que nada relevante haya cambiado. Cuando se detectan cambios, AIDE los registra en archivos de registro (`/var/log/aide/*.log`) y envía sus hallazgos al administrador por correo electrónico.

Protección de la base de datos Dado que AIDE utiliza una base de datos local para comparar los estados de los archivos, la validez de Sus resultados están directamente vinculados a la validez de la base de datos. Si un atacante obtiene root permisos en un sistema comprometido, podrán reemplazar la base de datos y cubrir sus huellas Una forma de evitar esta subversión es almacenar los datos de referencia. en medios de almacenamiento de solo lectura.

Puede usar las opciones en `/ etc / default / aide` para modificar el comportamiento del paquete de *ayuda* . los La configuración adecuada de AIDE se almacena en `/etc/aide/aide.conf` y `/etc/aide/aide.conf.d/` (ac- Por lo general, estos archivos solo los utiliza `update-aide.conf` para generar `/var/lib/aide/aide.conf.autogenerado`). La configuración indica qué propiedades de qué archivos deben verificarse. Por ejemplo, el contenido de los archivos de registro cambia de forma rutinaria, y dichos cambios pueden ignorarse siempre que ya que los permisos de estos archivos permanecen igual, pero tanto el contenido como los permisos del ejecutable Los programas deben ser constantes. Aunque no es muy complejo, la sintaxis de configuración no es completamente intuitivo y recomendamos leer la página del manual `aide.conf (5)` para más detalles.

Una nueva versión de la base de datos se genera diariamente en `/var/lib/aide/aide.db.new` ; si todo registrado los cambios fueron legítimos, se pueden usar para reemplazar la base de datos de referencia.

Tripwire es muy similar a AIDE; Incluso la sintaxis del archivo de configuración es casi la misma. El principal Además, *Tripwire* proporciona un mecanismo para firmar el archivo de configuración para que un atacante no puede hacer que apunte a una versión diferente de la base de datos de referencia.

Samhain también ofrece características similares, así como algunas funciones para ayudar a detectar rootkits (consulte el barra lateral "Los *CheckSecurity* y *chkrootkit* / *rkhunter* paquetes "[página 164]). También se puede implementar globalmente en una red y registrar sus rastros en un servidor central (con una firma).

La *verificación de seguridad* y *chkrootkit* / *rkhunter* paquetes

checksecurity consta de varios pequeños scripts que realizan comprobaciones básicas en el sistema (buscando contraseñas vacías, nuevos archivos setuid, etc.) y le advierte si estos Se detectan condiciones. A pesar de su nombre explícito, no debe confiar únicamente en él para asegúrese de que un sistema Linux sea seguro.

Los *chkrootkit* y *rkhunter* paquetes detectan ciertos *rootkits* potencialmente instalados en el sistema. Como recordatorio, estas son piezas de software diseñadas para ocultar el compromiso. Mise de un sistema manteniendo discretamente el control de la máquina. Las pruebas no son 100 por ciento confiable, pero generalmente pueden llamar su atención sobre posibles problemas.

7.6. Resumen

En este capítulo, analizamos el concepto de políticas de seguridad, destacando varios puntos para tenga en cuenta al definir dicha política y describir algunas de las amenazas para su sistema y para usted personalmente como profesional de seguridad. También hablamos sobre medidas de seguridad para computadoras portátiles y de escritorio

como firewalls y filtrado de paquetes. Finalmente, revisamos las herramientas y estrategias de monitoreo y mostramos cómo implementarlos mejor para detectar posibles amenazas a su sistema.

Consejos resumidos:

- Tómese el tiempo para definir una política de seguridad integral.
- Si está ejecutando Kali en un servidor de acceso público, cambie las contraseñas predeterminadas para servicios que pueden configurarse (ver sección 7.3, " Asegurando los servicios de red "[Página 153]) y restringir su acceso con un firewall (consulte la sección 7.4 , " Cortafuegos o filtrado de paquetes " [página 153]) antes de lanzarlos.
- Utilice *fail2ban para* detectar y bloquear contraseñas de adivinanzas y ataques automáticos ataques
- Si ejecuta servicios web, hágalos a través de HTTPS para evitar que los intermediarios de la red olfatear su tráfico (que puede incluir cookies de autenticación).
- El riesgo real a menudo surge cuando viaja de un cliente a otro. Por ejemplo, tu regazo la parte superior podría ser robada durante el viaje o incautada por la aduana. Prepárate para estas desafortunadas pos- posibilidades mediante el uso de cifrado de disco completo (consulte la sección 4.2.2 , " Instalación en un encriptado completo Sistema de archivos "[Página 85]) y tenga en cuenta la función nuclear (consulte" Agregar una contraseña nuclear para Seguridad adicional "[página 246]) para proteger los datos de sus clientes.
- Implementar reglas de firewall (ver sección 7.4, " Firewall o filtrado de paquetes "[Página 153]) para prohibir todo el tráfico saliente, excepto el tráfico generado por su acceso VPN. Thisismeantasasafety net, de modo que cuando la VPN está inactiva, la notas inmediatamente (en lugar de volver a la acceso a la red local).
- Desactive los servicios que no usa. Kali facilita hacer esto ya que toda la red externa Los servicios están deshabilitados por defecto.
- El kernel de Linux incorpora el firewall de *netfilter* . No existe una solución llave en mano para configurar cualquier firewall, ya que los requisitos de red y de usuario difieren. Sin embargo, puedes controlar *netfilter* desde el espacio del usuario con los comandos `iptables` e `ip6tables` .
- El programa `logcheck` monitorea los archivos de registro cada hora por defecto y envía mensajes de registro inusuales. sabios en correos electrónicos al administrador para su posterior análisis.
- `top` es una herramienta interactiva que muestra una lista de los procesos actualmente en ejecución.
- `dpkg --verify` (o `dpkg -V`) muestra los archivos del sistema que se han modificado (potencialmente por un atacante), pero se basa en sumas de comprobación, que pueden ser subvertidas por un atacante inteligente.
- La herramienta Advanced IntrusionDetectionEnvironment (AIDE) verifica la integridad y detección de archivos cualquier cambio contra una imagen previamente grabada del sistema válido.
- Tripwire es muy similar a AIDE pero utiliza un mecanismo para firmar el archivo de configuración, de modo que un atacante no puede hacer que apunte a una versión diferente de la base de datos de referencia.
- Considere el uso de `rkhunter` , `checksecurity` y `chkrootkit` para ayudar a detectar rootkits en tu sistema.

En el próximo capítulo, vamos a profundizar en los fundamentos de Debian y la gestión de paquetes. usted comprenderá rápidamente el poder detrás de las raíces de Debian de Kali y aprenderá cómo los desarrolladores tienen aprovechado ese poder. Tenga cuidado, el próximo capítulo es bastante denso, pero es crítico que usted no Comprenda los conceptos básicos de Debian y la gestión de paquetes si va a ser un usuario avanzado de Kali.

Página 194

Palabras clave

dpkg
apto
fuentes.lista
Actualizaciones
Repositorios de paquetes

Capítulo

8

Paquete Debian administración

Contenido

Introducción a APT 170 Paquete Básico Interacción 175 Configuración avanzada de APT y uso 194
Referencia del paquete: Profundizando en el sistema de paquetes Debian 204 Resumen 216

Después de lo básico de Linux, es hora de aprender el sistema de administración de paquetes de un sistema basado en Debian distribución. En tales distribuciones, incluida Kali, el paquete Debian es la forma canónica de poner el software a disposición de los usuarios finales. Comprender el sistema de gestión de paquetes dará Si tiene una gran comprensión de cómo está estructurado Kali, le permitirá solucionar problemas de manera más efectiva problemas y ayuda a ubicar rápidamente la documentación y la documentación para la amplia gama de herramientas y utilidades incluido en Kali Linux.

En este capítulo, presentaremos el sistema de gestión de paquetes de Debian y presentaremos `dpkg` y theAPTsuiteoftools. Una de las fuerzas primarias de KalaliLinuxlies en la flexibilidad de su paquete sistema de gestión, que aprovecha estas herramientas para proporcionar una instalación casi perfecta, actualizaciones, eliminación y manipulación del software de aplicación, e incluso del sistema operativo base en sí.

Es fundamental que comprenda cómo funciona este sistema para aprovechar Kali al máximo y optimizar sus esfuerzos. Los días de compilaciones dolorosas, actualizaciones desastrosas, depuración de `gcc` , `make` y los problemas de configuración se han ido, sin embargo, la cantidad de aplicaciones disponibles ha explotado y necesita comprender las herramientas diseñadas para aprovecharlas. Esto también es crítico

habilidad porque hay una serie de herramientas de seguridad que, debido a licencias u otros problemas, no se pueden incluido en Kali pero tiene paquetes Debian disponibles para descargar. Es importante que sepas Cómo procesar e instalar estos paquetes y cómo impactan en el sistema, especialmente cuando no vayas como se esperaba.

Comenzaremos con algunas descripciones básicas de APT, describiremos la estructura y el contenido de binarios y paquetes fuente, eche un vistazo a algunas herramientas y escenarios básicos, y luego profundice para ayudarlo exprima cada onza de utilidad de este espectacular sistema de paquetes y conjunto de herramientas.

8.1. Introducción a APT

Comencemos con algunas definiciones básicas, una descripción general y un poco de historia sobre los paquetes de Debian, comenzando con dpkg y APT.

8.1.1 Relación entre APT y dpkg

Un paquete Debian es un archivo comprimido de una aplicación de software. Un *paquete binario* (un archivo .deb) contiene archivos que se pueden usar directamente (como programas o documentación), mientras que un *paquete fuente age* contiene el código fuente del software y las instrucciones necesarias para construir un binario paquete. Un paquete Debian contiene los archivos de la aplicación, así como otros *metadatos,* incluido el nombres de las dependencias que necesita la aplicación, así como scripts que permiten la ejecución de comandos en diferentes etapas del ciclo de vida del paquete (instalación, eliminación y actualizaciones).

La herramienta dpkg fue diseñada para procesar e instalar paquetes .deb , pero si encuentra un problema dependencia dependiente (como una biblioteca que falta) que impediría la instalación del paquete, dpkg simplemente enumeraría la dependencia que falta, porque no tenía conocimiento o lógica incorporada para encontrar o procesar los paquetes que puedan satisfacer esas dependencias. La herramienta de paquete avanzado (APT),

incluyendo apt y apt-get , fueron diseñados para responder a las brechas y a las respuestas automáticas resolver estos problemas Hablaremos sobre dpkg y las herramientas APT en este capítulo.

El comando base para manejar paquetes Debian en el sistema es dpkg , que realiza la instalación ción o análisis de paquetes .deb y sus contenidos. Sin embargo, dpkg solo tiene una vista parcial de la Universo Debian: sabe lo que está instalado en el sistema y lo que usted proporcione en la computadora línea de comando, pero no sabe nada de los otros paquetes disponibles. Como tal, fallará si una dependencia No se cumple. APT aborda las limitaciones.

APT establece un conjunto de herramientas que ayudan a gestionar los paquetes de Debian, o la aplicación de su sistema Debian. usted puede usar APT para instalar y eliminar aplicaciones, actualizar paquetes e incluso actualizar todo sistema. La magia de APT radica en el hecho de que es un sistema completo de gestión de paquetes que no solo instalará o eliminará un paquete, sino que considerará los requisitos y dependencias de la aplicación empaquetada (e incluso sus requisitos y dependencias) e intenta satisfacer ellos automáticamente. APT se basa en dpkg pero APT difiere de dpkg , ya que el primero instala el último paquete de una fuente en línea y trabaja para resolver dependencias mientras dpkg instala un paquete ubicado en su sistema local y no resuelve automáticamente las dependencias.

Si ha estado lo suficiente como para recordar compilar programas con gcc (incluso con el ayuda de utilidades como hacer y configurar), probablemente recuerde que fue un proceso doloroso, especialmente si la aplicación tenía varias dependencias. Al descifrar las diversas advertencias y mensajes de error, puede determinar qué parte del código estaba fallando y con mayor frecuencia esa falla se debió a una biblioteca faltante u otra dependencia. Entonces rastrearías eso falta biblioteca o dependencia, corríjala e intente nuevamente. Entonces, si tuvo suerte, la compilación se completaba, pero a menudo la construcción fallaba nuevamente, quejándose de otra dependencia rota dency

APT fue diseñado para ayudar a solucionar el problema, cotejar los requisitos y dependencias del programa, y resolverlos Esta funcionalidad funciona de fábrica en Kali Linux, pero no es infalible. Eso es importante que comprenda cómo funciona el sistema de empaquetado de Debian y Kali porque lo hará necesita instalar paquetes, actualizar software o solucionar problemas con paquetes. Usarás APT en su trabajo diario con Kali Linux y en este capítulo, le presentaremos APT y mostrarle cómo instalar, eliminar, actualizar y administrar paquetes, e incluso mostrarle cómo mover paquetes entre diferentes distribuciones de Linux. También hablaremos sobre herramientas gráficas que aproveche APT, le muestre cómo validar la autenticidad de los paquetes y profundice en el concepto de una distribución continua, una técnica que trae actualizaciones diarias a su sistema Kali.

Antes de profundizar y mostrarle cómo usar dpkg y APT para instalar y administrar paquetes, es importante que profundicemos en algunos de los funcionamientos internos de APT y discutamos alguna terminología rodeándolo

Fuente del paquete y Paquete fuente

La palabra *fuente* puede ser ambigua. Un paquete fuente: un paquete que contiene código fuente de un programa, no debe confundirse con un paquete fuente, un repositorio tory (sitio web, servidor FTP, CD-ROM, directorio local, etc.) que contiene paquetes.

Página 198

APT recupera sus paquetes de un repositorio, un sistema de almacenamiento de paquetes o simplemente "paquete fuente". El archivo /etc/apt/sources.list enumera los diferentes repositorios (o fuentes) que publican Lish paquetes Debian.

8.1.2. Comprender el archivo sources.list

El archivo sources.list es el archivo de configuración clave para definir las fuentes del paquete, y es importante para comprender cómo se presenta y cómo configurarlo, ya que APT no funcionará sin un Lista de fuentes de paquetes correctamente definida. Analicemos su sintaxis, eche un vistazo a los diversos repositorios. las historias que usa Kali Linux y discuten los espejos y la redirección de espejos, entonces usted será listo para usar APT.

Cada línea activa del archivo /etc/apt/sources.list (y de /etc/apt/sources.list.d/*.

lista de archivos) contiene la descripción de una fuente, compuesta de tres partes separadas por espacios. Com- Las líneas marcadas comienzan con un carácter #:

```
# deb cdrom: [Debian GNU / Linux 2.16.1 _Kali-rolling_ - Instantánea oficial amd64 LIVE /
    ¯ INSTALL Binary 20160830-11: 29] / kali-rolling contrib main no libre

deb http://http.kali.org/kali kali-rolling main contrib no libre
```

Echemos un vistazo a la sintaxis de este archivo. El primer campo indica el tipo de fuente:

- deb para paquetes binarios,
- deb-src para paquetes fuente.

El segundo campo proporciona la URL base de la fuente: puede consistir en un espejo de Debian o cualquier otro archivo de paquete creado por un tercero. La URL puede comenzar con file: // para indicar una fuente local instalado en la jerarquía de archivos del sistema, con http: // para indicar una fuente accesible desde una web server, orwithftp: // forasourceavailableonanFTPserver. TheURLcanalsostartwithcdrom: para Instalaciones basadas en discos CD-ROM / DVD-ROM / Blu-ray, aunque esto es menos frecuente desde la red Los métodos de instalación basados son cada vez más comunes.

Las entradas de cdrom describen los CD / DVD-ROM que tiene. Al contrario de otras entradas, un CD-ROM es no siempre está disponible, ya que debe insertarse en la unidad y generalmente solo se puede leer un disco a la vez Por esas razones, estas fuentes se administran de una manera ligeramente diferente y necesitan se agregará con el programa apt-cdrom , generalmente ejecutado con el parámetro add. Este último luego solicite que el disco se inserte en la unidad y examinará su contenido buscando paquetes archivos. Utilizará estos archivos para actualizar su base de datos de paquetes disponibles (esta operación suele ser hecho por el comando apt update). Después de eso, APT solicitará el disco si necesita un paquete almacenado en él.

La sintaxis del último campo depende de la estructura del repositorio. En los casos más simples, usted simplemente puede indicar un subdirectorio (con una barra diagonal final requerida) de la fuente deseada (esto es a menudo un simple " ./ ", que se refiere a la ausencia de un subdirectorio; los paquetes son directamente

Page 199

en la URL especificada). Pero en el caso más común, los repositorios se estructurarán como un Espejo de Debian, con múltiples distribuciones, cada una con múltiples componentes. En esos casos nombra la distribución elegida, luego los componentes (o secciones) para habilitar. Tomemos un momento para presentar estas secciones.

Debian y Kali usan tres secciones para diferenciar paquetes de acuerdo con las licencias elegidas por Los autores de cada obra.

Main contiene todos los paquetes que cumplen totalmente con las Directrices de software libre de Debian [1] .

El archivo no libre es diferente porque contiene software que no se ajusta (enteramente) a estos principios pero que sin embargo pueden distribuirse sin restricciones.

Contrib (contribuciones) es un conjunto de software de código abierto que no puede funcionar sin algunos elementos libres Estos elementos pueden incluir software de la sección no libre o archivos no libres como ROM de juegos, BIOS de consolas, etc. Contrib también incluye software gratuito cuya compilación requiere elementos propietarios, como VirtualBox, que requiere un compilador no libre para compilar Algunos de sus archivos.

Ahora, echemos un vistazo a las fuentes o repositorios de paquetes estándar de Kali Linux.

8.1.3. Repositorios Kali

Un archivo standard sources.list fileforasystemrunningKaliLinuxreferstoonerepository (kali-rolling) y los tres componentes mencionados anteriormente: principal, contrib y no libre:

```
# Repositorio principal de Kali
deb http://http.kali.org/kali kali-rolling main contrib no libre
```

Echemos un vistazo a los diversos repositorios de Kali.

El repositorio de Kali-Rolling

Este es el repositorio principal para usuarios finales. Siempre debe contener paquetes instalables y recientes. Está gestionado por una herramienta que combina Debian Testing y los paquetes específicos de Kali de una manera que garantiza que las dependencias de cada paquete se puedan satisfacer con kali-rolling. En otras palabras, salvo cualquier error en las secuencias de comandos del mantenedor, todos los paquetes deben ser instalables.

Dado que las pruebas de Debian evolucionan diariamente, también lo hace Kali Rolling. Los paquetes específicos de Kali también son regu- actualizado a medida que supervisamos las versiones anteriores de los paquetes más importantes.

[1] https://www.debian.org/social_contract#guidelines

El repositorio de Kali-Dev

Este repositorio no es para uso público. Es un espacio donde los desarrolladores de Kali resuelven problemas de dependencia. Lems que surgen de la fusión de los paquetes específicos de Kali en Debian Testing.

También es el lugar donde los paquetes actualizados aterrizan primero, por lo que si necesita una actualización que se lanzó recientemente y que no ha llegado a Kali Rolling, puede ser capaz de capturar desde este repositorio. Esto no se recomienda para usuarios habituales.

El repositorio Kali-Bleeding-Edge

Este repositorio contiene paquetes construidos automáticamente desde el Git ascendente (o Subversion) repositorio. Lo bueno es que tiene acceso inmediato a las últimas funciones y correcciones de errores menos de 24 horas después de haber sido comprometidos. Esta es una forma ideal de verificar si un error que usted reportado aguas arriba ha sido reparado.

La desventaja es que estos paquetes no han sido probados ni examinados: si los cambios aguas arriba impactado el paquete (agregando una nueva dependencia), entonces ese paquete podría no funcionar. Porque de esto, el repositorio está marcado de tal manera que APT no instala automáticamente paquetes de él, particularmente durante una actualización.

Puede registrar el repositorio editando /etc/apt/sources.list o creando un nuevo archivo bajo el directorio /etc/apt/sources.list.d , que tiene la ventaja de dejar el original archivo de sistema sources.list sin alteraciones. En este ejemplo, optamos por crear un / etc / apt / separado El archivo sources.list.d / kali-bleeding-edge.list tiene este aspecto :

```
# Depósito Kali Bleeding Edge
deb http://http.kali.org/kali kali-bleeding-edge main contrib no libre
```

Los espejos de Kali Linux

Los extractos de sources.list anteriores se refieren a http.kali.org: este es un servidor que ejecuta MirrorBrain[2] , que redirigirá sus solicitudes HTTP a un espejo oficial cercano a usted. Monitores MirrorBrain cada espejo para asegurarse de que estén funcionando y actualizados; siempre te redirigirá a un buen

espejo.

Depuración de un espejo Redireccionamiento

Si tiene un problema con el espejo (por ejemplo, porque la actualización de apt falla), usted puede usar curl -sI para ver a dónde lo redirigen:

```
$ curl -sI http://http.kali.org/README
HTTP / 1.1 302 encontrado
Fecha: lunes 11 de abril de 2016 09:43:21 GMT
Servidor: Apache / 2.4.10 (Debian)
X-MirrorBrain-Mirror: ftp.free.fr
X-MirrorBrain-Realm: país
Enlace: <http://http.kali.org/README.meta4>; rel = descrito por;
        type = "application / metalink4 + xml"
Enlace: <http://ftp.free.fr/pub/kali/README>; rel = duplicar;
        pri = 1; geo = fr
Enlace: <http://de-rien.fr/kali/README>; rel = duplicar; pri = 2;
        geo = fr
Enlace: <http://ftp.halifax.rwth-aachen.de/kali/README>; rel =
        duplicado; pri = 3; geo = de
Enlace: <http://ftp.belnet.be/kali/kali/README>; rel = duplicar;
        pri = 4; geo = be
Enlace: <http://ftp2.nluug.nl/os/Linux/distr/kali/README>; rel =
        duplicado; pri = 5; geo = nl
Ubicación: http://ftp.free.fr/pub/kali/README
Tipo de contenido: texto / html; juego de caracteres = iso-8859-1

Si el problema persiste, puede editar /etc/apt/sources.list y codificar
nombre de otro espejo de trabajo conocido en lugar de (o antes) http.kali.org
entrada.
```

[2] http://mirrorbrain.org

También tenemos una segunda instancia de MirrorBrain: donde http.kali.org aloja los repositorios de paquetes, cdimage.kali.org aloja las imágenes ISO publicadas.

[2] http://cdimage.kali.org

Si desea solicitar una lista de espejos oficiales de Kali Linux, puede agregar .mirrorlist a cualquier URL válida apuntando a http.kali.org o cdimage.kali.org.

[2] http://http.kali.org/README.mirrorlist

[2] http://cdimage.kali.org/README.mirrorlist

Estas listas no son exhaustivas debido a algunas limitaciones de MirrorBrain (especialmente los espejos restringido a algunos países no aparecen en la lista a menos que se encuentre en el país dado). Pero contienen los mejores espejos: están bien mantenidos y tienen grandes cantidades de ancho de banda disponible.

8.2. Interacción básica del paquete

Armado con una comprensión básica del panorama APT, echemos un vistazo a algún paquete básico interacciones que incluyen la inicialización de APT; instalación, retiro y purga de paquetes; y actualización del sistema Kali Linux. Entonces, aventurémonos desde la línea de comando para echar un vistazo en algunas herramientas gráficas APT.

8.2.1. Inicializando APT

APTisavastprojectandtoolset, cuyos planes originales incluyen una interfaz gráfica. Del cliente perspectiva, se centra en la herramienta de línea de comandos apt-get y apt , que fue más tarde desarrollado para superar los defectos de diseño de apt-get .

Existen alternativas gráficas desarrolladas por terceros, que incluyen sináptica y aptitud ,

que discutiremos más adelante. Tendemos a preferir apt , que usamos en los ejemplos que siguen. Nosotros sin embargo, detallará algunas de las principales diferencias de sintaxis entre las herramientas, a medida que surjan.

Cuando trabaje con APT, primero debe descargar la lista de paquetes disponibles actualmente con apt update . Dependiendo de la velocidad de su conexión, esto puede demorar en algún momento porque La lista de paquetes, la lista de fuentes y los archivos de traducción han crecido en tamaño junto con el desarrollo de Debian. Por supuesto, los conjuntos de instalación de CD / DVD se instalan mucho más rápidamente, porque son locales para su máquina.

8.2.2. Instalar paquetes

Gracias al diseño atento del sistema de paquetes de Debian, puede instalar paquetes con o sin sus dependencias, con bastante facilidad. Echemos un vistazo a la instalación del paquete con dpkg y apto .

Instalación de paquetes con dpkg

dpkg es la herramienta principal que usará (ya sea directa o indirectamente a través de APT) cuando lo necesite para instalar un paquete También es una opción de elección si está operando sin conexión, ya que no requiere un Conexión a Internet. Recuerde, dpkg no instalará ninguna dependencia que el paquete pueda exigir. Para instalar un paquete con dpkg , simplemente proporcione la opción -i o --install y la ruta a el .deb . Esto implica que ha descargado previamente (u obtenido de alguna otra manera) el Archivo .deb del paquete a instalar.

```
# dpkg -i man-db_2.7.0.2-5_amd64.deb
(Leyendo la base de datos ... 86425 archivos y directorios actualmente instalados).
Preparación para desempaquetar man-db_2.7.0.2-5_amd64.deb ...
Desempacando man-db (2.7.0.2-5) sobre (2.7.0.2-4) ...
Configuración de man-db (2.7.0.2-5) ...
Actualización de la base de datos de páginas del manual ...
Procesando disparadores para mime-support (3.58) ...
```

Podemos ver los diferentes pasos realizados por dpkg y podemos ver en qué punto puede tener cualquier error ocurrió. La opción -i o --install realiza dos pasos automáticamente: desempaqueta el paquete y ejecuta los scripts de configuración. Puede realizar estos dos pasos de manera independiente (como se hace detrás) las escenas) con las opciones --unpack y --configure, respectivamente:

```
# dpkg --unpack man-db_2.7.0.2-5_amd64.deb
(Leyendo la base de datos ... 86425 archivos y directorios actualmente instalados).
Preparación para desempaquetar man-db_2.7.0.2-5_amd64.deb ...
Desempacando man-db (2.7.0.2-5) sobre (2.7.0.2-5) ...
Procesando disparadores para mime-support (3.58) ...
# dpkg --configure man-db
Configuración de man-db (2.7.0.2-5) ...
Actualización de la base de datos de páginas del manual ...
```

Tenga en cuenta que las líneas "Procesadores de activación" se refieren al código que se ejecuta automáticamente cada vez que un El paquete agrega, elimina o modifica archivos en algunos directorios monitoreados. Por ejemplo, el *mimo admite* paquetes monitores / usr / lib / mime / packages y ejecuta el comando update-mime cada vez que algo cambia en ese directorio (como / usr / lib / mime / packages / man-db en el caso específico de man-db).

A veces, dpkg no podrá instalar un paquete y devolverá un error. Sin embargo, puedes pedir dpkg para ignorar esto y solo emitir una advertencia con varias opciones --force- *. Emitir el dpkg --force- El comando de ayuda mostrará una lista completa de estas opciones. Por ejemplo, puede usar dpkg para instalar a la fuerza zsh :

```
$ dpkg -i --force-overwrite zsh_5.2-5 + b1_amd64.deb
```

Un error frecuente, que seguramente encontrará tarde o temprano, es una colisión de archivos. Cuando un El paquete contiene un archivo que ya está instalado por otro paquete, dpkg se negará a instalarlo. Aparecerán los siguientes tipos de mensajes:

```
Desembalaje de libgdm (de ... / libgdm_3.8.3-2_amd64.deb) ...
dpkg: error al procesar /var/cache/apt/archives/libgdm_3.8.3-2_amd64.deb (--unpack):
 ¯ tratando de sobrescribir '/ usr / bin / gdmflexiserver', que también está en el paquete gdm3
 ¯ 3.4.1-9
```

En este caso, si cree que reemplazar este archivo no es un riesgo significativo para la estabilidad de su sistema (que suele ser el caso), puede usar --force-overwrite para sobrescribir el archivo.

Si bien hay muchas opciones disponibles --force- *, solo es probable que se use --force-overwrite regularmente Larly Estas opciones existen en situaciones previas a la excepción, y es mejor dejar a la persona sola como muchas posible para respetar las normas impuestas por el mecanismo de embalaje. No olvides que estos Las reglas aseguran la consistencia y estabilidad de su sistema.

Instalación de paquetes con APT

Aunque APT es mucho más avanzado que dpkg y hace mucho más entre bastidores, usted Descubrir que interactuar con paquetes es bastante simple. Puede agregar un paquete al sistema con un *Paquete de* instalación simple y apto . APT instalará automáticamente las dependencias necesarias:


```
# apt install kali-linux-gpu
Leyendo listas de paquetes ... Hecho
Construyendo árbol de dependencia
Leyendo información del estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
    oclgausscrack oclhashcat
Se instalarán los siguientes paquetes NUEVOS:
    kali-linux-gpu oclgausscrack oclhashcat
0 actualizado, 3 recién instalados, 0 para eliminar y 416 no actualizado.
Necesito obtener 2,494 kB de archivos.
Después de esta operación, se usarán 51.5 MB de espacio en disco adicional.
¿Quieres continuar? [S / n]
Obtenga: 1 http://archive-2.kali.org/kali kali-rolling / non-free amd64 oclhashcat amd64 2.01+
        ¯ git20160114-0kali2 [2,451 kB]
Obtenga: 2 http://archive-2.kali.org/kali kali-rolling / main amd64 oclgausscrack amd64 1.3-1
        ¯ kali2 [37,2 kB]
Obtenga: 3 http://archive-2.kali.org/kali kali-rolling / main amd64 kali-linux-gpu amd64
        ¯ 2016.3.2 [6,412 B]
Obtenido 2,494 kB en 0s (3,060 kB / s)
Selección del paquete oclhashcat no seleccionado previamente.
(Leyendo la base de datos ... 317084 archivos y directorios actualmente instalados).
Preparándose para desempaquetar ... / 0-oclhashcat_2.01 + git20160114-0kali2_amd64.deb ...
Desembalaje de oclhashcat (2.01 + git20160114-0kali2) ...
Selección del paquete oclgausscrack no seleccionado previamente.
Preparándose para desempaquetar ... / 1-oclgausscrack_1.3-1kali2_amd64.deb ...
Desembalaje de oclgausscrack (1.3-1kali2) ...
Selección del paquete no seleccionado previamente kali-linux-gpu.
Preparación para desempaquetar ... / 2-kali-linux-gpu_2016.3.2_amd64.deb ...
Desembalaje de kali-linux-gpu (2016.3.2) ...
Configuración de oclhashcat (2.01 + git20160114-0kali2) ...
Configuración de oclgausscrack (1.3-1kali2) ...
Configuración de kali-linux-gpu (2016.3.2) ...
```

También puede usar apt-get install *package* o aptitude install *package* . Por paquete simple instalación de edad, hacen esencialmente lo mismo. Como verá más adelante, las diferencias son más significativo para actualizaciones o cuando la resolución de dependencias no tiene una solución perfecta.

Si sources.list enumera varias distribuciones, puede especificar la versión del paquete con apt install *paquete = versión* , pero indicando su distribución de origen (kali-rolling, kali-dev o kali-bleeding-edge) con apt install *package* / *distribution* generalmente se prefiere.

Con dpkg , también puede instruirlo para que instale el paquete de forma práctica sobre los archivos de escritura con - force-sobrescribir, pero la sintaxis es un poco extraña ya que está pasando el argumento a dpkg :

```
# apt -o Dpkg :: Opciones :: = ”- forzar-sobrescribir” instalar zsh
```


8.2.3. Actualización de Kali Linux

Como distribución continua, Kali Linux tiene capacidades de actualización espectaculares. En esta sección, lo haremos

eche un vistazo a lo simple que es actualizar Kali, y discutiremos las estrategias para planificar su actualizaciones

Recomendamos actualizaciones regulares, ya que instalarán las últimas actualizaciones de seguridad. Para actualizar, use apt update seguido de apt upgrade , apt-get upgrade o aptitude safe-upgrade . Estos comandos buscan paquetes instalados que se pueden actualizar sin quitar ningún paquete. En otras palabras, el objetivo es garantizar la actualización menos intrusiva posible. El comando apt-get la línea de herramientas es ligeramente más exigente que la aptitud o apta porque se rechazará para instalar paquetes que no fueron instalados de antemano.

La herramienta apt generalmente seleccionará el número de versión más reciente (excepto los paquetes de kali-sangrado, que se ignoran por defecto sea cual sea su número de versión).

Para indicarle a apt que use una distribución específica cuando busque paquetes actualizados, debe usar la opción -t o --target-release, seguida del nombre de la distribución que desea (por ejemplo: apt -t kali-rolling upgrade). Para evitar especificar esta opción cada vez que use apt , usted puede agregar APT :: Default-Release "kali-rolling"; en el archivo /etc/apt/apt.conf.d/local .

Para actualizaciones más importantes, como las actualizaciones de versiones principales, use apt full-upgrade . Con este instrucción, apt completará la actualización incluso si tiene que eliminar algunos paquetes obsoletos o Instalar nuevas dependencias. Este es también el comando que debe usar para actualizaciones regulares de Su sistema Kali Rolling. Es tan simple que apenas necesita explicación: la reputación de APT se basa en esta gran funcionalidad

A diferencia de apt y aptitude , apt-get no conoce el comando de actualización completa . En cambio, tu debería usar apt-get dist-upgrade (actualización de distribución), un comando bien conocido que apt y La aptitud también acepta la compatibilidad con versiones anteriores.

Sé consciente de lo importante Cambios Para anticipar algunos de estos problemas, puede instalar el paquete *apt-listchanges* , que muestra información sobre posibles problemas al comienzo de un paquete actualización de edad. Los mantenedores del paquete recopilan esta información y la ponen en / usr / share / doc / *package* /NEWS.Debian archivos para su beneficio. Leer estos archivos (posiblemente a través de *apt-listchanges*) debería ayudarlo a evitar sorpresas desagradables.

Desde que se convirtió en una distribución continua, Kali puede recibir actualizaciones varias veces al día. Sin embargo, Esa podría no ser la mejor estrategia. Entonces, ¿con qué frecuencia debe actualizar Kali Linux? No hay regla difícil, pero hay algunas pautas que pueden ayudarlo. Debes actualizar:

- Cuando conoce un problema de seguridad que se corrige en una actualización
- Cuando sospecha que una versión actualizada podría corregir un error que está experimentando
- Antes de informar un error para asegurarse de que todavía esté presente en la última versión que tenga disponible

- A menudo es suficiente para obtener las soluciones de seguridad de las que no ha oído hablar.

También hay casos en los que es mejor no actualizar. Por ejemplo, podría no ser una buena idea potenciar:

- Si no puede permitirse ninguna rotura (por ejemplo, porque se desconecta o porque está a punto de hacer una presentación con su computadora); es mejor hacer la actualización más tarde, cuando tiene tiempo suficiente para solucionar cualquier problema introducido en el proceso.
- Si un cambio disruptivo ocurrió recientemente (o aún está en curso) y teme que todos los problemas Todavía no han sido descubiertos. Por ejemplo, cuando se lanza una nueva versión de GNOME, no todas los paquetes se actualizan al mismo tiempo y es probable que tenga una combinación de paquetes con la versión anterior y la nueva versión. La mayoría de las veces esto está bien y ayuda a todos a liberar esas actualizaciones progresivamente, pero siempre hay excepciones y algunas aplicaciones podría romperse debido a tales discrepancias.
- Si la salida de actualización completa de apt le indica que eliminará los paquetes que considere importante para tu trabajo En esos casos, desea revisar la situación e intentar entender por qué apt quiere eliminarlos. Tal vez los paquetes están actualmente rotos y en este en caso de que desee esperar hasta que las versiones fijas estén disponibles, o hayan quedado obsoletas y debe identificar sus reemplazos y luego continuar con la actualización completa de todos modos.

En general, le recomendamos que actualice Kali al menos una vez por semana. Ciertamente puedes actualizar diariamente, pero no tiene sentido hacerlo más a menudo que eso. Incluso si los espejos están sincronizados cuatro veces al día, las actualizaciones que provienen de Debian generalmente llegan solo una vez al día.

8.2.4. Eliminar y purgar paquetes

Eliminar un paquete es aún más simple que instalar uno. Echemos un vistazo a cómo eliminar un paquete con dpkg y apt .

Para eliminar un paquete con dpkg , proporcione la opción -r o --remove, seguida del nombre de un paquete-años. Sin embargo, esta eliminación no está completa: todos los archivos de configuración, scripts de mantenimiento, registro archivos (registros del sistema), datos generados por el demonio (como el contenido de un directorio de servidor LDAP o el contenido de una base de datos para un servidor SQL), y la mayoría de los demás datos de usuario manejados por el paquete permanece intacto. La opción eliminar facilita la desinstalación de un programa y luego lo reinstala con La misma configuración. Recuerde también que las dependencias no se eliminan. Considera este examen ple:

```
# dpkg --remove kali-linux-gpu
(Leyendo la base de datos ... 317681 archivos y directorios actualmente instalados).
Eliminando kali-linux-gpu (2016.3.2) ...
```

También puede eliminar *paquetes del* sistema con apt remove *package* . APTwillautomatically elimine los paquetes que dependen del paquete que se está eliminando. Como el ejemplo dpkg , los archivos de configuración y los datos del usuario no se eliminarán.

Mediante la adición de sufijos a los nombres de paquetes, puede usar apt (o apt-get y aptitude) para instalar ciertos paquetes y eliminar otros en la misma línea de comando. Con un inst apto todos los comandos, agregue "-" a los nombres de los paquetes que desea eliminar. Con un apt remove comando, agregue "+" a los nombres de los paquetes que desea instalar.

El siguiente ejemplo muestra dos formas diferentes de instalar *package1* y eliminar *package2* .

```
# apt install package1 package2-
[...]
# apt remove package1 + package2
[...]
```

Esto también se puede utilizar para excluir paquetes que de otro modo se instalarían, por ejemplo debido a a Recomienda (discutido más adelante). En general, el solucionador de dependencias utilizará esa información como un Sugerencia para buscar soluciones alternativas.

Para eliminar todos los datos asociados con un paquete, puede purgar el paquete con dpkg -P *package* o apt purge *package* comandos. Esto eliminará completamente el paquete y todo los datos del usuario, y en el caso de apt , también eliminarán las dependencias.

```
# dpkg -r debian-cd
(Leyendo la base de datos ... 97747 archivos y directorios actualmente instalados).
Eliminando debian-cd (3.1.17) ...
# dpkg -P debian-cd
(Leyendo la base de datos ... 97401 archivos y directorios actualmente instalados).
Eliminando debian-cd (3.1.17) ...
Depuración de archivos de configuración para debian-cd (3.1.17) ...
```

¡Advertencia! Dada la naturaleza definitiva de la purga, no la ejecute a la ligera. Perderás todo asociado con ese paquete.

8.2.5. Inspección de paquetes

A continuación, echemos un vistazo a algunas de las herramientas que se pueden utilizar para inspeccionar los paquetes de Debian. Lo haremos Conozca los comandos dpkg , apt y apt-cache que se pueden usar para consultar y visualizar el paquete base de datos.

Consultar la base de datos de dpkg e inspeccionar archivos .deb

Comenzaremos con varias opciones de dpkg que consultan la base de datos interna de dpkg. Esta base de datos reside en el sistema de archivos en / var / lib / dpkg y contiene varias secciones, incluida la configuración scripts (/ var / lib / dpkg / info), una lista de archivos que el paquete instaló (/ var / lib / dpkg / info / *. lista) y el estado de cada paquete que se ha instalado (/ var / lib / dpkg / status). Usted puede use dpkg para interactuar con los archivos en esta base de datos. Tenga en cuenta que la mayoría de las opciones están disponibles en un largo

versión (una o más palabras relevantes, precedidas por un guión doble) y una versión corta (una sola letra, a menudo la inicial de una palabra de la versión larga, precedida por un solo guión). Esta La convención es tan común que es un estándar POSIX.

Primero, echemos un vistazo al *paquete* --listfiles (o -L), que enumera los archivos que fueron instalados por paquete especificado:

```
$ dpkg -L base-passwd
/.
/ usr
/ usr / sbin
/ usr / sbin / update-passwd
/ usr / share
/ usr / share / lintian
/ usr / share / lintian / overrides
/ usr / share / lintian / overrides / base-passwd
/ usr / share / doc-base
/ usr / share / doc-base / users-and-groups
/ usr / share / base-passwd
/usr/share/base-passwd/group.master
/usr/share/base-passwd/passwd.master
/ usr / share / man
/ usr / share / man / pl
/ usr / share / man / pl / man8
/usr/share/man/pl/man8/update-passwd.8.gz
[...]
/ usr / share / doc
/ usr / share / doc / base-passwd
/usr/share/doc/base-passwd/users-and-groups.txt.gz
/usr/share/doc/base-passwd/changelog.gz
/ usr / share / doc / base-passwd / copyright
/ usr / share / doc / base-passwd / README
/usr/share/doc/base-passwd/users-and-groups.html
```

A continuación, dpkg --search *file* (o -S), encuentra los paquetes que contienen el archivo o la ruta pasada en argumento. Por ejemplo, para buscar el paquete que contiene / bin / date :

```
$ dpkg -S / bin / date
coreutils: / bin / date
```

El comando dpkg --status *package* (o -s) muestra los encabezados de un paquete instalado. por ejemplo, para buscar en los encabezados el paquete coreutils:

```
$ dpkg -s coreutils
Paquete: coreutils
Esencial: sí
Estado: instalar ok instalado
```



```
Prioridad: requerida
Sección: utils
Tamaño instalado: 13855
Mantenedor: Michael Stone <mstone@debian.org>
Arquitectura: amd64
Multi-arco: extranjero
Versión: 8.23-3
Reemplaza: mktemp, realpath, timeout
Predepende: libacl1 (> = 2.2.51-8), libattr1 (> = 1: 2.4.46-8), libc6 (> = 2.17),
        ¯ libselinux1 (> = 2.1.13)
Conflictos: tiempo de espera
Descripción: utilidades principales de GNU
Este paquete contiene la manipulación básica de archivos, shell y texto.
utilidades que se espera que existan en todos los sistemas operativos.
.
Específicamente, este paquete incluye:
arco base64 basename gato chcon chgrp chmod chown chroot cksum comm cp
csplit fecha de corte dd df dir dircolors dirname du echo env expand expr
factor false flock fmt fold groups head hostid id install join link ln
nombre de registro ls md5sum mkdir mkfifo mknod mktemp mv nice nl nohup nproc numfmt
od pegar pathchk pinky pr printenv printf ptx pwd readlink realpath rm
rmdir runcon sha * sum seq shred sleep sort split stat stty sum sync tac
cola tee prueba tiempo de espera toque tr verdadero truncado tsort tty uname unspand
uniq desvincular usuarios vdir wc whoami sí
Página de inicio: http://gnu.org/software/coreutils
```

El comando dpkg --list (o -l) muestra la lista de paquetes conocidos por el sistema y sus estado de instalación. También puede usar grep en la salida para buscar ciertos campos, o proporcionar comodines (como b *) para buscar paquetes que coincidan con una cadena de búsqueda parcial particular. Esta mostrará un resumen de los paquetes. Por ejemplo, para mostrar una lista resumida de todos los paquetes que comience con 'b':

```
$ dpkg -l 'b *'
Deseado = Desconocido / Instalar / Eliminar / Purgar / Retener
El | Estado = No / Inst / Conf-files / Unpacked / halF-conf / Half-inst / trig-aWait / Trig-pend
| / Err? = (None) / Reinst-required (Estado, Err: mayúsculas = incorrecto)
|| / Nombre                    Versión              Descripción de la arquitectura
+++ - ============== - ============ - ============ - ===== ============================
ii b43-fwcutter                1: 019-3             amd64        utilidad para extraer Broadcom 4
ii backdoor-facto 3.4.2-0kali1 todos                             Parche win32 / 64 binarios con shel
un backupninja                 <ninguno>            <ninguno>    (No hay descripción disponible)
un backuppc                    <ninguno>            <ninguno>    (No hay descripción disponible)
ii baobab                      3.22.1-1             amd64        Analizador de uso de disco de GNOME
[...]
```


Página 210

El comando dpkg --contents *file.deb* (o -c) enumera todos los archivos en un archivo .deb particular :

```
$ dpkg -c /var/cache/apt/archives/gnupg_1.4.18-6_amd64.deb
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./lib/
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./lib/udev/
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./lib/udev/rules.d/
-rw-r - r-- raíz / raíz      2711 2014-12-04 23:03 ./lib/udev/rules.d/60-gnupg.rules
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./usr/
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./usr/lib/
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./usr/lib/gnupg/
-rwxr-xr-x raíz / raíz     39328 2014-12-04 23:03 ./usr/lib/gnupg/gpgkeys_ldap
-rwxr-xr-x raíz / raíz     92872 2014-12-04 23:03 ./usr/lib/gnupg/gpgkeys_hkp
-rwxr-xr-x raíz / raíz     47576 04/12/2014 23:03 ./usr/lib/gnupg/gpgkeys_finger
-rwxr-xr-x raíz / raíz     84648 04/12/2014 23:03 ./usr/lib/gnupg/gpgkeys_curl
-rwxr-xr-x raíz / raíz      3499 04/12/2014 23:03 ./usr/lib/gnupg/gpgkeys_mailto
drwxr-xr-x raíz / raíz         0 2014-12-04 23:03 ./usr/bin/
-rwxr-xr-x raíz / raíz     60128 04/12/2014 23:03 ./usr/bin/gpgsplit
-rwxr-xr-x raíz / raíz   1012688 2014-12-04 23:03 ./usr/bin/gpg
[...]
```

El comando dpkg --info *file.deb* (o -I) muestra los encabezados del archivo .deb especificado :

```
$ dpkg -I /var/cache/apt/archives/gnupg_1.4.18-6_amd64.deb
 nuevo paquete debian, versión 2.0.
 tamaño 1148362 bytes: archivo de control = 3422 bytes.
       1264 bytes,    26 líneas      controlar
       4521 bytes,    65 líneas      md5sums
        479 bytes,    13 líneas   * postinst                #! / bin / sh
        473 bytes,    13 líneas   * preinst                 #! / bin / sh
 Paquete: gnupg
 Versión: 1.4.18-6
 Arquitectura: amd64
 Mantenedor: Debian GnuPG-Maintainers <pkg-gnupg-maint@lists.alioth.debian.org>
 Tamaño instalado: 4888
 Depende: gpgv, libbz2-1.0, libc6 (> = 2.15), libreadline6 (> = 6.0), libusb-0.1-4 (> =
        ¯ 2: 0.1.12), zlib1g (> = 1: 1.1.4)
 Recomienda: gnupg-curl, libldap-2.4-2 (> = 2.4.7)
 Sugiere: gnupg-doc, libpcsclite1, parcimonie, xloadimage | imagemagick | eog
 Sección: utils
 Prioridad: importante
 Multi-arco: extranjero
 Página de inicio: http://www.gnupg.org
 Descripción: GNU Privacy Guard: un reemplazo gratuito de PGP
   GnuPG es la herramienta de GNU para la comunicación segura y el almacenamiento de datos.
   Se puede utilizar para cifrar datos y crear firmas digitales.
   Incluye una instalación avanzada de administración de claves y cumple
```

con el estándar de Internet OpenPGP propuesto como se describe en RFC 4880.
[...]

También puede usar dpkg para comparar los números de versión del paquete con la opción --compare-version, que a menudo se llama por programas externos, incluida la configuración de script ejecutada por dpkg . Esta opción requiere tres parámetros: un número de versión, un operador de comparación y un segundo número de versión. Los diferentes operadores posibles son: lt (estrictamente menor que), le (menor o igual que to), eq (igual), ne (no igual), ge (mayor o igual que) y gt (estrictamente mayor que). Si el la comparación es correcta, dpkg devuelve 0 (éxito); si no, da un valor de retorno distinto de cero (que indica fracaso). Considere estas comparaciones:

```
$ dpkg --compare-versiones 1.2-3 gt 1.1-4
$ echo $?
0 0
$ dpkg --compare-versiones 1.2-3 lt 1.1-4
$ echo $?
1
$ dpkg --compare-versiones 2.6.0pre3-1 lt 2.6.0-1
$ echo $?
1
```

Tenga en cuenta la falla inesperada de la última comparación: para dpkg , la cadena "pre" (generalmente denota un pre-lanzamiento) no tiene un significado particular, y dpkg simplemente lo interpreta como una cadena, en cuyo caso "2. 6.0pre3-1 "es alfabéticamente mayor que" 2.6.0-1 ". Cuando queremos que el número de versión de un paquete indica que es un prelanzamiento, utilizamos el carácter tilde, "~":

```
$ dpkg --compare-versiones 2.6.0 ~ pre3-1 lt 2.6.0-1
$ echo $?
0 0
```

Consultar la base de datos de paquetes disponibles con apt-cache y apt

El comando apt-cache puede mostrar gran parte de la información almacenada en la base de datos interna de APT. Esta información es una especie de caché, ya que se recopila de las diferentes fuentes enumeradas en el archivo sources.list . Esto sucede durante la operación de actualización de apt .

VOCABULARIO

Cache

Un caché es un sistema de almacenamiento temporal utilizado para acelerar el acceso frecuente a datos cuando El método de acceso habitual es costoso (en términos de rendimiento). Este concepto puede ser aplicado en numerosas situaciones y a diferentes escalas, desde el núcleo de los microprocesadores hasta Sistemas de almacenamiento de alta gama.

En el caso de APT, los archivos de paquetes de referencia son aquellos ubicados en los espejos de Debian. Dicho esto, sería muy ineficaz impulsar cada búsqueda a través del paquete en línea bases de datos Es por eso que APT almacena una copia de esos archivos (en / var / lib / apt / lists /) y las búsquedas se realizan dentro de esos archivos locales. Del mismo modo, / var / cache / apt / archives / contiene una copia en caché de los paquetes ya descargados para evitar descargarlos de nuevo si necesita reinstalarlos.

Para evitar el uso excesivo del disco cuando actualiza con frecuencia, debe ordenar regularmente a través del directorio / var / cache / apt / archives / . Se pueden usar dos comandos para esto: apt clean (o apt-get clean) vacía completamente el directorio; apto autoclean (apt-get autoclean) solo elimina los paquetes que ya no se pueden descargar porque porque han desaparecido del espejo y por lo tanto son inútiles. Tenga en cuenta que el El parámetro de configuración APT :: Clean-Installed se puede utilizar para evitar la eliminación de archivos .deb que están instalados actualmente. Además, tenga en cuenta que apt descarta la descarga archivos una vez que se han instalado, por lo que esto es importante principalmente cuando utiliza otras herramientas.

El apt-cache comando puede hacer búsquedas de paquetes basados en palabras clave con apt-cache search *clave*

palabra . También puede mostrar los encabezados de las versiones disponibles del paquete con apt-cache show *empaquetar* . Este comando proporciona la descripción del paquete, sus dependencias y el nombre de su mantenedor. Esta característica es particularmente útil para determinar el paquete que se instala metapaquetes, como *kali-linux-wireless* , *kali-linux-web* y *kali-linux-gpu* . Tenga en cuenta que apt search , apt show , aptitude search y aptitude show funcionan de la misma manera.

Una alternativa: axi-cache

apt-cache search es una herramienta muy rudimentaria, básicamente implementa grep en el paquete descripciones de la edad. A menudo devuelve demasiados resultados o ninguno en absoluto, cuando demasiados Se incluyen palabras clave.

El *término de* búsqueda axi-cache , por otro lado, proporciona mejores resultados, ordenados por relevancy. Utiliza el motor de búsqueda *Xapian* y es parte del paquete *apt-xapian-index* , que indexa toda la información del paquete (y más, como los archivos .desktop de todos los Depaquetes bian). Conoce las etiquetas y devuelve resultados en cuestión de milisegundos.

$ **axi-cache search forense gráfico**

5 resultados encontrados.

Resultados 1-5:

Autopsia 100%: interfaz gráfica para SleuthKit

82% forense-colorize - muestra las diferencias entre archivos usando
¯ gráficos en color

73% dff: análisis forense digital potente, eficiente y modular
¯ marco

53% gpart - Adivina la tabla de particiones de disco de PC, encuentra perdido
¯ particiones

46% testdisk: escáner de particiones y herramienta de recuperación de disco, y
¯ Herramienta de recuperación de archivos PhotoRec

Más términos: colorear particiones archivo autopsia de etiqueta de disco
¯ diferencias digitales

Más etiquetas: admin :: seguridad forense :: rol forense :: programa
¯ admin :: interfaz de recuperación :: línea de comando admin :: arranque
¯ alcance :: utilidad

Algunas funciones se usan con menos frecuencia. Por ejemplo, la política de apt-cache muestra las prioridades de fuentes de paquetes, así como las de paquetes individuales. Otro ejemplo es apt-cache dumpavail , que muestra los encabezados de todas las versiones disponibles de todos los paquetes. apt-cache pkgnames muestra la lista de todos los paquetes que aparecen al menos una vez en el caché.

8.2.6. Solución de problemas

Tarde o temprano, se encontrará con un problema al interactuar con un paquete. En esta sección, nosotros describirá algunos pasos básicos de solución de problemas que puede tomar y le proporcionará algunas herramientas que lo llevará más cerca de una posible solución.

Manejo de problemas después de una actualización

A pesar de los mejores esfuerzos de los mantenedores de Kali / Debian, la actualización del sistema no se realiza siempre esperaría Las nuevas versiones de software pueden ser incompatibles con las anteriores (por ejemplo, su comportamiento predeterminado o su formato de datos puede haber cambiado), o los errores pueden pasar desapercibidos a pesar de las pruebas realizadas por los mantenedores de paquetes y los usuarios inestables de Debian.

Aprovechando los informes de errores, a veces puede encontrar una nueva versión de software que no funciona en absoluto. Esto generalmente sucede si la aplicación no es particularmente popular y no ha sido probada suficiente. Lo primero que debe hacer es echar un vistazo al rastreador de errores Kali [3] y al error Debian sistema de rastreo[4] en https://bugs.debian.org/ *package* , y verifique si el problema ya ha sido reportado Si no es así, debe declararse a sí mismo (ver sección 6.3 , " FilingaGoodBugReport " [página 129] para obtener instrucciones detalladas). Si ya se conoce, el informe de error y el asociado Los mensajes suelen ser una excelente fuente de información relacionada con el error. En algunos casos, un parche ya existe y se ha puesto a disposición en el informe de error en sí mismo; entonces puedes recompilar un fijo versión del paquete roto localmente (ver sección 9.1, " Modificación de paquetes de Kali " [página 222]). En En otros casos, los usuarios pueden haber encontrado una solución para el problema y compartir sus ideas sobre en sus respuestas al informe; esas instrucciones pueden ayudarlo a solucionar el problema hasta que Se libera la corrección o parche. En el mejor de los casos, es posible que el paquete ya haya sido reparado y usted puede encontrar detalles en el informe de error.

[3] http://bugs.kali.org

[4] [4] https://bugs.debian.org

Página 214

Bajar de categoría a una versión de trabajo cuando el problema es una regresión clara (donde la primera versión trabajada), puede intentar degradar el paquete. En este caso, necesitará una copia del versión antigua. Si tiene acceso a la versión anterior en uno de los repositorios configurados en APT, usted puede usar un comando simple de una línea para bajar de categoría (ver sección 8.2.2.2, " Instalación de paquetes con APTO"[Página 177]). Pero con el lanzamiento continuo de Kali, generalmente solo encontrará una versión única de cada paquete en cualquier momento.

Todavía puede intentar encontrar el archivo .deb antiguo e instalarlo manualmente con dpkg . Los viejos archivos .deb pueden ser encontrado en múltiples lugares:

- en el caché de APT en / var / cache / apt / archives /
- en el directorio del grupo en su espejo Kali habitual (los paquetes eliminados y obsoletos se mantienen durante tres o cuatro días para evitar problemas con los usuarios que no tienen los últimos índices de paquetes)
- en http://snapshot.debian.org si el paquete afectado fue proporcionado por Debian y no por Kali; Este servicio mantiene versiones históricas de todos los paquetes de Debian

Tratar con scripts de mantenimiento rotos Algunas veces las **actualizaciones se interrumpen porque** de las secuencias de comandos del mantenedor del paquete falla (por lo general, es el postinst). En esos casos, puedes intentar diagnostica el problema y posiblemente lo solucione editando el script problemático.

Aquí confiamos en el hecho de que los scripts de mantenedor se almacenan en / var / lib / dpkg / info / y que puede revisarlos y modificarlos.

Dado que las secuencias de comandos de mantenimiento suelen ser simples secuencias de comandos de shell, es posible agregar una línea set -x justo después la línea shebang y organícelos para que se vuelvan a ejecutar (con dpkg --configure -a para postinst) para ver precisamente lo que está sucediendo y dónde está fallando. Esta salida también puede complementar muy bien cualquier informe de error que puede presentar.

Con este conocimiento recién adquirido, puede solucionar el problema subyacente o transformar el comando fallido en uno que funciona (por ejemplo, agregando || verdadero al final de la línea).

Tenga en cuenta que este consejo no funciona para una preinst fallida ya que ese script se ejecuta incluso antes el paquete se instala, por lo que aún no está en su ubicación final. Funciona para postrm y prerm aunque deberá ejecutar la eliminación de un paquete (respectivamente actualización) para activarlos.

El archivo de registro dpkg

La herramienta dpkg mantiene un registro de todas sus acciones en /var/log/dpkg.log . Este registro es extremadamente detallado, ya que detalla todas las etapas de cada paquete. Además de ofrecer una forma de rastrear el comportamiento de dpkg ior, ayuda a mantener un historial del desarrollo del sistema: puede encontrar el momento exacto cuando cada paquete ha sido instalado o actualizado, y esta información puede ser extremadamente útil en entender un cambio reciente en el comportamiento. Además, con todas las versiones grabadas, es es fácil verificar la información con changelog.Debian.gz para los paquetes en cuestión, o incluso con informes de errores en línea.

Page 215

```
# tail /var/log/dpkg.log
2016-12-22 09:04:05 estado instalado kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 paquetes de inicio eliminar
2016-12-22 09:20:07 estado instalado kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 eliminar kali-linux-gpu: amd64 2016.3.2 <ninguno>
2016-12-22 09:20:07 estado medio configurado kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 estado medio instalado kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 status config-files kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 status config-files kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 status config-files kali-linux-gpu: amd64 2016.3.2
2016-12-22 09:20:07 estado no instalado kali-linux-gpu: amd64 <ninguno>
```

Reinstalar paquetes con apt --reinstall y aptitude reinstall

Cuando daña su sistema por error al eliminar o modificar ciertos archivos, la forma más fácil para restaurar el almacén, instale el paquete afectado. Desafortunadamente, el sistema de embalaje encuentra que el paquete ya está instalado y educadamente se niega a reinstalarlo. Para evitar esto, use --reinstall opción de los comandos apt y apt-get . El siguiente comando reinstala *postfix* incluso si es ya presente:

```
# apt --reinstalar instalar postfix
```

La línea de comando de aptitude es ligeramente diferente pero logra el mismo resultado con aptitude reinstalar postfix . El comando dpkg no impide la reinstalación, pero rara vez se llama directamente.

No use apt - reinstalar para recuperar de un ataque	Usar apt --reinstall para restaurar paquetes modificados durante un ataque ciertamente No recuperar el sistema como estaba. Después de un ataque, no puede confiar en nada: dpkg y apt podrían haber sido reemplazados por programas maliciosos, no reinstalar los archivos como le gustaría que lo hagan. El atacante También podría haber alterado o creado archivos fuera del control de dpkg .

Recuerde que también puede especificar una distribución específica con apt , lo que significa que puede rodar volver a una versión anterior de un paquete (si, por ejemplo, sabe que funciona bien), siempre que todavía está disponible en una de las fuentes a las que hace referencia el archivo sources.list :

```
# apt install w3af / kali-rolling
```

*Apalancamiento --force- * para reparar dependencias rotas*

Si no tiene cuidado, el uso de una opción --force- * o algún otro mal funcionamiento puede conducir a un sistema donde la familia de comandos APT se negará a funcionar. En efecto, algunas de estas opciones permiten

instalación de un paquete cuando no se cumple una dependencia, o cuando hay un conflicto. El resultado es un sistema inconsistente desde el punto de vista de las dependencias, y los comandos APT rechazarán para ejecutar cualquier acción, excepto las que harán que el sistema vuelva a un estado consistente (esto a menudo consiste en instalar la dependencia que falta o eliminar un paquete problemático). Esto por lo general da como resultado un mensaje como este, obtenido después de instalar una nueva versión de *rdesktop* mientras se ignora su dependencia de una versión más nueva de *libc6* :

```
# apt full-upgrade
[...]
Es posible que desee ejecutar 'apt-get -f install' para corregirlos.
Los siguientes paquetes tienen dependencias insatisfechas:
rdesktop: Depende: libc6 (> = 2.5) pero 2.3.6.ds1-13etch7 está instalado
E: dependencias insatisfechas. Intenta usar -f.
```

Si usted es un administrador valiente que está seguro de la exactitud de su análisis, puede elija ignorar una dependencia o conflicto y use la opción --force- * correspondiente. En este caso, si desea poder seguir usando apt o aptitude , debe editar / var / lib / dpkg / status para eliminar o modificar la dependencia o conflicto que ha elegido anular.

Esta manipulación es un truco feo y nunca debe usarse, excepto en el caso más extremo de necesidad. Con bastante frecuencia, una solución más adecuada es recompilar el paquete que está causando el problema o use una nueva versión (potencialmente corregida) de un repositorio que proporcione backports (los backports son versiones más nuevas especialmente recompiladas para trabajar en un entorno antiguo).

8.2.7. Frontales: aptitud y sináptica

APT es un programa C ++ cuyo código reside principalmente en la biblioteca compartida libapt-pkg . Gracias a esto biblioteca compartida, abrió la puerta para la creación de interfaces de usuario (front-end), ya que El código de la biblioteca se puede reutilizar fácilmente. Históricamente, apt-get solo fue diseñado como un front-end de prueba para libapt-pkg pero su éxito tiende a ocultar este hecho.

Con el tiempo, a pesar de la popularidad de las interfaces de línea de comandos como apt y apt-get , varios gráficos Se desarrollaron interfaces ical. Echaremos un vistazo a dos de esas interfaces en esta sección: aptitud y sináptica .

Aptitud

Aptitud, que se muestra en la Figura 8.1, " El administrador de paquetes de aptitud"[Página 191], es un programa interactivo
gramo que se puede utilizar en modo semi-gráfico en la consola. Puedes navegar por la lista de instaladas
y paquetes disponibles, busque toda la información y seleccione paquetes para instalar o eliminar. los
El programa está diseñado específicamente para ser utilizado por los administradores, por lo que su comportamiento predeterminado es mucho más
inteligente que APT, y su interfaz mucho más fácil de entender.

Figura 8.1 *El administrador de paquetes de aptitude*

Cuando ejecuta aptitude , se le muestra una lista de paquetes ordenados por estado (instalado, no instalado,
o instalado pero no disponible en los espejos), mientras que otras secciones muestran tareas, paquetes virtuales,
y nuevos paquetes aparecieron recientemente en los espejos. Para facilitar la navegación temática, otras vistas
están disponibles.

En todos los casos, aptitude muestra una lista que combina categorías y paquetes en la pantalla. Categorias
se organizan a través de una estructura de árbol, cuyas ramas se pueden desplegar o plegar respectivamente
con las teclas Enter, [y]. La tecla + debe usarse para marcar un paquete para la instalación, - para marcar
para quitarlo y para purgarlo. Tenga en cuenta que estas teclas también se pueden usar para categorías, en cuyo caso
Las acciones correspondientes se aplicarán a todos los paquetes de la categoría. Las actualizaciones clave u
La lista de paquetes disponibles y Shift + u prepara una actualización global del sistema. La tecla g cambia
a una vista de resumen de los cambios solicitados (y al escribir g nuevamente se aplicarán los cambios), y q
sale de la vista actual. Si está en la vista inicial, esto cerrará la aptitud .

Documentación de aptitude Esta sección no cubre los detalles más finos del uso de aptitude , sino que se centra en dándote un kit de supervivencia para el usuario. la aptitud está bastante bien documentada y le aconsejamos utilizar su manual completo disponible en el paquete *aptitude-doc-en* .

[2] archivo: ///usr/share/doc/aptitude/html/en/index.html

Para buscar un paquete, puede escribir / seguido de un patrón de búsqueda. Este patrón coincide con el
nombre del paquete, pero también se puede aplicar a la descripción (si va precedido de ~ d), a la sección

(con ~ s), u otras características detalladas en la documentación. Los mismos patrones pueden filtrar
la lista de paquetes mostrados: escriba la tecla l (como en el *límite*) e ingrese el patrón.

Gestionar el *indicador automático* de paquetes Debian (ver sección 8.3.4, " Rastreo automático en-
Paquetes estancados "[página 199]) es una brisa con aptitud . Es posible navegar por la lista de instaladas
paquetes y marque paquetes como automáticos con Shift + mo puede eliminar la marca con m
llave. Los paquetes automáticos se muestran con una "A" en la lista de paquetes. Esta característica también ofrece
Una forma sencilla de visualizar los paquetes en uso en una máquina, sin todas las bibliotecas y
negaciones que realmente no te importan. El patrón relacionado que se puede usar con l (para activar
el modo de filtro) es ~ i! ~ M. Especifica que solo desea ver los paquetes instalados (~ i) no marcados
como automático (! ~ M).

Usando aptitud en el Interfaz de línea de comandos

Se puede acceder a la mayoría de las funciones de Aptitude a través de la interfaz interactiva, así como a través de La línea de comandos. Estas líneas de comando les resultarán familiares a los usuarios habituales de apt-obtener y apt-cache .

Las características avanzadas de aptitude también están disponibles en la línea de comandos. Usted puede use los mismos patrones de búsqueda de paquetes que en la versión interactiva. Por ejemplo, si desea limpiar la lista de paquetes instalados manualmente, y si sabe que ninguno de los programas instalados localmente requiere bibliotecas particulares o módulos Perl, Puede marcar los paquetes correspondientes como automáticos con un solo comando:

```
# aptitude markauto '~ slibs | ~ sperl'
```

Aquí, puede ver claramente el poder del sistema de aptitud del patrón de búsqueda , que permite la selección instantánea de todos los paquetes en las secciones libs y perl .

Cuidado, si algunos paquetes están marcados como automáticos y si ningún otro paquete depende en ellos, serán eliminados inmediatamente (después de una solicitud de confirmación).

Administrar recomendaciones, sugerencias y tareas Otra característica interesante de aptitud es el hecho de que respeta las recomendaciones entre paquetes y al mismo tiempo brinda a los usuarios la opción de no instalarlos caso por caso. Por ejemplo, el paquete *gnome* recom-Mends *Gdebi* (entre otros). Cuando selecciona el primero para la instalación, el segundo también será seleccionado (y marcado como automático si aún no está instalado en el sistema). Escribir g lo hará obvio: *gdebi* aparece en la pantalla de resumen de acciones pendientes en la lista de paquetes instalados automáticamente para satisfacer dependencias. Sin embargo, puede decidir no instalarlo deseleccionándolo antes de confirmar las operaciones.

Tenga en cuenta que esta función de seguimiento de recomendaciones no se aplica a las actualizaciones. Por ejemplo, si un nuevo la versión de *gnome* recomienda un paquete que no se recomendó anteriormente, el paquete no será marcado para la instalación. Sin embargo, aparecerá en la pantalla de actualización para que el administrador Todavía puede seleccionarlo para la instalación.

Las sugerencias entre paquetes también se tienen en cuenta, pero de una manera adaptada a sus especificaciones. estado cific. Por ejemplo, dado que *gnome* sugiere *dia-gnome* , este último se mostrará en la suma

pantalla de Mary de acciones pendientes (en la sección de paquetes sugeridos por otros paquetes). Esta es visible y el administrador puede decidir si tiene en cuenta la sugerencia o no. Como es solo una sugerencia y no una dependencia o una recomendación, el paquete no se selecciona automáticamente: su selección requiere intervención manual (por lo tanto, el paquete no se marcará como automático).

En el mismo espíritu, recuerde que la aptitud hace un uso inteligente del concepto de tareas. Ya que las tareas se muestran como categorías en las pantallas de las listas de paquetes, puede seleccionar una tarea completa para la instalación o eliminación o explore la lista de paquetes incluidos en la tarea para seleccionar una más pequeña subconjunto.

Algoritmos de mejor solucionador para concluir esta suposición, notemos que la aptitud tiene más trabajo algoritmos en comparación con apt cuando se trata de resolver situaciones difíciles. Cuando un conjunto de acciones se solicita y cuando estas acciones combinadas conduzcan a un sistema incoherente, aptitud evalúa varios escenarios posibles y presenta el menor orden de disminución de relevancia. Sin embargo, Estos algoritmos no son infalibles. Afortunadamente, siempre existe la posibilidad de seleccionar manualmente Las acciones a realizar. Cuando las acciones seleccionadas actualmente conducen a contradicciones, la parte superior de la pantalla indica una cantidad de paquetes rotos (puede navegar directamente a esos paquetes presionando b). Entonces puede construir manualmente una solución. En particular, puede obtener acceso a diferentes versiones disponibles seleccionando el paquete con Enter. Si la selección de uno de estos versiones resuelve el problema, no debe dudar en utilizar la función. Cuando el número de los paquetes rotos se reducen a cero, puede ir con seguridad a la pantalla de resumen de acciones pendientes para un último cheque antes de aplicarlos.

Registro de Aptitude Al igual que dpkg , aptitude mantiene un rastro de acciones ejecutadas en su archivo de registro (/ var / log / aptitud). Sin embargo, dado que ambos comandos funcionan a un nivel muy diferente, no puede encontrar la misma información en sus respectivos archivos de registro. Mientras dpkg registra toda la opera-

ejecutadas en paquetes individuales paso a paso. aptitudeofrece una visión más amplia de operaciones de alto nivel como una actualización de todo el sistema.

Cuidado, este archivo de registro solo contiene un resumen de las operaciones realizadas por aptitude . Si ocasionalmente se usan otros front-end (o incluso dpkg), el registro de aptitude solo contendrá una vista parcial de las operaciones, por lo que no puede confiar en ella para construir un historia confiable del sistema.

Sináptico

Synaptic es un administrador de paquetes gráficos que presenta una interfaz gráfica limpia y eficiente (se muestra en la Figura 8.2 , "Administrador de paquetes sináptico "[página 194]) basado en GTK + y GNOME. Sus muchos filtros listos para usar brindan acceso rápido a paquetes recientemente disponibles, paquetes instalados, actualizaciones paquetes capaces, paquetes obsoletos, etc. Si navega por estas listas, puede seleccionar las operaciones a realizar en los paquetes (instalar, actualizar, eliminar, purgar); estas operaciones son no se realiza de inmediato, pero se coloca en una lista de tareas. Un solo clic en un botón luego valida el operaciones y se realizan de una vez.

Figura 8.2 *Administrador de paquetes sináptico*

8.3. Configuración avanzada de APT y uso

Ahora es el momento de sumergirse en algunos temas más avanzados. Primero, echaremos un vistazo a avanzado configuración de APT, que le permitirá establecer opciones más permanentes que se aplicarán a APT herramientas. Luego mostraremos cómo se pueden manipular las prioridades del paquete, lo que abre la puerta para actualizaciones y actualizaciones personalizadas y bien ajustadas. Wewillalsoshowhowtohandlemultiple distribuciones para que pueda comenzar a experimentar con paquetes que provienen de otras distribuciones. A continuación, tomaremos un vistazo para hacer un seguimiento de paquetes instalados automáticamente, capacidad de almacenamiento para administrar paquetes que se instalan a través de dependencias. También explicaremos cómo multi- El soporte de arco abre la puerta para ejecutar paquetes creados para varias arquitecturas de hardware. Último

pero no menos importante, discutiremos los protocolos criptográficos y las utilidades vigentes que le permitirán validar la autenticidad de cada paquete.

8.3.1. Configurar APT

Antes de sumergirnos en la configuración de APT, tomemos un momento para discutir la configuración

mecanismo del sistema Debian. Históricamente, la configuración fue manejada por configuraciones dedicadas archivos de secciones. Sin embargo, en sistemas Linux modernos como Debian y Kali, los directorios de configuración con El sufijo .d se está volviendo más utilizado. Cada directorio representa un archivo de configuración eso se divide en múltiples archivos. En este sentido, todos los archivos en /etc/apt/apt.conf.d/ son instrucopciones para la configuración de APT. APT procesa los archivos en orden alfabético, de modo que Los archivos pueden modificar los elementos de configuración definidos en los archivos anteriores.

Esta estructura brinda cierta flexibilidad a los administradores y mantenedores de paquetes, permitiéndoles para realizar cambios en la configuración del software mediante la adición de archivos sin tener que cambiar un archivo isting. Esto es especialmente útil para los mantenedores de paquetes porque pueden usar este enfoque adaptar la configuración de otro software para asegurar que coexista perfectamente con el suyo, con: rompiendo la política de Debian que prohíbe explícitamente modificar archivos de configuración de otros paquetes siglos. Debido al mecanismo de configuración .d , no tiene que seguir manualmente múltiples las instrucciones de configuración del paquete generalmente se encuentran en el paquete / usr / share / doc / *package* /README.Debian , ya que el instalador puede colocar archivos de configuración.

Cuidado con la configuración Archivos generados a partir de .d Directorios

Si bien APT tiene soporte nativo de su directorio /etc/apt/apt.conf.d , esto no es todomaneras el caso. Para algunas aplicaciones (como exim, por ejemplo), el directorio .d es un Adición específica de Debian utilizada como entrada para generar dinámicamente la configuración canónica. archivo de ración utilizado por la aplicación. En esos casos, los paquetes proporcionan una "actualización- *" comando (por ejemplo: update-exim4.conf) que concatenará los archivos del .d directorio y sobrescribe el archivo de configuración principal.

En esos casos, no debe editar manualmente el archivo de configuración principal como sus cambios se perderá en la próxima ejecución del comando update- * , y tampoco debe olvide ejecutar el comando anterior después de haber editado un archivo fuera del directorio .d (o sus cambios no serán utilizados).

Armado con una comprensión del mecanismo de configuración .d , hablemos de cómo puede aprovecharlo para configurar APT. Como hemos discutido, puede alterar el comportamiento de APT a través de argumentos de línea de comandos para dpkg como este ejemplo, que realiza una instalación forzada de sobrescritura de zsh :

```
# apt -o Dpkg :: Opciones :: = ”- forzar-sobrescribir” instalar zsh
```

Obviamente, esto es muy engorroso, especialmente si usa opciones con frecuencia, pero también puede usar la estructura de configuración del directorio .d para configurar ciertos aspectos de APT agregando directivas a un archivo en el directorio /etc/apt/apt.conf.d/ . Por ejemplo, esta (y cualquier otra) directiva puede

se puede agregar fácilmente a un archivo en /etc/apt/apt.conf.d/ . El nombre de este archivo es algo arbitrario, pero una convención común es usar local o 99local :

```
$ cat /etc/apt/apt.conf.d/99local
Dpkg :: Opciones {
      "--Force-sobrescribe";
}
```

Hay muchas otras opciones de configuración útiles y ciertamente no podemos cubrirlas todas, pero uno que tocaremos involucra conectividad de red. Por ejemplo, si solo puede acceder a la web a través de un proxy, agregue una línea como Adquirir :: http :: proxy "http: // *yourproxy* : 3128". Para un proxy FTP, use Acquire :: ftp :: proxy "ftp: // *yourproxy* ".

Para descubrir más opciones de configuración, lea la página de manual de apt.conf (5) con man apt. comando conf (para obtener detalles sobre las páginas del manual, consulte la sección 6.1.1, “ Páginas del manual ” [página 124]).

8.3.2. Administrar prioridades de paquete

Uno de los aspectos más importantes en la configuración de APT es la gestión de las prioridades. lazos asociados con cada fuente de paquetes. Por ejemplo, es posible que desee prolongar su Kalali Rolling sistema con uno o dos paquetes más nuevos de Debian Unstable o Debian Experimental. Es pos- Es posible asignar una prioridad a cada paquete disponible (el mismo paquete puede tener varias prioridades dependiendo de su versión o la distribución que lo proporcione). Estas prioridades influirán en los APT comportamiento: para cada paquete, siempre seleccionará la versión con la máxima prioridad (excepto si esta versión es anterior a la instalada y su prioridad es inferior a 1000).

APT define varias prioridades predeterminadas. Cada versión de paquete instalada tiene una prioridad de 100. La versión instalada tiene una prioridad de 500 por defecto, pero puede saltar a 990 si es parte del objetivo release (definido con la opción de línea de comandos -t o APT :: Default-Release configuration directive).

Puede modificar las prioridades agregando entradas en el archivo / etc / apt / preferencias con los nombres de los paquetes afectados, su versión, su origen y su nueva prioridad.

APT nunca instalará una versión anterior de un paquete (es decir, un paquete cuyo número de versión es menor que el del paquete instalado actualmente) excepto cuando su prioridad sea superior a 1000. APT siempre instalará el paquete de mayor prioridad que siga esta restricción. Si dos paquetes tienen la misma prioridad, APT instala el más nuevo (cuyo número de versión es el más alto). Si dos paquetes de la misma versión tienen la misma prioridad pero difieren en su contenido, APT instala el versión que no está instalada (esta regla se ha creado para cubrir el caso de una actualización de paquete sin el incremento del número de revisión, que generalmente se requiere).

En términos más concretos, nunca se instalará un paquete cuya prioridad sea inferior a 0. Un paquete con un rango de prioridad entre 0 y 100 se instalará de forma gratuita si no hay otra versión del paquete ya instalado. Con una prioridad entre 100 y 500, el paquete solo se instalará si hay

Página 223

No hay otra versión más nueva instalada o disponible en otra distribución. Un paquete de prioridad entre 501 y 990 solo se instalarán si no hay una versión más nueva instalada o disponible en el distribución objetivo. Con una prioridad entre 990 y 1000, el paquete se instalará excepto si La versión instalada es más nueva. Una prioridad superior a 1000 siempre conducirá a la instalación de el paquete incluso si obliga a APT a degradar a una versión anterior.

Cuando APT verifica / etc / apt / preferencias , primero tiene en cuenta las entradas más específicas (a menudo los que especifican el paquete en cuestión), luego los más genéricos (incluso para el examen- ple todos los paquetes de una distribución). Si existen varias entradas genéricas, se utiliza la primera coincidencia. los Los criterios de selección disponibles incluyen el nombre del paquete y la fuente que lo proporciona. Cada paquete la fuente se identifica por la información contenida en un archivo Release que APT descarga conjuntamente con los archivos de paquetes . Estos archivos especifican el origen, generalmente "Kali" para los paquetes de Kali réplicas oficiales y "Debian" para los paquetes de las réplicas oficiales de Debian, pero el origen puede también sea el nombre de una persona o de una organización para repositorios de terceros. El archivo de lanzamiento también proporciona el nombre de la distribución junto con su versión. Echemos un vistazo a su sintaxis a través de algunos estudios de casos realistas de este mecanismo.

Prioridad de Kali-Bleeding-Edge y Debian Experimental

Si incluiste kali-bleeding-edge o Debian experimental en tu archivo sources.list , los paquetes correspondientes casi nunca se instalarán porque su APT predeterminado la prioridad es 1. Este es, por supuesto, un caso específico, diseñado para evitar que los usuarios instalen paquetes de última generación por error. Los paquetes solo pueden instalarse escribiendo apt instale el*paquete* / kali-bleeding-edge , suponiendo, por supuesto, que tenga conocimiento de Los riesgos y posibles dolores de cabeza de la vida al límite. Todavía es posible (aunque *no* reco- recomendado) para tratar paquetes de kali-sangrado / experimental como los de otros distribuciones dándoles una prioridad de 500. Esto se hace con una entrada específica en / etc / apt / preferencias :

```
Paquete: *
Pin: suelte a = borde de sangrado kali
Prioridad de clavija: 500
```

Supongamos que solo quiere usar paquetes de Kali y que solo quiere paquetes Debian- edades instaladas cuando se solicita explícitamente. Puede escribir las siguientes entradas en / etc / apt / archivo de preferencias (o en cualquier archivo en /etc/apt/preferences.d/):

```
Paquete: *
Pin: liberar o = Kali
Prioridad de clavija: 900

Paquete: *
Pin: lanzamiento o = Debian
Prioridad de clavija: -10
```


Página 224

En los últimos dos ejemplos, ha visto un = kali-sangrado-borde, que define el nombre de la se- distribución seleccionada y o = Kali y o = Debian, que limitan el alcance a paquetes cuyo origen es Kali y Debian, respectivamente.

Supongamos que tiene un servidor con varios programas locales que dependen de la versión 5.22 de Perl y que desea asegurarse de que las actualizaciones no instalen otra versión de la misma. Tú podrías usa esta entrada:

```
Paquete: perl
Pin: versión 5.22 *
Prioridad de clavija: 1001
```

La documentación de referencia para este archivo de configuración está disponible en la página del manual apt_preferences (5) , que puede mostrar con man apt_preferences .

Agregar comentarios en / etc / apt / preferencias

No hay una sintaxis oficial para comentarios en / etc / apt / preferencias , pero algunos textos se pueden proporcionar descripciones anteponiendo uno o más campos de Explicación en cada entrada:

```
Explicación: El paquete xserver-xorg-video-intel proporcionado
Explicación: en experimental se puede usar de forma segura
Paquete: xserver-xorg-video-intel
Pin: liberar a = experimental
Prioridad de clavija: 500
```

8.3.3. Trabajando con varias distribuciones

Dado que apt es una herramienta tan maravillosa, es probable que desee sumergirse y comenzar a experimentar con paquetes que vienen de otras distribuciones. Por ejemplo, después de instalar un sistema KalaliRollings, es posible que desee probar un paquete de software disponible en Kali Dev, Debian Unstable o Debian Experimental sin divergir demasiado del estado inicial del sistema.

Incluso si ocasionalmente encuentra problemas al mezclar paquetes de diferentes distribuciones Además, apt gestiona muy bien dicha coexistencia y limita los riesgos de manera muy eficaz (siempre que las dependencias del paquete son precisas). Primero, enumere todas las distribuciones utilizadas en /etc/apt/sources.list y defina su distribución de referencia con el parámetro APT :: Default-Release (consulte la sección 8.2.3 , " Actualización de Kali Linux " [página 179]).

Supongamos que Kali Rolling es su distribución de referencia, pero que Kali Dev y Debian Unstable también se enumeran en su archivo sources.list . En este caso, puede usar apt install *package* / inestable para instalar un paquete desde Debian Unstable. Si la instalación falla debido a algún error dependencias confiables, deje que resuelva esas dependencias dentro de Inestable agregando -t inestable parámetro.

En esta situación, las actualizaciones (actualización y actualización completa) se realizan dentro de Kali Rolling a excepción de los paquetes ya están actualizados a otra distribución: los siguientes seguirán las fechas disponibles en el otro distribuciones Supondremos que esta conducta se comporta con la ayuda de las prioridades predeterminadas establecidas por APT a continuación. No dude en usar la política apt-cache (consulte la barra lateral " Uso de la política apt-cache "[página 199]) para verificar las prioridades dadas.

Todo se basa en el hecho de que APT solo considera paquetes de versiones superiores o iguales que el paquete instalado (suponiendo que / etc / apt / preferencias no se ha utilizado para forzar prioridades superior a 1000 para algunos paquetes).

Usar la política de apt-cache

Para obtener una mejor comprensión del mecanismo de prioridad, no dude en ejecutar linda política de apt-cache para mostrar la prioridad predeterminada asociada con cada paquete fuente. También puede usar el *paquete de* políticas apt-cache para mostrar las prioridades de todos versiones disponibles de un paquete dado.

Supongamos que ha instalado la versión 1 de un primer paquete de *KaliRolling* y que la versión 2 y 3 están disponibles respectivamente en *Kali Dev* y *Debian Unstable* . La versión instalada tiene prioridad de 100 pero la versión disponible en *Kali Rolling* (la misma) tiene una prioridad de 990 (porque es parte del lanzamiento objetivo). Los paquetes en *Kali Dev* y *Debian Unstable* tienen una prioridad de 500 (el prioridad predeterminada de una versión no instalada). El ganador es, por lo tanto, la versión 1 con una prioridad de 990. El paquete se queda en *Kali Rolling* .

Tomemos el ejemplo de otro paquete cuya versión 2 ha sido instalada desde *Kali Dev* . Ver- *La* versión 1 está disponible en *Kali Rolling* y la versión 3 en *Debian Unstable* . Versión 1 (de prioridad 990, por lo tanto inferior a 1000) se descarta porque es inferior a la versión instalada. Esto solo deja version 2 y 3, ambas de prioridad 500. Ante esta alternativa, APT selecciona la versión más nueva, la

uno de *Debian Unstable* . Si no desea que un paquete instalado desde *Kali Dev* migre a *Debian Inestable* , debe asignar una prioridad inferior a 500 (490 por ejemplo) a los paquetes procedentes de *Debian inestable* . Puede modificar / etc / apt / preferencias a este efecto:

```
Paquete: *
Pin: suelte a = inestable
Prioridad de clavija: 490
```

8.3.4. Seguimiento de paquetes instalados automáticamente

Una de las funcionalidades esenciales de apt es el seguimiento de paquetes instalados solo a través de pendencias Estos paquetes se denominan *automáticos* y a menudo incluyen bibliotecas.

Con esta información, cuando se eliminan los paquetes, los administradores de paquetes pueden calcular una lista de paquetes automáticos que ya no son necesarios (porque no hay paquetes instalados manualmente dependiendo de ellos). El comando apt autoremove eliminará los paquetes. Aptitud

no tiene este comando porque los elimina automáticamente tan pronto como se identifican. En En todos los casos, las herramientas muestran un mensaje claro que enumera los paquetes afectados.

Es una buena costumbre marcar como automático cualquier paquete que no necesite directamente para que se eliminan automáticamente cuando ya no son necesarios. Puedes usar apt-mark auto *paquete* para marcar el paquete dado como automático, mientras que el *paquete* manual apt-mark hace el opuesto. aptitude markauto y aptitude unmarkauto funcionan de la misma manera, aunque ofrecer más características formatear muchos paquetes al mismo tiempo (ver sección 8.2.7.1 , " Aptitud "[página190]). La interfaz interactiva de aptitude basada en la consola también facilita la revisión automática bandera en muchos paquetes.

Es posible que desee saber por qué un paquete instalado automáticamente está presente en el sistema. Llegar esta información desde la línea de comandos, puede usar aptitude why *package* (apt y apt-get no tienen una característica similar):

```
$ aptitude por qué python-debian
yo aptitud Recomienda apt-xapian-index
i Depende de un índice apt-xapian python-debian (> = 0.1.15)
```

8.3.5. Aprovechando la compatibilidad con múltiples arcos

Todos los paquetes de Debian tienen un campo de Arquitectura en su información de control. Este campo puede contener ya sea "todos" (para paquetes que son independientes de la arquitectura) o el nombre de la arquitectura que apunta (como amd64 o armhf). En el último caso, por defecto, dpkg solo instalará el paquete si su arquitectura coincide con la arquitectura del host según lo devuelto por dpkg --print-architecture .

Esta restricción asegura que no termines con binarios compilados para una arquitectura incorrecta Ture. Todo sería perfecto, excepto que (algunas) computadoras pueden ejecutar binarios para múltiples arquitecturas, ya sea de forma nativa (un sistema amd64 puede ejecutar binarios i386) o mediante emuladores.

Habilitar Multi-Arch

El soporte de múltiples arcos para dpkg permite a los usuarios definir arquitecturas extranjeras que se pueden instalar en El sistema actual. Esto se hace fácilmente con dpkg --add-architecture , como en el ejemplo a continuación donde la arquitectura i386 debe agregarse al sistema amd64 para ejecutar Windows ap- aplicaciones usando Wine[5] . Hay un dpkg correspondiente --remove-architecture para dejar el soporte de una arquitectura extranjera, pero solo se puede usar cuando no quedan paquetes de esta arquitectura instalado

```
# dpkg --print-architecture
amd64
```

[5] [5] https://www.winehq.org/

```
# vino
parece que falta wine32, deberías instalarlo.
multiarch necesita ser habilitado primero.  como root, por favor
ejecutar "dpkg --add-architecture i386 y apt-get update &
apt-get install wine32 ”
Uso: vino PROGRAMA [ARGUMENTOS ...]                Ejecuta el programa especificado
          vino - ayuda                             Mostrar esta ayuda y salir
          vino --versión                           Salida de información de versión y salida
# dpkg --add-architecture i386
# dpkg --print-foreign-architectures
i386
# apt update
[...]
# apt install wine32
[...]
Configuración de libwine: i386 (1.8.6-5) ...
Configuración de vdpau-driver-all: i386 (1.1.1-6) ...
Configuración de wine32: i386 (1.8.6-5) ...
Configuración de plugins libasound2: i386 (1.1.1-1) ...
Procesador de disparadores para libc-bin (2.24-9)
# vino
Uso: vino PROGRAMA [ARGUMENTOS ...]                Ejecuta el programa especificado
        vino - ayuda                               Mostrar esta ayuda y salir
        vino --versión                             Salida de información de versión y salida
# dpkg --remove-architecture i386
dpkg: error: no se puede eliminar la arquitectura 'i386' actualmente en uso por la base de datos
# dpkg --print-foreign-architectures
i386
```

APT detectará automáticamente cuándo se ha configurado dpkg para admitir arquitecturas extranjeras y comenzará a descargar los archivos de paquetes correspondientes durante su proceso de actualización.

Los paquetes externos se pueden instalar con apt install *package* : *architecture* .

Usando i386 patentado Binarios en amd64

Existen múltiples casos de uso para múltiples arcos, pero el más popular es la posibilidad ejecutar binarios de 32 bits (i386) en sistemas de 64 bits (amd64), en particular desde varios Las aplicaciones propietarias populares (como Skype) solo se proporcionan en versiones de 32 bits.

Cambios relacionados con varios arcos

Para hacer que el multi-arco sea realmente útil y utilizable, las bibliotecas tuvieron que ser reempaquetadas y trasladadas a un directorio específico de la arquitectura para que se puedan copiar múltiples copias (dirigidas a diferentes arquitecturas) instaledalongsideoneoneotherother. Dichos paquetes actualizados contienen el Multi-Arch: sameheaderfield para que el sistema de embalaje que las diversas arquitecturas del paquete puedan instalarse correctamente (y que esos paquetes solo pueden satisfacer dependencias de paquetes de la misma arquitectura).

Página 228

```
$ dpkg -s libwine
dpkg-query: error: --status necesita un nombre de paquete válido pero 'libwine' no es: ambiguo
        ¯ nombre del paquete 'libwine' con más de una instancia instalada

Use --help para obtener ayuda sobre la consulta de paquetes.
$ dpkg -s libwine: amd64 libwine: i386 |  grep ^ Multi
Multi-Arch: mismo
Multi-Arch: mismo
$ dpkg -L libgcc1: amd64 | grep .so
[...]
/usr/lib/x86_64-linux-gnu/wine/libwine.so.1
$ dpkg -S / usr / share / doc / libwine / copyright
libwine: amd64, libwine: i386: / usr / share / doc / libwine / copyright
```

Vale la pena señalar que Multi-Arch: los mismos paquetes deben tener sus nombres calificados con su arquitectura para ser inequívocamente identificable. Estos paquetes también pueden compartir archivos con otros instancias del mismo paquete; dpkg asegura que todos los paquetes tengan archivos idénticos bit por bit cuando son compartidos Además, todas las instancias de un paquete deben tener la misma versión, por lo tanto, deben Ser actualizado juntos.

El soporte Multi-Arch también presenta algunos desafíos interesantes en la forma en que se manejan las dependencias. Satisfacer una dependencia requiere que se marque el paquete Multi-Arch: paquete extranjero o cuyo paquete la arquitectura coincide con la del paquete que declara la dependencia (en esta dependencia la dependencia

proceso de solución, se supone que los paquetes independientes de la arquitectura son de la misma arquitectura como el anfitrión). Una dependencia también se puede debilitar para permitir que cualquier arquitectura la cumpla, con el *paquete* : cualquier sintaxis, pero los paquetes externos solo pueden satisfacer dicha dependencia si están marcados Multi-Arco: permitido.

8.3.6. Validación de autenticidad de paquete

Las actualizaciones del sistema son operaciones muy confidenciales y realmente desea asegurarse de que solo instale paquetes oficiales de los repositorios de Kali. Si el espejo Kali que está utilizando ha sido comprobado errado, un pirata informático podría intentar agregar código malicioso a un paquete legítimo. Dicho paquete, si está instalado, podría hacer cualquier cosa que el cracker lo diseñó para hacer, incluida la divulgación contraseñas o información confidencial. Para evitar este riesgo, Kali proporciona un sello a prueba de manipulaciones para garantizar, en el momento de la instalación, que un paquete realmente proviene de su responsable oficial y no sido modificado por un tercero.

Estas obras tienen una cadena de hash criptográficos y una firma. Los archivos firmadosel lanzamiento archivo, proporcionado por los espejos Kali. Contiene una lista de los archivos de paquetes (incluidos sus archivos formularios presionados, Packages.gz y Packages.xz , y las versiones incrementales), junto con sus MD5, SHA1 y SHA256 hashes, lo que garantiza que los archivos no hayan sido manipulados. Estas

Los archivos de paquetes se encuentran en el paquete de Debian disponible en su pantalla junto con sus cascarillas, lo que asegura a su vez que el contenido de los paquetes no haya sido alterado tampoco.

Las teclas de confianza se administran con el comando apt-key que se encuentra en el paquete *apt* . Este programa mantiene un conjunto de claves públicas de GnuPG, que se utilizan para verificar las firmas en Release.gpg archivos disponibles en los espejos. Se puede usar para agregar nuevas claves manualmente (cuando espejos no oficiales Se necesitan). Sin embargo, generalmente solo se necesitan las llaves oficiales de Kali. Estas teclas son automáticas. actualizado con el paquete *kali-archive-keyring* (que coloca los llaveros correspondientes en /etc/apt/trusted.gpg.d). Sin embargo, la primera instalación de este paquete en particular requiere precaución: incluso si el paquete está firmado como cualquier otro, la firma no se puede verificar externamente. Por lo tanto, los administradores cautelosos deben verificar las huellas digitales de las claves importadas antes de confiar ellos para instalar nuevos paquetes:

```
# huella digital apt-key
/etc/apt/trusted.gpg.d/debian-archive-jessie-automatic.gpg
------------------------------------------------------------ --------
pub         4096R / 2B90D010 2014-11-21 [caduca: 2022-11-19]
            Huella digital clave = 126C 0D24 BD8A 2942 CC7D                F8AC 7638 D044 2B90 D010
uid                              Clave de firma automática del archivo Debian (8 / jessie) <ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-security-automatic.gpg
------------------------------------------------------------ ----------------
pub         4096R / C857C906 2014-11-21 [caduca: 2022-11-19]
            Huella digital clave = D211 6914 1CEC D440 F2EB                8DDA 9D6D 8F6B C857 C906
uid                              Clave de firma automática del archivo de seguridad de Debian (8 / jessie) <ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-stable.gpg
------------------------------------------------------------ -----
pub         4096R / 518E17E1 2013-08-17 [caduca: 2021-08-15]
            Huella digital clave = 75DD C3C4 A499 F1A1 8CB5                F3C8 CBF8 D6FD 518E 17E1
uid                              Jessie Stable Release Key <debian-release@lists.debian.org>

/etc/apt/trusted.gpg.d/debian-archive-squeeze-automatic.gpg
------------------------------------------------------------ ---------
pub         4096R / 473041FA 2010-08-27 [caduca: 2018-03-05]
            Huella digital clave = 9FED 2BCB DCD2 9CDF 7626                78CB AED4 B06F 4730 41FA
uid                              Clave de firma automática del archivo Debian (6.0 / squeeze) <ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-squeeze-stable.gpg
------------------------------------------------------------ ------
pub         4096R / B98321F9 2010-08-07 [caduca: 2017-08-05]
            Huella digital clave = 0E4E DE2C 7F3E 1FC0 D033                800E 6448 1591 B983 21F9
uid                              Apriete la tecla de liberación estable <debian-release@lists.debian.org>

/etc/apt/trusted.gpg.d/debian-archive-wheezy-automatic.gpg
------------------------------------------------------------ --------
pub         4096R / 46925553 2012-04-27 [caduca: 2020-04-25]
            Huella digital clave = A1BD 8E9D 78F7 FE5C 3E65                D8AF 8B48 AD62 4692 5553
uid                              Clave de firma automática del archivo Debian (7.0 / wheezy) <ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-wheezy-stable.gpg
------------------------------------------------------------ -----
pub         4096R / 65FFB764 2012-05-08 [caduca: 2019-05-07]
            Huella digital clave = ED6D 6527 1AAC F0FF 15D1                2303 6FB2 A1C2 65FF B764
uid                              Clave de lanzamiento estable de Wheezy <debian-release@lists.debian.org>
```

```
/etc/apt/trusted.gpg.d/kali-archive-keyring.gpg
------------------------------------------------
pub   4096R / 7D8D0BF6 2012-03-05 [caduca: 2018-02-02]
      Huella digital clave = 44C6 513A 8E4F B3D3 0875 F758 ED44 4FF0 7D8D 0BF6
uid                  Kali Linux Repository <devel@kali.org>
sub   4096R / FC0D0DCB 2012-03-05 [caduca: 2018-02-02]
```

Cuando se agrega una fuente de paquete de terceros al archivo sources.list , se debe indicar a APT que confíe en la clave de autenticación GPG correspondiente (de lo contrario, seguirá quejándose de que no puede asegurar la autenticidad de los paquetes que provienen de ese repositorio). El primer paso es, por supuesto. para obtener la clave pública. La mayoría de las veces, la clave se proporcionará como un pequeño archivo de texto, que llamará a key.asc en los siguientes ejemplos.

Para agregar la clave al llavero de confianza, el administrador puede ejecutar apt-key add <key.asc . Unotra forma es usar la interfaz gráfica sináptica : su pestaña Autenticación en la Configuración → *El* menú Repositorios brinda la posibilidad de importar una clave desde el archivo key.asc .

Para las personas que se dedican a la aplicación de aplicaciones y más detalles sobre las claves confiables, es posible use gui-apt-key (en el paquete del mismo nombre), como una interfaz de usuario gráfica que administra El llavero de confianza.

Una vez que las claves apropiadas estén en el llavero, APT verificará las firmas antes de cualquier operación arriesgada. para que los front-end muestren una advertencia si se le pide que instale un paquete cuya autenticidad No se puede determinar.

8.4. Referencia del paquete: profundizar en el sistema de paquetes Debian

Ahora es el momento de sumergirse realmente en el sistema de paquetes de Debian y Kali. En este punto, estamos irá más allá de las herramientas y la sintaxis y se centrará más en las tuercas y tornillos del embalaje sistema. Esta vista detrás de escena lo ayudará a comprender cómo funciona APT en su base y le dará una idea de cómo optimizar y personalizar seriamente su sistema Kali. usted puede que no necesariamente memorice todo el material de esta sección, pero el recorrido y la referencia El material le servirá bien a medida que crezca en su dominio del sistema Kali Linux.

Hasta ahora, ha interactuado con el paquete de datos de APT a través de las diversas herramientas diseñadas para la interfaz con eso. A continuación, profundizaremos y echaremos un vistazo dentro de los paquetes y observaremos el *meta-* interno. *información* (o información sobre otra información) utilizada por las herramientas de administración de paquetes.

Esta combinación de un archivo comprimido y de metainformación es directamente visible en la estructura de un .deb , que es simplemente un archivo ar, concatenando tres archivos:

```
$ ar t /var/cache/apt/archives/apt_1.4~beta1_amd64.deb
debian-binary
control.tar.gz
data.tar.xz
```

El archivo binario debian contiene un solo número de versión que describe el formato del archivo:


```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb debian-binary
2,0
```

El archivo control.tar.gz contiene metainformación:

```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb control.tar.gz | tar -tzf -
./
./conffiles
./controlar
./md5sums
./postinst
./postrm
./preinst
./prerm
./shlibs
./activadores
```

Y finalmente, el archivo data.tar.xz (el formato de compresión puede variar) contiene el archivo real

archivos que se instalarán en el sistema de archivos:

```
$ ar p /var/cache/apt/archives/apt_1.4~beta1_amd64.deb data.tar.xz | tar -tJf -
./
./etc/
./etc/apt/
./etc/apt/apt.conf.d/
./etc/apt/apt.conf.d/01autoremove
./etc/apt/preferences.d/
./etc/apt/sources.list.d/
./etc/apt/trusted.gpg.d/
./etc/cron.daily/
./etc/cron.daily/apt-compat
./etc/kernel/
./etc/kernel/postinst.d/
./etc/kernel/postinst.d/apt-auto-removal
./etc/logrotate.d/
./etc/logrotate.d/apt
./lib/
./lib/systemd/
[...]
```

Tenga en cuenta que en este ejemplo, está viendo un paquete `.deb` en el caché de archivos de APT y que su El archivo puede contener archivos con números de versión diferentes a los que se muestran.

En esta sección, presentaremos esta metainformación contenida en cada paquete y le mostraremos cómo aprovecharlo.

8.4.1 El archivo de `control`

Comenzaremos mirando el archivo de `control`, que está contenido en el archivo `control.tar.gz`. El archivo de `control` contiene la información más vital sobre el paquete. Utiliza una estructura similar para enviar encabezados por correo electrónico y se puede ver con el comando `dpkg -I`. Por ejemplo, el archivo de `control` para *apt se* ve así:

```
$ dpkg -I apt_1.4 ~ beta1_amd64.deb control
Paquete: apto
Versión: 1.4 ~ beta1
Arquitectura: amd64
Mantenedor: Equipo de Desarrollo APT <deity@lists.debian.org>
Tamaño instalado: 3478
Depende: adduser, gpgv | gpgv2 | gpgv1, debian-archive-keyring, init-system-helpers (> =
 ¯ 1.18 ~), libapt-pkg5.0 (> = 1.3 ~ rc2), libc6 (> = 2.15), libgcc1 (> = 1: 3.0),
 ¯ libstdc ++ 6 (> = 5.2)
Recomienda: gnupg | gnupg2 | gnupg1
Sugiere: apt-doc, aptitude | sináptica | wajig, dpkg-dev (> = 1.17.2), powermgmt-base,
 ¯ python-apt
Saltos: apt-utils (<< 1.3 ~ exp2 ~)
Reemplaza: apt-utils (<< 1.3 ~ exp2 ~)
Sección: admin
Prioridad: importante
Descripción: administrador de paquetes de línea de comandos
  Este paquete proporciona herramientas de línea de comandos para buscar y
  gestionar y consultar información sobre paquetes
  como un acceso de bajo nivel a todas las funciones de la biblioteca libapt-pkg.
  .
  Éstas incluyen:
    * apt-get para recuperar paquetes e información sobre ellos
       de fuentes autenticadas y para instalación, actualización y
       eliminación de paquetes junto con sus dependencias
    * apt-cache para consultar la información disponible sobre instalado
       así como paquetes instalables
    * apt-cdrom para usar medios extraíbles como fuente de paquetes
    * apt-config como interfaz para la configuración
    * apt-key como interfaz para administrar claves de autenticación
```

En esta sección, lo guiaremos a través del archivo de control y le explicaremos los diversos campos. Cada uno de esto le dará una mejor comprensión del sistema de empaque, le dará más detalles control de configuración y proporcionarle la información necesaria para solucionar problemas que pueden

ocurrir.

Página 233

Dependencias: el campo depende

Las dependencias del paquete se definen en el campo Depende del encabezado del paquete. Esta es una lista de condiciones que se deben cumplir para que el paquete funcione correctamente: esta información es utilizada por herramientas como apto para instalar las bibliotecas requeridas, en versiones apropiadas que cumplan las dependencias de El paquete a instalar. Para cada dependencia, puede restringir el rango de versiones que cumplen esa condición En otras palabras, es posible expresar el hecho de que necesita el paquete *libc6* en una versión igual o mayor que "2.15" (escrita " libc6 (> = 2.15) "). Comparación de versiones los operadores son los siguientes:

- << : menor que;
- <= : menor o igual que;
- = : igual a (tenga en cuenta que "2.6.1" no es igual a "2.6.1-1");
- > = : mayor o igual que;
- >> : mayor que.

En una lista de condiciones que deben cumplirse, la coma sirve como separador, interpretada como un "Y" lógico. En condiciones, la barra vertical ("|") expresa un "OR" lógico (es un "OR" inclusivo, no un ex clusivo "o / o"). Con mayor prioridad que “Y”, puede usarlo tantas veces como sea necesario. Ensayo Por lo tanto, la dependencia "(A OR B) Y C" se escribe A | B, C . En contraste, el expreso La sección "A OR (B Y C)" debe escribirse como "(A OR B) Y (A OR C)", ya que el campo Depende no tolera paréntesis que cambian el orden de prioridades entre los operadores lógicos "O" y "Y". Por lo tanto, se escribiría A | B, A | C . Ver http://www.debian.org/doc/ debian-policy / ch-relations.html para más información.

El sistema de dependencias es un buen mecanismo para garantizar el funcionamiento de un programa, pero tiene otro uso con metapaquetes. Estos son paquetes vacíos que solo describen dependencias. Facilitan la instalación de un grupo consistente de programas preseleccionados por el metapaquete mantenedor; como tal, apt install *meta-package* instalará automáticamente todos estos programas utilizando las dependencias del metapaquete. Los paquetes *gnome* , *kde-full* y *kali-linux-full* son exámenes. ples de metapaquetes.

Predepende, depende más exigente

Las dependencias previas, que se enumeran en el campo Predependencias en los encabezados del paquete, completan el dependencias normales; Su sintaxis es idéntica. Una dependencia normal indica que el paquete la edad en cuestión debe desempacarse y configurarse antes de que la configuración del paquete declare La dependencia. Una dependencia previa estipula que el paquete en cuestión debe desempacarse y configurado antes de la ejecución del script de preinstalación del paquete que declara el pre dependencia, eso es antes de su instalación.

Página 234

Una dependencia previa es muy exigente para apt porque agrega una restricción estricta en el orden de Los paquetes a instalar. Como tal, se desaconsejan las dependencias previas a menos que sea absolutamente necesario. Eso isevenrecommendedtoconsultotherdeveloperson debian-devel@lists.debian.org beforeadding una dependencia previa, ya que generalmente es posible encontrar otra solución como solución alternativa.

Recomienda, sugiere y mejora los campos

Los campos Recomendar y Sugerir describen dependencias que no son obligatorias. El rec dependencias omitidas, las más importantes, mejoran considerablemente la funcionalidad ofrecida por el paquete pero no son indispensables para su funcionamiento. Las dependencias sugeridas, de secundaria importancia, indicar que ciertos paquetes pueden complementar y aumentar su utilidad respectiva,

pero es perfectamente razonable instalar uno sin los otros.
Siempre debe instalar los paquetes recomendados a menos que sepa exactamente por qué no los necesito Por el contrario, no es necesario instalar los paquetes sugeridos a menos que sepa por qué los necesito

El campo Mejora también describe una sugerencia, pero en un contexto diferente. De hecho, se encuentra en el paquete sugerido, y no en el paquete que se beneficia de la sugerencia. Su interés radica en que es posible agregar una sugerencia sin tener que modificar el paquete en cuestión.
Por lo tanto, todos los complementos, complementos y otras extensiones de un programa pueden aparecer en la lista de sugerencias Gestiones relacionadas con el software. Aunque ha existido durante varios años, este último campo sigue siendo en gran parte ignorado por programas como apt o synaptic . El objetivo original era dejar que un paquete como *xul-ext-adblock-plus* (una extensión de Firefox) declara Enhances: firefox, firefox-esr y, por lo tanto, aparece en la lista de paquetes sugeridos asociados a *firefox* y *firefox-esr* .

Conflictos: el campo de conflictos

El campo Conflictos indica cuándo no se puede instalar un paquete simultáneamente con otro. los Las razones más comunes para esto son que ambos paquetes incluyen un archivo con el mismo nombre. mismo servicio en el mismo puerto de protocolo de control de transmisión (TCP), o podría obstaculizar el uno al otro operación.

Si desencadena un conflicto con un paquete ya instalado, dpkg se negará a instalar un paquete, excepto si el nuevo paquete especifica que reemplazará el paquete instalado, en cuyo caso dpkg elegirá reemplazar el paquete anterior por el nuevo. APT siempre sigue sus instrucciones: si Si elige instalar un nuevo paquete, se ofrecerá automáticamente para desinstalar el paquete que plantea un problema.

Incompatibilidades: el campo Breaks

El campo Breaks tiene un efecto similar al del campo Conflictos, pero con un significado especial. Eso señala que la instalación de un paquete romperá otro paquete (o versiones particulares del mismo). En general, esta incompatibilidad entre dos paquetes es transitoria y la relación Breaks se refiere específicamente a las versiones incompatibles.

Cuando un paquete rompe un paquete ya instalado, dpkg se negará a instalarlo y apt intentará para resolver el problema actualizando el paquete que se rompería a una versión más nueva (que se supone que es fijo y, por lo tanto, compatible de nuevo).

Este tipo de situación puede ocurrir en el caso de actualizaciones sin compatibilidad con versiones anteriores: esto es el caso si la nueva versión ya no funciona con la versión anterior y causa un mal funcionamiento en otro programa sin hacer provisiones especiales. El campo Saltos ayuda a prevenir estos tipos. de problemas

Elementos proporcionados: el campo Proporciona

Thisfieldintroducestheveryinterestingconceptofa *virtualpackage* . Ithasmanyroles, buttwoare De particular importancia. El primer rol consiste en usar un paquete virtual para asociar un genérico servicio con él (el paquete proporciona el servicio). El segundo indica que un paquete completamente reemplaza a otro y que para este propósito, también puede satisfacer las dependencias que el otro Lo satisfaría. Por lo tanto, es posible crear un paquete de sustitución sin tener que usar el mismo Nombre del paquete.

Metapaquete y virtual Paquete

Es esencial distinguir claramente los metapaquetes de los paquetes virtuales. El para-Mer son paquetes reales (incluidos archivos .deb reales), cuyo único propósito es expresar dependencias

Los paquetes virtuales, sin embargo, no existen físicamente; son solo un medio de identificación ing paquetes reales basados en criterios comunes y lógicos (por ejemplo, servicio prestado o compatibilidad con un programa estándar o un paquete preexistente).

Brindar un servicio Analicemos el primer caso con mayor detalle con un ejemplo: todo el correo Se dice que los servidores, como *Postfix* o *Sendmail* , proporcionan el paquete virtual de *agente de transporte de correo* . Por lo tanto, cualquier paquete que necesite este servicio para funcionar (por ejemplo, un administrador de listas de correo, como

lista inteligente o *sympa*) se limita a establecer en sus dependencias que requiere un *-transporte-agente de correo* en vez de especificar una lista grande pero incompleta de posibles soluciones. Además, es inútil instalar dos servidores de correo en la misma máquina, razón por la cual cada uno de estos paquetes declara un conflicto con el paquete virtual *mail-transport-agent* . Un conflicto entre un paquete y sí mismo es ignorado por el sistema, pero esta técnica prohibirá la instalación de dos servidores de correo uno al lado del otro.

Página 236

Intercambiabilidad con otro paquete El campo Proporciona también es interesante cuando el La carpa de un paquete se incluye en un paquete más grande. Por ejemplo, el módulo Perl *libdigest-md5-perl* era un módulo opcional en Perl 5.6, y se ha integrado como estándar en Perl 5.8. Como tal, el El paquete *perl* desde la versión 5.8 ha declarado Proporciona: libdigest-md5-perl para que las dependencias en este paquete se cumplen si el sistema tiene Perl 5.8 (o más reciente). El *paquete libdigest-md5-perl en* sí fue eliminado, ya que ya no tenía ningún propósito cuando se eliminaron las versiones antiguas de Perl.

Figura 8.3 *Uso de un campo Proporciona para no romper dependencias*

Esta característica es muy útil, ya que nunca es posible anticipar los caprichos del desarrollo. y es necesario poder ajustar el cambio de nombre y otro reemplazo automático de obsoletos software.

Reemplazar archivos: el campo Reemplaza

El campo Reemplazar indica que el paquete contiene archivos que también están presentes en otro paquete. edad, pero que el paquete tiene derecho legítimo a reemplazarlos. Sin esta especificación, dpkg falla, indicando que no puede sobrescribir los archivos de otro paquete (técnicamente, es posible forzarlo a hacerlo con la opción --force-overwrite, pero eso no se considera operación estándar). Esto permite la identificación de posibles problemas y requiere que el responsable del estudio estudie el asunto. antes de elegir si desea agregar dicho campo.

Página 237

El uso de este campo se justifica cuando cambian los nombres de los paquetes o cuando se incluye un paquete en otro. Esto también sucede cuando el responsable decide distribuir los archivos de manera diferente entre varios paquetes binarios producidos a partir del mismo paquete fuente de origen: son archivos colocados más largos al paquete anterior, pero solo al nuevo.

Si se han reemplazado todos los archivos en un paquete instalado, se considera que el paquete es re movido. Finalmente, este campo también alienta a dpkg a eliminar el paquete reemplazado donde hay un conflicto.

8.4.2. Scripts de configuración

Además del archivo de control , el archivo control.tar.gz para cada paquete Debian puede contener una serie de scripts (postinst , postrm , preinst , prerm) llamados por dpkg en diferentes etapas en el procesamiento de un paquete. Podemos usar dpkg -I para mostrar estos archivos ya que residen en un paquete .deb archivo:

```
$ dpkg -I /var/cache/apt/archives/zsh_5.3-1_amd64.deb | cabeza
 nuevo paquete debian, versión 2.0.
 tamaño 814486 bytes: archivo de control = 2557 bytes.
         838 bytes,    20 líneas      controlar
        3327 bytes,    43 líneas      md5sums
         969 bytes,    41 líneas   * postinst             #! / bin / sh
         348 bytes,    20 líneas   * postrm              #! / bin / sh
         175 bytes,     5 lineas   * preinst             #! / bin / sh
         175 bytes,     5 lineas   * prerm               #! / bin / sh
 Paquete: zsh
 Versión: 5.3-1
$ dpkg -I zsh_5.3-1_amd64.deb preinst
#! / bin / sh
conjunto -e
# Agregado automáticamente por dh_installdeb
dpkg-maintscript-helper symlink_to_dir / usr / share / doc / zsh zsh-common 5.0.7-3 - "$ @"
# Fin de la sección agregada automáticamente
```

La Política de Debian describe cada uno de estos archivos en detalle, especificando los scripts llamados y el argumento menciona que reciben. Thesesequencesmaybecomplicated, sinceifoneofthescriptsfails, dpkg voluntad intente volver a un estado satisfactorio cancelando la instalación o eliminación en curso (en la medida en que es posible).

La base de datos dpkg Puede recorrer la base de datos dpkg en el sistema de archivos en / var / lib / dpkg / . Este di-
La rectoría contiene un registro de todos los paquetes que se han instalado en el sistema. Todos los scripts de configuración para los paquetes instalados se almacenan en directorio / var / lib / dpkg / info / , en forma de archivo con el prefijo del paquete nombre:

```
$ ls /var/lib/dpkg/info/zsh.*
/var/lib/dpkg/info/zsh.list
/var/lib/dpkg/info/zsh.md5sums
/var/lib/dpkg/info/zsh.postinst
/var/lib/dpkg/info/zsh.postrm
/var/lib/dpkg/info/zsh.preinst
/var/lib/dpkg/info/zsh.prerm
```

Este directorio también incluye un archivo con la extensión .list para cada paquete, que contiene ing la lista de archivos que pertenecen a ese paquete:

```
$ head /var/lib/dpkg/info/zsh.list
/.
/compartimiento
/ bin / zsh
/ bin / zsh5
/ usr
/ usr / lib
/ usr / lib / x86_64-linux-gnu
/ usr / lib / x86_64-linux-gnu / zsh
/usr/lib/x86_64-linux-gnu/zsh/5.2
/usr/lib/x86_64-linux-gnu/zsh/5.2/zsh
[...]
```

El archivo / var / lib / dpkg / status contiene una serie de bloques de datos (en el formato de la famosa solicitud de comentarios de encabezados de correo, RFC 2822) que describe el estado de cada paquete La información del archivo de control de los paquetes instalados también es replicado allí.

```
$ more / var / lib / dpkg / status
Paquete: personajes de gnomo
Estado: instalar ok instalado
Prioridad: opcional
```

Sección: gnomo
Tamaño instalado: 1785
Mantenedor: Debian GNOME Maintainers <pkg-gnome-
maintenanceers@lists.alioth.debian.org >
Arquitectura: amd64
Versión: 3.20.1-1
[...]

Analicemos los archivos de configuración y veamos cómo interactúan. En general, el guión preinst es ejecutado antes de la instalación del paquete, mientras que el postinst lo sigue. Del mismo modo, prerm es invocado antes de la eliminación de un paquete y después de la fecha de nacimiento . Una actualización de un paquete es equivalente a la eliminación de la versión anterior e instalación de la nueva. No es posible describir en detalle todos los escenarios posibles aquí, pero discutiremos los dos más comunes: una instalación / up-fecha y una remoción.

Estas secuencias pueden ser bastante confusas, pero una representación visual puede ayudar. Manoj Srivastava hizo estos diagramas explicando cómo dpkg llama a los scripts de configuración . Dia similar los gramos también han sido desarrollados por el proyecto Debian Women; son un poco más simples de entender de pie, pero menos completo.

[2] https://people.debian.org/~srivasta/MaintainerScripts.html

[2] https://wiki.debian.org/MaintainerScripts

Precaución

Nombres simbólicos de la Guiones

Las secuencias descritas en esta sección llaman scripts de configuración por nombres específicos, como old-prerm o new-postinst . Son, respectivamente, la secuencia de comandos prerm con-incluido en la versión anterior del paquete (instalado antes de la actualización) y en el postinst script contenido en la nueva versión (instalada por la actualización).

Instalación y secuencia de secuencia de comandos de actualización

Esto es lo que sucede durante una instalación (o una actualización):

1. Para una actualización, dpkg llama a la *versión* anterior de actualización anterior .
2. Aún para una actualización, dpkg ejecuta entonces nueva preinst actualización de *la vieja versión* ; por primera vez instalación, ejecuta la instalación new-preinst . Puede agregar la versión anterior en el último parámetro el paquete ya está instalado y eliminado (pero no purgado, la configuración archivos retenidos).
3. Los nuevos archivos del paquete se desempaquetan. Si ya existe un archivo, se reemplaza, pero una copia de seguridad Se realiza una copia y se almacena temporalmente.
4. Para una actualización, dpkg ejecuta una *nueva versión de la* actualización de postrm *antigua* .
5. dpkg actualiza todos los datos internos (lista de archivos, scripts de configuración, etc.) y elimina el copias de seguridad de los archivos reemplazados. Este es el punto sin retorno: dpkg ya no tiene acceso a todos de los elementos necesarios para volver al estado anterior.
6. dpkg actualizará los archivos de configuración, solicitándole que decida si no puede automatizar ically gestionar esta tarea. Los detalles de este procedimiento se discuten en la sección 8.4.3 , " Verificar-sumas, Conffiles"[Página 214].
7. Finalmente, dpkg configura el paquete ejecutando new-postinst configure *last-Versión-configurado* .

Retiro de paquete

Esto es lo que sucede durante la eliminación de un paquete.

1. dpkg llama a prerm remove .
2. dpkg elimina todos los archivos del paquete, con la excepción de los archivos de configuración y guiones de configuración.

3. dpkg ejecuta la eliminación postrm . Todos los scripts de configuración, excepto postrm , se eliminan.
   Si no ha utilizado la opción de purga, el proceso se detiene aquí.
4. Para una purga completa del paquete (comando emitido con dpkg --purge o dpkg -P),
   los archivos de configuración también se eliminan, así como una cierta cantidad de copias (* .dpkg-tmp ,
   * .dpkg-old , * .dpkg-new) y archivos temporales; dpkg luego ejecuta la purga postrm .

En algunos casos, un paquete puede usar debconf para requerirle información de configuración:
cuatro scripts detallados anteriormente se complementan con un script de configuración diseñado para adquirir esa información
formación. Durante la instalación, este script define en detalle qué preguntas hará debconf . los
Las respuestas se registran en la base de datos de debconf para referencia futura. El guión es generalmente exe-
preparado por apt antes de instalar los paquetes uno por uno para agrupar todas las preguntas en
El comienzo del proceso. Los scripts previos y posteriores a la instalación pueden usar esta información
para operar de acuerdo a sus deseos.

La herramienta debconf La herramienta debconf se creó para resolver un problema recurrente en Debian. Todo Debian los paquetes no pueden funcionar sin un mínimo de configuración utilizada para hacer preguntas funciones con llamadas a los comandos echo y read en scripts de shell postinst (y otros guiones similares). Esto obligó al instalador a cuidar grandes instalaciones o actualizaciones en para responder a varias consultas de configuración a medida que surgían. Estos manuales inter- ahora se han prescindido casi por completo de las acciones, gracias a debconf .

La herramienta debconf tiene muchas características interesantes: requiere que el desarrollador especifique la interacción del usuario; Permite la localización de todas las cadenas mostradas (todas las traducciones son almacenado en el archivo de plantillas que describe las interacciones); proporciona diferentes frentes tiende a preguntas (modo texto, modo gráfico, no interactivo); y permite crear ación de una base de datos central de respuestas para compartir la misma configuración con varios ordenadores. La característica más importante es que todas las preguntas se pueden presentar en una fila, todo a la vez, antes de comenzar una larga instalación o proceso de actualización. Ahora usted puede seguir con su negocio mientras el sistema maneja la instalación por sí solo, sin tener que permanecer allí mirando la pantalla, esperando que surjan preguntas.

8.4.3. Sumas de control, Conffiles

Además de las secuencias de comandos del mantenedor y los datos de control ya mencionados en las secciones anteriores,
El archivo control.tar.gz de un paquete Debian puede contener otros archivos interesantes:

```
# ar p /var/cache/apt/archives/bash_4.4-2_amd64.deb control.tar.gz | tar -tzf -
```



```
./
./conffiles
./controlar
./md5sums
./postinst
./postrm
./preinst
./prerm
```

El primero, md5sums, contiene las sumas de comprobación MD5 para todos los archivos del paquete. Su principal ventaja
es que permite que dpkg --verify verifique si estos archivos se han modificado desde su instalación.
Tenga en cuenta que cuando este archivo no existe, dpkg lo generará dinámicamente en el momento de la instalación (y
guárdelo en la base de datos dpkg al igual que otros archivos de control).

conffiles enumera los archivos de paquete que deben manejarse como archivos de configuración. Los archivos de configuración pueden ser modificado por el administrador, y dpkg intentará preservar esos cambios durante un paquete actualizar.

En efecto, en esta situación, dpkg se comporta de la manera más inteligente posible: si la configuración estándar
el archivo no ha cambiado entre las dos versiones, no hace nada. Sin embargo, si el archivo ha cambiado,
intentará actualizar este archivo. Son posibles dos casos: o el administrador no ha tocado esto
archivo de configuración, en cuyo caso dpkg instala automáticamente la nueva versión; o el archivo ha sido
modificado, en cuyo caso dpkg le pregunta al administrador qué versión desea usar (la anterior
con modificaciones, o la nueva provista con el paquete). Para ayudar a tomar esta decisión,
dpkg ofrece mostrar una diferencia que muestra la diferencia entre las dos versiones. Si eliges
retener la versión anterior, la nueva será almacenada en la misma ubicación en el archivo con el .dpkg-dist
sufijo. Si elige la nueva versión, la anterior se conserva en un archivo con el sufijo .dpkg-old .
Otra acción disponible consiste en interrumpir momentáneamente dpkg para editar el archivo e intentar
restablecer las modificaciones relevantes (previamente identificadas con diff).

dpkg maneja las actualizaciones del archivo de configuración, pero, mientras lo hace, interrumpe regularmente su trabajo para preguntar para aportes del administrador. Esto puede llevar mucho tiempo e inconveniente. Por suerte,

Puede indicar a dpkg que responda a estas indicaciones automáticamente. La opción --force-confold conserva la versión anterior del archivo, mientras que --force-confnew usará la nueva versión. Estas opciones son respetados, incluso si el archivo no ha sido cambiado por el administrador, que solo rara vez tiene efecto deseado. Agregar la opción --force-confdef dice dpkg para decidir por sí mismo cuando sea posible (en en otras palabras, cuando el archivo de configuración original no ha sido tocado), y solo usa --force-confnew o --force-confold para otros casos.

Estas opciones se aplican a dpkg , pero la mayoría de las veces el administrador trabajará directamente con programas de aptitud o aptos . Por lo tanto, es necesario conocer la sintaxis utilizada para indicar las opciones. pasar al comando dpkg (sus interfaces de línea de comandos son muy similares).

```
# apt -o DPkg :: options :: = ”- force-confdef” -o DPkg :: options :: = ”- force-confold” full-
  actualizar
```


Estas opciones se pueden almacenar directamente en la configuración de apt . Para hacerlo, simplemente escriba lo siguiente línea en el archivo /etc/apt/apt.conf.d/local :

```
DPkg :: options {”--force-confdef”; "--Force-confold"; }
```

La inclusión de esta opción en el archivo de configuración significa que también se utilizará en una interfaz gráfica. cara como la aptitud .

Por el contrario, también puede forzar a dpkg a hacer preguntas sobre el archivo de configuración. El --force-confask La opción indica a dpkg que muestre las preguntas sobre los archivos de configuración, incluso en los casos en que normalmente no serían necesarios. Por lo tanto, al reinstalar un paquete con esta opción, dpkg hará las preguntas nuevamente para todos los archivos de configuración modificados por el administrador. Esto es muy conveniente, especialmente para reinstalar el archivo de configuración original si se ha eliminado y no hay otra copia disponible: una reinstalación normal no funcionará, porque dpkg considera la eliminación como una forma de modificación legítima y, por lo tanto, no instala el archivo de configuración deseado.

8.5. Resumen

En esta sección, aprendimos más sobre el sistema de paquetes Debian, discutimos el paquete avanzado age Tool (APT) y dpkg , aprendieron sobre la interacción básica del paquete, configuración avanzada de APT y uso, y profundizó en el sistema de paquetes de Debian con una breve referencia del archivo .deb formato. Observamos el archivo de control , los scripts de configuración, las sumas de verificación y el archivo de conffiles .

Consejos resumidos:

Un paquete Debian es un archivo comprimido de una aplicación de software. Contiene la aplicación archivos, así como otros metadatos, incluidos los nombres de las dependencias que necesita la aplicación así como scripts que permiten la ejecución de comandos en diferentes etapas de la vida del paquete. ciclo (instalación, eliminación, actualizaciones).

La herramienta dpkg , a diferencia de apt y apt-get (de la familia APT), no tiene conocimiento de toda la disponibilidad. paquetes capaces que podrían usarse para cumplir con las dependencias de paquetes. Por lo tanto, para gestionar el paquete Debian edades, es probable que utilice las herramientas para que puedan resolver automáticamente problemas de dependencia.

Puede usar APT para instalar y eliminar aplicaciones, actualizar paquetes e incluso actualizar su sistema entero. Estos son los puntos clave que debe conocer sobre APT y su configuración:

- El archivo sources.list es el archivo de configuración clave para definir las fuentes del paquete (o repositorio). tories que contienen paquetes).
- Debiana y Kali utilizan las tres secciones para diferenciar el paquete según el sentido de la sonda. por los autores de cada trabajo: main contiene todos los paquetes que cumplen totalmente con Debian Pautas de software libre [6] ; no libre contiene software que no se ajusta (enteramente) a las Directrices de software libre pero, sin embargo, pueden distribuirse sin restricciones; y

[6] https://www.debian.org/social_contract#guidelines

contrib (contribuciones) incluye software de código abierto que no puede funcionar sin algunos elementos no libres

- Kali mantiene varios repositorios que incluyen: kali-rolling, que es el repositorio principal para los usuarios finales y los usuarios siempre deben contener paquetes instalables y recientes; kali-dev, que usó por los desarrolladores de Kali y no es para uso público; y kali-sangrado-borde, que a menudo contiene paquetes no comprobados y examinados automáticamente construidos de forma automática (o Subversion) repositorio menos de veinticuatro horas después de haber sido comprometidos.
- Cuando trabaje con APT, primero debe descargar la lista de paquetes disponibles actualmente con actualización apta .
- Puede agregar un paquete al sistema con un simple *paquete de* instalación de apt . APT se auto-Instale matemáticamente las dependencias necesarias.
- Para eliminar un paquete, use apt remove *package* . También eliminará la dependencia inversa cies del paquete (es decir, paquetes que dependen del paquete que se va a eliminar).
- Para eliminar todos los datos asociados con un paquete, puede "purgar" el paquete con el apt comando de *paquete de* purga . A diferencia de una eliminación, esto no solo eliminará el paquete sino que también sus archivos de configuración y, a veces, los datos de usuario asociados.

Recomendamos actualizaciones periódicas para instalar las últimas actualizaciones de seguridad. Para actualizar, use apt actualización seguida de apt upgrade , apt-get upgrade o aptitude safe-upgrade . Estas
Los comandos buscan paquetes instalados que se pueden actualizar sin eliminar ningún paquete.

Para actualizaciones más importantes, como las actualizaciones de versiones principales, use apt full-upgrade . Con este instrucción, apt completará la actualización incluso si tiene que eliminar algunos paquetes obsoletos o Instalar nuevas dependencias. Este es también el comando que debe usar para actualizaciones regulares de Su sistema Kali Rolling. Revise los pros y los contras de las actualizaciones que describimos en este capítulo.

Se pueden usar varias herramientas para inspeccionar los paquetes de Debian:

- dpkg --listfiles *package* (o -L) enumera los archivos que fueron instalados por el paquete especificado.
- dpkg: el *archivo de* búsqueda (o -S) encuentra los paquetes que contienen el archivo o la ruta que se pasa en argumento.
- dpkg --list (o -l) muestra la lista de paquetes conocidos por el sistema y su instalación estado.
- dpkg --contents *file.deb* (o -c) enumera todos los archivos en un archivo .deb en particular .
- dpkg --info *file.deb* (o -I) muestra los encabezados del archivo .deb especificado .
- Los diversos subcomandos apt-cache muestran gran parte de la información almacenada en base de datos ternal.

Para evitar el uso excesivo del disco, debe ordenar regularmente / var / cache / apt / archives / .
Se pueden utilizar dos comandos para esto: apt clean (o apt-get clean) vacía completamente la dirección

conservador; apt autoclean (apt-get autoclean) solo elimina los paquetes que ya no se pueden desactivar cargado porque han desaparecido del espejo y por lo tanto son inútiles.

Aptitude es un programa interactivo que se puede usar en modo semi-gráfico en la consola. Está Un programa extremadamente robusto que puede ayudarlo a instalar y solucionar problemas de paquetes.

synaptic es un administrador de paquetes gráficos que presenta una interfaz gráfica limpia y eficiente.

Como usuario avanzado, puede crear archivos en /etc/apt/apt.conf.d/ para configurar ciertos aspectos de APT. También puede administrar prioridades de paquetes, rastrear paquetes instalados automáticamente, trabajar con varias distribuciones o arquitecturas a la vez, use firmas criptográficas para validar paquetes, y actualice archivos utilizando las técnicas descritas en este capítulo.

A pesar de los mejores esfuerzos de los mantenedores de Kali / Debian, una actualización del sistema no siempre es tan fácil como Esperamos Cuando esto sucede, puedes mirar el rastreador de errores de Kali[7] y en el error de Debian sistema de seguimiento [8] en https://bugs.debian.org/ *paquete* para verificar si el problema ya ha sido reportado También puede intentar degradar el paquete o depurar y reparar un paquete fallido secuencia de comandos mantenedor.

[7] [7] http://bugs.kali.org
[8] https://bugs.debian.org

Palabras clave

Paquetes personalizados
Kernel personalizado
Imágenes personalizadas
construcción en vivo
Persistencia

Capítulo

9 Uso avanzado

Contenido

Modificación de paquetes de Kali 222
Recompilación del kernel de Linux 233
Creación de imágenes ISO de Kali Live personalizadas 237
Agregar persistencia al ISO en vivo con una llave USB 240
Resumen 246

Kali se ha creado como un marco de prueba de penetración altamente modular y personalizable y también mínimos para una personalización y uso bastante avanzados. Las personalizaciones pueden suceder en múltiples niveles, comenzando en el nivel del código fuente. Las fuentes de todos los paquetes de Kali están disponibles públicamente. En este capítulo, le mostraremos cómo puede recuperar paquetes, modificarlos y crear su propio paquete. paquetes personalizados fuera de ellos. El kernel de Linux es algo así como un caso especial y, como tal, es cubierto en una sección dedicada (sección 9.2 , " Recompilando el kernel de Linux "[página 233]), donde discutirá dónde encontrar fuentes, cómo configurar la compilación del núcleo y, finalmente, cómo compilar y cómo construir los paquetes de kernel asociados.

El segundo nivel de personalización está en el proceso de creación de imágenes ISO en vivo. Mostraremos como la herramienta live-build ofrece muchos ganchos y opciones de configuración para personalizar el resultado Imagen ISO, incluida la posibilidad de usar paquetes personalizados de Debian en lugar de los paquetes disponibles capaz en espejos.

También discutiremos cómo puede crear un ISO en vivo persistente integrado en una llave USB que preservará archivos y cambios en el sistema operativo entre reinicios.

9.1. Modificación de paquetes de Kali

La modificación de los paquetes de Kali suele ser una tarea para los contribuyentes y desarrolladores de Kali: actualizan los paquetes envejece con nuevas versiones ascendentes, ajustan la configuración predeterminada para una mejor integración en la distribución, o corrigen errores reportados por los usuarios. Pero es posible que tenga necesidades específicas no satisfechas

por los paquetes oficiales y saber cómo construir un paquete modificado puede ser muy valioso.

Quizás se pregunte por qué necesita molestarse con el paquete. Después de todo, si tiene que modificar una pieza de software, siempre puede tomar su código fuente (generalmente con `git`) y ejecutar el modificado versión directamente desde la salida de origen. Esto está bien cuando es posible y cuando usa su el directorio principal para este propósito, pero su solicitud requiere una configuración de todo el sistema (por ejemplo, con un paso de `instalación`) luego contaminará su sistema de archivos con archivos desconocidos en `dpkg` y pronto creará problemas que las dependencias de paquetes no pueden detectar. Además, con la debida paquetes podrá compartir sus cambios y desplegarlos en múltiples computadoras mucho más fácilmente o revierta los cambios después de haber descubierto que no funcionaban tan bien como esperabas

Entonces, ¿cuándo quieres modificar un paquete? Echemos un vistazo a algunos ejemplos. Primero nosotros asumirá que usted es un gran usuario de SET y notó una nueva versión anterior pero el Los desarrolladores de Kali están todos ocupados en una conferencia y quieres probarla de inmediato. Usted quiere para actualizar el paquete usted mismo. En otro caso, asumiremos que está luchando para obtener su tarjeta MIFARE NFC funciona y desea reconstruir "libfreefare" para habilitar los mensajes de depuración para tener datos procesables para proporcionar en un informe de error que está preparando actualmente. en un En el último caso, asumiremos que el programa "pyrit" falla con un mensaje de error críptico. Después de una web buscar, encuentra una confirmación que espera solucionar su problema en el repositorio GitHub ascendente y desea reconstruir el paquete con esta corrección aplicada.

Revisaremos todas esas muestras en las siguientes secciones. Intentaremos generalizar la explicación. naciones para que pueda aplicar mejor las instrucciones a otros casos, pero es imposible cubrir todas las situaciones que puedas encontrar. Si tiene problemas, aplique su mejor criterio para encontrar un solución o busque ayuda en los foros más apropiados (vea el capítulo 6, "Ayudándote a ti mismo y Obteniendo ayuda"[Página 124]).

Independientemente del cambio que desee realizar, el proceso general es siempre el mismo: tome el paquete fuente. edad, extráigala, realice los cambios y luego cree el paquete. Pero para cada paso, a menudo hay Múltiples herramientas que pueden manejar la tarea. Elegimos las herramientas más relevantes y populares, pero Nuestra revisión no es exhaustiva.

9.1.1. Obteniendo las fuentes

La reconstrucción de un paquete Kali comienza con la obtención de su código fuente. Un paquete fuente está compuesto de múltiples archivos: el archivo principal es el archivo `*.dsc` (*Control de código fuente de Debian*), ya que enumera los otros acompañamientos. archivos nying, que pueden ser `*.tar.gz, bz2, xz`, a veces `*.diff.gz` o `*.debian.tar.gz, bz2, xz` archivos.

Los paquetes fuente se almacenan en los espejos Kali que están disponibles a través de HTTP. Podrías usar tu navegador web para descargar todos los archivos necesarios, pero la forma más fácil de lograr esto es usar el comando `apt source source_package_name`. Este comando requiere una línea deb-src en el archivo `/etc/apt/sources.list` y archivos de índice actualizados (logrado ejecutando `apt update`). De manera predeterminada, Kali no agrega la línea requerida, ya que pocos usuarios de Kali realmente necesitan recuperar la fuente paquetes, pero puede agregarlos fácilmente (consulte el archivo de muestra en la sección 8.1.3, "Repositorios Kali"[página 173] y las explicaciones asociadas en la sección 8.1.2, "Comprender el archivo sources.list"[página 172]).

```
$ apt source libfreefare
Leyendo listas de paquetes ... Hecho
AVISO: el paquete 'libfreefare' se mantiene en el sistema de control de versiones 'Git' en:
git: //anonscm.debian.org/collab-maint/libnfc.git
Por favor use:
git clone git: //anonscm.debian.org/collab-maint/libnfc.git
para recuperar las últimas actualizaciones (posiblemente inéditas) del paquete.
Necesita obtener 119 kB de archivos fuente.
Obtenga: 1 http://archive-2.kali.org/kali kali-rolling / main libfreefare 0.4.0-2 (dsc) [2,090 B]
Obtenga: 2 http://archive-2.kali.org/kali kali-rolling / main libfreefare 0.4.0-2 (tar) [113 kB]
Obtenga: 3 http://archive-2.kali.org/kali kali-rolling / main libfreefare 0.4.0-2 (diff) [3,640 B]
Obtenido 119 kB en 1s (63.4 kB / s)
gpgv: recurso de bloqueo de teclas '/home/rhertzog/.gnupg/trustedkeys.gpg': error de archivo abierto
gpgv: Firma realizada el martes 04 mar 2014 06:57:36 PM EST utilizando la clave RSA ID 40AD1FA6
gpgv: No se puede verificar la firma: clave pública no encontrada
dpkg-source: advertencia: no se pudo verificar la firma en ./libfreefare_0.4.0-2.dsc
dpkg-source: info: extracción de libfreefare en libfreefare-0.4.0
dpkg-source: info: desempacando libfreefare_0.4.0.orig.tar.gz
dpkg-source: info: desempacando libfreefare_0.4.0-2.debian.tar.xz
$ cd libfreefare-0.4.0
$ ls
Autores          CMakeLists.txt  PROCESO DE COMPARTIR  m4          LÉAME
ChangeLog        configure.ac    debian                libfreefare  Makefile.am  prueba
```

```
cmake                contrib                    ejemplos      libfreefare.pc.in          NOTICIAS          QUE HACER
$ ls debian
registro de cambios  derechos de autor                        libfreefare-dev.install                reglas
compat               libfreefare0.install                     libfreefare-doc.install                fuente
controlar            libfreefare-bin.install                  README.Source                          reloj
```

En este ejemplo, mientras recibimos el paquete fuente de un espejo Kali, el paquete es el igual que en Debian ya que la cadena de versión no contiene "kali". Esto significa que no hay kali-específico Se han aplicado cambios.

Si necesita una versión específica del paquete fuente, que actualmente no está disponible en los repositorios historias enumeradas en /etc/apt/sources.list , entonces la forma más fácil de descargarlo es averiguar el URL de su archivo .dsc buscándolo en http://pkg.kali.org y luego entregándolo a dget (del paquete *devscripts*).

Después de haber buscado la URL del paquete fuente libreefare disponible en kali-bleeding-edge, puedes descargarlo con dget . Primero descargará el archivo .dsc , luego lo analizará para saber qué se hace referencia a otros archivos y luego los descarga de la misma ubicación:

```
$ dget http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~
    ¯ git1439352548.ffde4d-1.dsc
dget: recuperando http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~
    ¯ git1439352548.ffde4d-1.dsc
  % Total    % Recibido% Xferd Velocidad media                    Hora         Hora         Tiempo actual
                                 Cargar carga                     Total        Gastado      Velocidad izquierda
100   364 100   364    0 0     0 0    852      0 -:-:- -:-:- -:-:-                                  854
100 1935 100 1935              0 0     0 0   2650      0 -:-:- -:-:- -:-:- 19948
dget: recuperando http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~
    ¯ git1439352548.ffde4d.orig.tar.gz
[...]
dget: recuperando http://http.kali.org/pool/main/libf/libfreefare/libfreefare_0.4.0+0~
    ¯ git1439352548.ffde4d-1.debian.tar.xz
[...]
libfreefare_0.4.0 + 0 ~ git1439352548.ffde4d-1.dsc:
dscverify: libfreefare_0.4.0 + 0 ~ git1439352548.ffde4d-1.dsc falló la verificación de firma:
gpg: Firma realizada el miércoles 12 de agosto 06:14:03 CEST 2015
gpg:                utilizando la clave RSA 43EF73F4BD8096DA
gpg: No se puede verificar la firma: Sin clave pública
¡¡Validación fallida!!
$ dpkg-source -x libfreefare_0.4.0 + 0 ~ git1439352548.ffde4d-1.dsc
gpgv: Firma realizada el miércoles 12 de agosto 06:14:03 CEST 2015
gpgv:                utilizando la clave RSA 43EF73F4BD8096DA
gpgv: No se puede verificar la firma: Sin clave pública
dpkg-source: advertencia: no se pudo verificar la firma en ./libfreefare_0.4.0+0~git1439352548
    ¯ .ffde4d-1.dsc
dpkg-source: info: extracción de libfreefare en libfreefare-0.4.0 + 0 ~ git1439352548.ffde4d
dpkg-source: info: desempacando libfreefare_0.4.0 + 0 ~ git1439352548.ffde4d.orig.tar.gz
dpkg-source: info: desempacando libfreefare_0.4.0 + 0 ~ git1439352548.ffde4d-1.debian.tar.xz
```


Vale la pena señalar que dget no extrajo automáticamente el paquete fuente porque podría no verifique la firma PGP en el paquete fuente. Así hicimos ese paso manualmente con dpkg-fuente -x *dsc-file* . También puede forzar la extracción del paquete fuente pasando el --allow-opción no autenticada o -u. Inversamente, puede usar --download-only para omitir el paquete fuente Paso de extracción.

Recuperando fuentes de Git

Es posible que haya notado que la invocación de origen de apt le informa sobre un posible Git repositorio utilizado para mantener el paquete. Puede apuntar a un repositorio Debian Git o a un repositorio Kali Git.

Todos los paquetes específicos de Kali se mantienen en repositorios de Git alojados en gitlab.com/-kalilinux / paquetes , . Puede recuperar las fuentes de esos repositorios con git clon https://gitlab.com/kalilinux/packages/ *source-package* .git .

Al contrario de lo que obtienes con apt source , el árbol obtenido no tendrá parches aplicado automáticamente Eche un vistazo a debian / parches / para conocer las posibles cambios realizados por Kali.

```
$ git clone https://gitlab.com/kalilinux/packages/kali-meta.
    ¯ git
```

```
Clonación en 'kali-meta' ...
remoto: Contando objetos: 760, hecho.
remoto: Comprimir objetos: 100% (614/614), hecho.
remoto: Total 760 (delta 279), reutilizado 0 (delta 0)
Recepción de objetos: 100% (760/760), 141.01 KiB |  0 bytes / s,
¯ hecho.
Deltas de resolución: 100% (279/279), hecho.
Comprobando la conectividad ... hecho.
$ cd kali-meta
$ ls
debian
$ ls debian
fuente de reglas de copyright control de compatibilidad de registro
```

Puede usar los repositorios git como otra forma de recuperar las fuentes y, por lo tanto, (principalmente) siga las otras instrucciones de esta sección. Pero cuando los desarrolladores de Kali trabajan con esos repositorios, usan otro flujo de trabajo de empaque y usan herramientas del paquete *git-buildpackage* que no cubriremos aquí. Puedes aprender más sobre esas herramientas aquí:

[2] https://honk.sigxcpu.org/piki/projects/git-buildpackage/

[1] https://gitlab.com/kalilinux/packages

9.1.2. Instalación de dependencias de compilación

Ahora que tiene las fuentes, aún necesita instalar dependencias de compilación. Serán necesarios para compilar los paquetes binarios deseados, pero también es probable que sean necesarios para compilaciones parciales que podría desea ejecutar para probar los cambios mientras los realiza.

Cada paquete fuente declara sus dependencias de compilación en el campo Build-Depends del debian / archivo de control Vamos a instruir apta para instalar los (suponiendo que esté en un directorio que contiene un paquete fuente desempaquetado):

```
$ sudo apt build-dep ./
Nota, usando el directorio './' para obtener las dependencias de compilación
Leyendo listas de paquetes ... Hecho
Construyendo árbol de dependencia
Leyendo información del estado ... Hecho
Se instalarán los siguientes paquetes NUEVOS:
    autoconf automake autopoint autotools-dev debhelper dh-autoreconf
    dh-strip-non determinismism gettext intltool-debian libarchive-zip-perl
    libfile-stripnondeterminism-perl libtool po-debconf
0 actualizado, 13 recién instalados, 0 para eliminar y 0 no actualizado.
Necesito obtener 4 456 kB de archivos.
Después de esta operación, se utilizarán 14,6 MB de espacio en disco adicional.
¿Quieres continuar? [S / n]
[...]
```

En este ejemplo, todas las dependencias de compilación pueden satisfacerse con los paquetes disponibles para APT. Esto podría no siempre es así, ya que la herramienta de construcción kali-rolling no garantiza la instalabilidad del diseño de construcción pendencias (solo se tienen en cuenta las dependencias de paquetes binarios). En la práctica, binario.
Las dependencias y las dependencias de compilación a menudo están estrechamente relacionadas y la mayoría de los paquetes tendrán Construir dependencias satisfactorias.

9.1.3. Haciendo cambios

No podemos abarcar todos los posibles cambios que desee realizar en un paquete dado en este sección. Esto equivaldría a enseñarte todo lo esencial[2] detalles del embalaje de Debian. Cómo-Sin embargo, cubriremos los tres casos de uso común presentados anteriormente y explicaremos algunos de los partes inevitables (como mantener el archivo de registro de cambios).

Lo primero que debe hacer es cambiar el número de versión del paquete para que los paquetes reconstruidos puedan ser distinguido de los paquetes originales proporcionados por Kali o Debian. Para lograr esto, generalmente agregue un sufijo que identifique a la entidad (persona o empresa) que aplica los cambios. Desde buxy es mi Apodo IRC, lo usaré como sufijo. Tal cambio se efectúa mejor con el comando dch (*Debian CHangelog*) del paquete *devscripts* , con un comando como dch --local buxy . Esto invoca

[2] https://www.debian.org/doc/manuals/maint-guide/

un editor de texto (sensible-editor , que ejecuta el editor asignado en el entorno VISUAL o EDITOR-
variables de ment, o / usr / bin / editor de lo contrario), que le permite documentar las diferencias
introducido por esta reconstrucción. Este editor muestra que dch realmente cambió el debian / changelog
archivo:

```
$ head -n 1 debian / changelog
libfreefare (0.4.0-2) inestable; urgencia = baja
$ dch - buxy local
[...]
$ head debian / changelog
libfreefare (0.4.0-2buxy1) SIN LANZAMIENTO; urgencia = medio

  * Habilitar la opción de configuración --with-debug.

 - Raphael Hertzog <buxy@kali.org> Vie, 22 de abril de 2016 10:36:00 -0400

libfreefare (0.4.0-2) inestable; urgencia = baja

  * Actualización de debian / copytight.
    Corregir licencia para LGPL3 +.
```

Si realiza dichos cambios regularmente, es posible que desee establecer DEBFULLNAME y DEBEMAIL en-
variables de entorno a su nombre completo y su correo electrónico, respectivamente. Sus valores serán utilizados
por muchas herramientas de embalaje, incluido dch , que las incrustará en la línea de remolque que se muestra arriba
(empezando con " -- ").

Aplicando un parche

En uno de *nuestros* casos de uso, hemos *descargado el* paquete *fuente de* pirita y queremos *aplicar un* parche
que encontramos en el repositorio git ascendente. Esta es una operación común y siempre debe ser
simple. Desafortunadamente, los parches se pueden manejar de manera diferente dependiendo del paquete fuente
formato y en el flujo de trabajo de empaquetado de Git en uso (cuando se usa Git para mantener el paquete).

Con un paquete fuente desempaquetado Has ejecutado apt source pyrit y tienes un pyrit-0.
4.0 directorio. Puede aplicar su parche directamente con patch -p1 < *patch-file* :

```
$ apt source pyrit
[...]
$ cd pyrit-0.4.0
$ wget https://github.com/JPaulMora/Pyrit/commit/14
      ec997174b8e8fd20d22b6a97c57e19633f12a0.patch -O / tmp / pyrit-patch
[...]
$ patch -p1 </ tmp / pyrit-patch
parchear el archivo cpyrit / pckttools.py
```



```
Hunk # 1 tuvo éxito en 53 (desplazamiento de -1 líneas).
$ dch - local buxy "Aplicar parche para trabajar con scapy 2.3"
```

En este punto, ha parcheado manualmente el código fuente y ya puede construir un paquete binario.
edades de su versión modificada (consulte la sección 9.1.4 , " Inicio de la compilación "[página 231]). Pero si tu
intente construir un paquete fuente actualizado, fallará, quejándose de "flujo inesperado
cambios ". Esto se debe a que pyrit (como la mayoría de los paquetes fuente) usa el formato fuente (ver
debian / source / format file) conocido como 3.0 (quilt), donde los cambios en el código ascendente deben ser
grabados en parches separados almacenados en debian / parches / y en donde debian / parches / series
El archivo indica el orden en que se deben aplicar los parches. Puede registrar sus cambios en un nuevo
parche ejecutando dpkg-source --commit :

```
$ dpkg-source --commitir
dpkg-source: info: cambios locales detectados, los archivos modificados son:
  pyrit-0.4.0 / cpyrit / pckttools.py
```

Ingrese el nombre del parche deseado: **fix-for-scapy-2.3.patch**
dpkg-source: info: se han registrado cambios locales en un nuevo parche: pyrit-0.4.0 / debian /
parches / fix-for-scapy-2.3.patch

$ **tail -n 1 debian / parches / series**
fix-for-scapy-2.3.patch

Serie de parches de edredones Esta convención de administración de parches ha sido popularizada por una herramienta llamada edredón y el formato del paquete fuente "3.0 (edredón)" es, por lo tanto, compatible con esta herramienta, con la pequeña desviación que usa debian / parches en lugar de parches . Esta herramienta es disponible en el paquete del mismo nombre y puede encontrar un buen tutorial aquí:

[2] https://raphaelhertzog.com/2012/08/08/

cómo-usar-quilt-to-manage-patches-in-debian-packages /

Si el paquete fuente usa el formato fuente 1.0 o 3.0 (nativo), entonces no hay ningún requisito para registrar nuestro cambio de corriente en el parche. Estas áreas se agrupan automáticamente en la fuente de resultados paquete.

Con un repositorio de Git Si ha utilizado Git para recuperar el paquete fuente, la situación es incluso más complicado. Hay múltiples flujos de trabajo de Git y herramientas asociadas, y obviamente no todos Los paquetes Debian están utilizando los mismos flujos de trabajo y herramientas. La distinción ya explicada sobre el formato de origen sigue siendo relevante, pero también debe verificar si los parches se aplican previamente en árbol fuente o cuando están almacenados solo en Debian / parches (en este caso, se aplican en tiempo de construcción).

La herramienta más popular es *git-buildpackage* . Es lo que usamos para administrar todos los repositorios en git-lab.com/kalilinux/packages. Cuando lo usa, los parches no se aplican previamente en el árbol de origen, sino se almacenan en debian / parches . Puede agregar parches manualmente en ese directorio y enumerarlos

---

en debian / parches / series pero los usuarios de git-buildpackage tienden a usar gbp pq para editar todo serie de parches como una rama única que puede ampliar o modificar a su gusto. Verifique gbp-pq (1) para aprende a invocarlo.

git-dpm (con el comando asociado del mismo nombre) es otra herramienta de empaquetado de git que puede encontrar en uso. Registra metadatos en debian / .git-dpm y mantiene los parches aplicados en el árbol fuente fusionando una rama constantemente modificada que se construye a partir del contenido de debian / parches .

Ajustar las opciones de compilación

Por lo general, debe ajustar las opciones de compilación cuando desea habilitar una característica o comportamiento opcional que no está activado en el paquete oficial o cuando desea personalizar los parámetros que son establecido en tiempo de compilación a través de una opción ./configure o mediante variables establecidas en el entorno de compilación.

En esos casos, los cambios generalmente se limitan a debian / rules , que impulsa los pasos en El proceso de compilación del paquete. En los casos más simples, las líneas relativas a la configuración inicial (./configure ...) o la compilación real ($ (MAKE) ... o make ...) son fáciles de detectar. Si estos comandos no se llaman explícitamente, probablemente son un efecto secundario de otro comando explícito, en el que caso, consulte su documentación para obtener más información sobre cómo cambiar el comportamiento predeterminado ior. Con los paquetes que usan dh , es posible que deba agregar una anulación para dh_auto_configure o Comandos dh_auto_build (consulte sus páginas manuales respectivas antes de la explicación sobre cómo lograrlo) esta).

Para hacer esas explicaciones más concretas, apliquémoslas a nuestro caso de uso de muestra. Tú decidiste para modificar libfreefare para pasar la opción --enable-debug al script ./configure para que pueda podría obtener un resultado más detallado de sus herramientas de comunicación de campo cercano (NFC) y presentar una mejor informe de error sobre su tarjeta Mifare NFC no reconocida. Dado que el paquete usa dh para conducir el proceso de compilación, agrega (o en este caso modifica) el objetivo override_dh_auto_configure. Aquí está el extracto correspondiente del archivo debian / rules de libfreefare :

```
override_dh_auto_configure:
        dh_auto_configure - --with-cutter --disable-silent-rules --enable-debug
```

Empaquetando una Nueva Versión Upstream

Echemos un vistazo a un ejemplo en este punto, mientras discutimos el empaquetado de versiones anteriores. Digamos usted es un usuario avanzado de SET y notó una nueva versión ascendente (7.4.5) que aún no está disponible en Kali (que solo tiene la versión 7.4.4). Desea compilar un paquete actualizado e intentar salir. Esto es un versión menor y, por lo tanto, no espera que la actualización requiera ningún cambio en el paquete nivel.

Page 256

Para actualizar el paquete fuente, extraiga el nuevo tarball fuente junto al paquete fuente actual. envejece y copia el directorio debian del paquete fuente actual al nuevo. Entonces topa la versión en debian / changelog .

Página 257

conjunto de fuentes $ **apt**
Leyendo listas de paquetes ... Hecho
AVISO: el paquete 'set' se mantiene en el sistema de control de versiones 'Git' en:
https://gitlab.com/kalilinux/packages/set.git
Por favor use:
git clone https://gitlab.com/kalilinux/packages/set.git
para recuperar las últimas actualizaciones (posiblemente inéditas) del paquete.
Necesita obtener 42.3 MB de archivos fuente.
[...]
dpkg-source: advertencia: no se pudo verificar la firma en ./set_7.4.4-0kali1.dsc
dpkg-source: info: extracción del conjunto en set-7.4.4

```
dpkg-source: info: desempaquetado set_7.4.4.orig.tar.gz
dpkg-source: información: desempaquetado set_7.4.4-0kali1.debian.tar.xz
dpkg-source: info: aplicando edit-config-file
dpkg-source: info: aplicando fix-path-interpreter.patch
$ wget https://github.com/trustedsec/social-engineer-toolkit/archive/7.4.5.tar.gz -O
      set_7.4.5.orig.tar.gz
[...]
$ tar xvf set_7.4.5.orig.tar.gz
[...]
social-engineer-toolkit-7.4.5 / src / wireless / wifiattack.py
$ cp -a set-7.4.4 / debian social-engineer-toolkit-7.4.5 / debian
$ cd social-engineer-toolkit-7.4.5
$ dch -v 7.4.5-0buxy1 "Nueva versión ascendente"
```

Eso es. Ahora puede compilar el paquete actualizado.

Dependiendo del tipo de cambios que introduce la nueva versión ascendente, es posible que también necesite para cambiar dependencias de compilación y dependencias de tiempo de ejecución e instalar nuevos archivos. Esos son mucho operaciones más involucradas que no están cubiertas por este libro.

9.1.4. Comenzando la construcción

Cuando todos los cambios necesarios se hayan aplicado a las fuentes, puede comenzar a generar el actual paquete binario o archivo .deb . Todo el proceso es administrado por el comando dpkg-buildpackage y se ve así:

```
$ dpkg-buildpackage -us -uc -b
dpkg-buildpackage: paquete fuente libfreefare
dpkg-buildpackage: versión de origen 0.4.0-2buxy1
dpkg-buildpackage: distribución fuente SIN LANZAMIENTO
dpkg-buildpackage: fuente modificada por Raphael Hertzog <buxy@kali.org>
dpkg-buildpackage: arquitectura de host amd64
[...]
      dh_builddeb
dpkg-deb: compilando el paquete 'libfreefare0-dbgsym' en '../libfreefare0-dbgsym_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: compilando el paquete 'libfreefare0' en '../libfreefare0_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: compilando el paquete 'libfreefare-dev' en '../libfreefare-dev_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: compilando el paquete 'libfreefare-bin-dbgsym' en '../libfreefare-bin-dbgsym_0.4.0-2buxy1_amd64.deb'.
```



```
dpkg-deb: compilando el paquete 'libfreefare-bin' en '../libfreefare-bin_0.4.0-2buxy1_amd64.deb'.
dpkg-deb: compilando el paquete 'libfreefare-doc' en '../libfreefare-doc_0.4.0-2buxy1_all.deb'.
  dpkg-genchanges -b> ../ libfreefare_0.4.0-2buxy1_amd64.changes
dpkg-genchanges: carga solo binaria (no incluye código fuente)
  dpkg-source --after-build libfreefare-0.4.0
dpkg-buildpackage: carga solo binaria (sin fuente incluida)
```

Las-nosotros -ucopciones desactivan firmas de algunos de los archivos generados (.dsc , .changes) porque esto la operación fallará si no tiene una clave GnuPG asociada con la identidad que ha puesto en archivo de registro de cambios . The-boptionasksfora "binary-onlybuild". En este caso, el paquete fuente (.dsc) no se creará, solo los paquetes binarios (.deb) lo harán. Use esta opción para evitar fallas durante el paquete fuente de construcción: si no ha registrado correctamente sus cambios en la gestión de parches sistema, puede quejarse e interrumpir el proceso de compilación.

Como lo sugieren los mensajes de dpkg-deb , los paquetes binarios generados ahora están disponibles en directorio padre (el que aloja el directorio del paquete fuente). Puedes instalarlos con dpkg -i o apt install .

```
$ sudo apt install ../libfreefare0_0.4.0-2buxy1_amd64.deb \
    ../libfreefare-bin_0.4.0-2buxy1_amd64.deb
Leyendo listas de paquetes ... Hecho
Construyendo árbol de dependencia
Leyendo información del estado ... Hecho
Nota, seleccionando 'libfreefare0' en lugar de '../libfreefare0_0.4.0-2buxy1_amd64.deb'
Nota, seleccionando 'libfreefare-bin' en lugar de '../libfreefare-bin_0.4.0-2buxy1_amd64.deb'
Se actualizarán los siguientes paquetes:
    libfreefare-bin libfreefare0
2 actualizados, 0 recién instalados, 0 para eliminar y 0 no actualizados.
Necesita obtener 0 B / 69,4 kB de archivos.
Después de esta operación, se utilizarán 2 048 B de espacio en disco adicional.
[...]
```

Preferimos instalar apt sobre dpkg -i, ya que tratará las dependencias faltantes con gracia. Pero no hace mucho tiempo, tenía que usar dpkg ya que apt no podía manejar archivos .deb fuera de cualquier repositorio.

dpkg-buildpackage La mayoría de las veces, los desarrolladores de Debian usan un programa de nivel superior como debuild ; esto ejecuta dpkg-buildpackage como de costumbre, pero también agrega una invocación de un programa

envoltorios (lintian) que ejecuta muchas comprobaciones para validar el paquete generado contra el De-
Política bian [3] . Este script también limpia el entorno para que el entorno local
Las variables no contaminan la compilación del paquete. El comando debuild es una de las herramientas.
en la suite *devscripts* , que comparten cierta consistencia y configuración para hacer que el
tarea de los mantenedores más fácil.

[3] https://www.debian.org/doc/debian-policy/

9.2. Recompilando el kernel de Linux

Los núcleos proporcionados por Kali incluyen el mayor número posible de características, así como el máximo
cantidad mínima de controladores, para cubrir el espectro más amplio de configuraciones de hardware existentes
raciones Es por eso que algunos usuarios prefieren recompilar el kernel para incluir solo lo que
Necesidad específica. Hay dos razones para esta elección. Primero, es una forma de optimizar la memoria.
consumo ya que todo el código del kernel, incluso si nunca se usa, ocupa memoria física. Porque
las porciones del núcleo compiladas estáticamente nunca se mueven al espacio de intercambio, una disminución general
en el rendimiento del sistema resultará de tener controladores y funciones integradas que nunca se usan.
En segundo lugar, la reducción de la cantidad de controladores y características del kernel reduce el riesgo de problemas de seguridad
ya que solo se está ejecutando una fracción del código de kernel disponible.

Importante

Si elige compilar su propio núcleo, debe aceptar el consentimiento
quences: Kali no puede garantizar actualizaciones de seguridad para su kernel personalizado. Por
manteniendo el núcleo proporcionado por Kali, se beneficia de las actualizaciones preparadas por
El Proyecto Debian.

La recompilación del kernel también es necesaria si desea utilizar ciertas funciones que son solo
disponible como parches (y no incluido en la versión estándar del kernel).

El núcleo de Debian Manual El equipo del núcleo de Debian mantiene el *Manual del núcleo de Debian* (también disponible en el paquete *debian-kernel-handbook*) con documentación completa sobre la mayoría tareas relacionadas con el núcleo y sobre cómo se manejan los paquetes oficiales del núcleo de Debian. Esta es el primer lugar que debe buscar si necesita más información de la que necesita proporcionado en esta sección.

[2] http://kernel-handbook.alioth.debian.org

9.2.1. Introducción y requisitos previos

Como era de esperar, Debian y Kali administran el núcleo en forma de paquete, que no es cómo
Los nels han sido tradicionalmente compilados e instalados. Dado que el núcleo permanece bajo el control de
El sistema de empaquetado se puede quitar limpiamente o desplegar en varias máquinas. Más lejos-
Además, los scripts asociados con estos paquetes automatizan la interacción con el gestor de arranque
y el generador initrd.

Las fuentes ascendentes de Linux contienen todo lo necesario para construir un paquete Debian del núcleo
pero aún necesita instalar el paquete *build-essential* para asegurarse de tener las herramientas necesarias para

buildaDebianpackage. Además, las configuraciones que se *fortalecen en el* núcleo *delkerrequieren que la libncurse5-dev* paquete. Finalmente, el paquete *fakeroot* permitirá la creación del paquete Debian sin necesidad de
ing privilegios administrativos.

```
# apt install build-essential libncurses5-dev fakeroot
```

9.2.2. Obteniendo las fuentes

Dado que las fuentes del kernel de Linux están disponibles como un paquete, puede recuperarlas instalando el paquete de versión de *fuente de linux* . El comando `apt-cache search ^ linux-source` debería enumerar última versión del kernel empaquetada por Kali. Tenga en cuenta que el código fuente contenido en estos paquetes no corresponde exactamente con lo publicado por Linus Torvalds y los desarrolladores del kernel [4] ; como todas las distribuciones, Debian y Kali aplican una serie de parches, que podrían (o no) encontrar su camino hacia la versión ascendente de Linux. Estas modificaciones incluyen backports de arreglos / fea- Tures / controladores de las versiones más recientes del kernel, nuevas características aún no (completamente) fusionadas en el upstream Árbol de Linux, y a veces incluso cambios específicos de Debian o Kali.

El resto de esta sección se centra en la versión 4.9 del kernel de Linux, pero los ejemplos pueden, por supuesto, se adaptará a la versión particular del núcleo que desee.

En este ejemplo, suponemos que se ha instalado el paquete binario *linux-source-4.9* . Tenga en cuenta que Instalamos un paquete binario que contiene las fuentes ascendentes pero no recuperamos la fuente Kali paquete llamado *linux* .

```
# apt install linux-source-4.9
Leyendo listas de paquetes ... Hecho
Construyendo árbol de dependencia
Leyendo información del estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
    bc libreadline7
Paquetes sugeridos:
    libncurses-dev | ncurses-dev libqt4-dev
Se instalarán los siguientes paquetes NUEVOS:
    bc libreadline7 linux-source-4.9
0 actualizado, 3 recién instalados, 0 para eliminar y 0 no actualizado.
Necesita obtener 95.4 MB de archivos.
Después de esta operación, se utilizarán 95.8 MB de espacio en disco adicional.
¿Quieres continuar? [S / n] y
[...]
# ls / usr / src
linux-config-4.9 linux-patch-4.9-rt.patch.xz linux-source-4.9.tar.xz
```

Noticethatthepackagecontains `/usr/src/linux-source-4.9.tar.xz` , acompressedarchiveof las fuentes del kernel Debe extraer estos archivos en un nuevo directorio (no directamente bajo `/ usr / src /` ,

[4] https://kernel.org/

ya que no hay necesidad de permisos especiales para compilar un kernel de Linux). En cambio, `~ / kernel /` es más apropiado.

```
$ mkdir ~ / kernel; cd ~ / kernel
$ tar -xaf /usr/src/linux-source-4.9.tar.xz
```

9.2.3. Configurando el Kernel

El siguiente paso consiste en configurar el núcleo de acuerdo a sus necesidades. El procedimiento exacto Depende de los objetivos.

La compilación del núcleo depende de un archivo de configuración del núcleo. En la mayoría de los casos, lo más probable es que mantenga lo más cerca posible de lo propuesto por Kali, que, como todas las distribuciones de Linux, está instalado en `/` directorio de `arranque` . En este caso, en lugar de reconfigurar todo desde cero, es suficiente haga una copia del archivo `/ boot / config-` *version* . (La versión debe ser la misma que esa versión del núcleo utilizado actualmente, que se puede encontrar con el comando `uname -r` .) Coloque la copia en un archivo `.config` en el directorio que contiene las fuentes del núcleo.

```
$ cp /boot/config-4.9.0-kali1-amd64 ~ / kernel / linux-source-4.9 / .config
```

Alternativamente, dado que el núcleo proporciona configuraciones predeterminadas en `arch / arch / configs / * _ defconfig` , puede poner su configuración seleccionada en su lugar con un comando como `make x86_64_defconfig` (en el caso de una PC de 64 bits) o `hacer i386_defconfig` (en el caso de una `computadora` de 32 bits ORDENADOR PERSONAL).

A menos que necesite cambiar la configuración, puede detenerse aquí y pasar a la sección 9.2.4, " Com- apilando y construyendo el paquete"[Página 236]. Si necesita hacer cambios o si decide reconfigure todo desde cero, debe tomarse el tiempo para configurar su núcleo. Existen varias interfaces dedicadas en el directorio de origen del núcleo que se pueden usar llamando a `make` comando *target* , donde *target* es uno de los valores que se describen a continuación.

make menuconfig compila y lanza una interfaz de configuración de kernel en modo texto (esto es
donde se requiere el paquete *libncurses5-dev*), que permite navegar por los muchos ker-
nel opciones en una estructura jerárquica. Presionando la tecla Espacio cambia el valor del seleccionado
opción, y Enter valida el botón seleccionado en la parte inferior de la pantalla; Seleccionar vuelve a la
submenú seleccionado; Salir cierra la pantalla actual y retrocede en la jerarquía; La ayuda
muestra información más detallada sobre el rol de la opción seleccionada. Las teclas de flecha permiten mover
ing dentro de la lista de opciones y botones. Para salir del programa de configuración, elija Salir de
El menú principal. El programa luego ofrece guardar los cambios que ha realizado; acepta si tu
Están satisfechos con sus elecciones.

Otras interfaces tienen características similares pero funcionan dentro de interfaces gráficas más modernas,
como make xconfig , que usa una interfaz gráfica Qt, y make gconfig , que usa GTK +.
El primero requiere *libqt4-dev* , mientras que el segundo depende de *libglade2-dev* y *libgtk2.0-dev* .

Página 262

Tratar con anticuado Archivos .config

Cuando proporciona un archivo .config que se ha generado con otro (generalmente más antiguo)
versión del núcleo, tendrá que actualizarlo. Puede hacerlo con make oldconfig , que
le preguntará interactivamente las preguntas correspondientes a la nueva configuración
iones Si desea utilizar la respuesta predeterminada a todas esas preguntas, puede utilizar make
olddefconfig . Con make oldnoconfig, asumirá una respuesta negativa a todas las preguntas.
iones

9.2.4. Compilar y construir el paquete

Limpiar antes Reconstrucción

Si ya compiló un núcleo en el directorio y desea reconstruir todo
desde cero (por ejemplo, porque cambió sustancialmente la configuración del núcleo-
), deberá ejecutar make clean para eliminar los archivos compilados. hacer distclean
elimina aún más archivos generados, incluido su archivo .config , así que asegúrese de volver
primero.

Una vez que la configuración del núcleo está lista, un simple make deb-pkg generará hasta cinco Debian
paquetes en formato .deb estándar : *linux-image-* version, que contiene la imagen del núcleo y el
módulos asociados; *linux-headers-* version, que contiene los archivos de encabezado necesarios para compilar ex-
módulos termales; *linux-firmware-image-* version, que contiene los archivos de firmware que necesitan algunos
controladores (este paquete puede faltar cuando compila desde las fuentes del núcleo proporcionadas por
Debian o Kali); *linux-image-* version *-dbg* , que contiene los símbolos de depuración para el kernel
imagen y sus módulos; y *linux-libc-dev* , que contiene encabezados relevantes para algún espacio de usuario
bibliotecas como la biblioteca C de GNU (glibc).

La *versión* se define por la concatenación de la versión ascendente (como se define por la vari-
VERSIÓN, PATCHLEVEL, SUBLEVEL y EXTRAVERSION en el Makefile), de
Parámetro de configuración LOCALVERSION y de la variable de entorno LOCALVERSION.
La versión del paquete reutiliza la misma cadena de versión con una revisión adjunta que es regularmente
incrementado (y almacenado en .version), excepto si lo anula con KDEB_PKGVERSION
Variable ambiental.

```
$ make deb-pkg LOCALVERSION = -custom KDEB_PKGVERSION = $ (make kernelversion) -1
[...]
$ ls ../*.deb
../linux-headers-4.9.0-kali1-custom_4.9.2-1_amd64.deb
../linux-image-4.9.0-kali1-custom_4.9.2-1_amd64.deb
../linux-image-4.9.0-kali1-custom-dbg_4.9.2-1_amd64.deb
../linux-libc-dev_4.9.2-1_amd64.deb
```

Para usar realmente el kernel integrado, el único paso que queda es instalar los paquetes necesarios con dpkg
-i *file.deb* . Se requiere el paquete "linux-image"; solo tiene que instalar los "encabezados de linux"
paquete si tiene algunos módulos de kernel externos para construir, que es el caso si tiene algunos

Página 263

Paquetes "* -dkms" instalados (verifique con dpkg -l "* -dkms" | grep ^ ii). Los otros paquetes
generalmente no son necesarios (¡a menos que sepa por qué los necesita!).

9.3. Creación de imágenes ISO de Kali Live personalizadas

Kali Linux tiene una tonelada de funcionalidad y flexibilidad desde el primer momento. Una vez que Kali está instalado, usted puede realizar todo tipo de hazañas increíbles con un poco de orientación, creatividad, paciencia y práctica.
Sin embargo, también puede personalizar una compilación de Kali para que contenga archivos o paquetes específicos (para escalar aumentar o reducir el rendimiento y las funciones) y puede realizar ciertas funciones automáticamente. por ejemplo, el Kali ISO de Doom[5] y Kali Evil Wireless Access Point [6] son excelentes proyectos que se basan en una implementación personalizada de Kali Linux. Echemos un vistazo al proceso de rodadura una imagen ISO Kali Linux personalizada.

Las imágenes oficiales de Kali ISO se crean con live-build[7] , que es un conjunto de scripts que permite Completa automatización y personalización de todas las facetas de la creación de imágenes ISO. La suite *live-build* usa una estructura de directorio completa como entrada para su configuración. Almacenamos esta configuración y algunas scripts auxiliares asociados en un repositorio Git live-build-config. Utilizaremos este repositorio como base para construir imágenes personalizadas.

Antes de continuar, debe saber que los comandos que se muestran en esta sección están destinados a ser ejecutarse en un sistema Kali Linux actualizado. Es muy probable que fallen si se ejecutan en un sistema no Kali o si el sistema no está actualizado

9.3.1. Instalación de requisitos previos

El primer paso es instalar los paquetes necesarios y recuperar el repositorio de Git con Kali configuración de *construcción en vivo* :

```
# apt install curl git live-build
[...]
# git clone https://gitlab.com/kalilinux/build-scripts/live-build-config.git
[...]
# cd live-build-config
# ls
auto build_all.sh build.sh kali-config README
```

En este punto, ya puede crear una imagen ISO de Kali actualizada (pero no modificada) simplemente ejecutando ./build.sh --verbose . La construcción tardará mucho tiempo en completarse, ya que descargará todos los paquetes para incluir. Cuando termine, encontrará la nueva imagen ISO en el directorio de imágenes .

[5] https://www.offensive-security.com/kali-linux/kali-linux-iso-of-doom
[6] https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/
[7] http://debian-live.alioth.debian.org/live-build/

9.3.2. Creación de imágenes en vivo con diferentes entornos de escritorio

El contenedor build- sh live-build que proporcionamos es responsable de configurar el directorio de configuración historia que live-build espera encontrar. Puede establecer diferentes configuraciones dependiendo de su opción --variante.

El contenedor crea el directorio de configuración combinando archivos de kali-config / common y kali-config / variant- *X* , donde *X* es el nombre de una variante dada con el parámetro --variant.
Cuando la opción no se proporciona explícitamente, utiliza el valor predeterminado como el nombre de la variante.

El directorio kali-config contiene directorios para los entornos de escritorio más comunes:

- e17 para la Iluminación;
- gnome para GNOME;
- i3wm para el administrador de ventanas correspondiente;
- kde para KDE;
- lxde para LXDE;
- mate para el entorno de escritorio Mate;
- xfce para XFCE.

La variante ligera es un poco especial; se basa en XFCE[8] y se utiliza para generar la "luz" oficial Imágenes ISO que contienen un conjunto reducido de aplicaciones.

Puede crear fácilmente una imagen en vivo de Kali usando KDE como entorno de escritorio con esta única computadora mand:

```
# ./build.sh --variante kde --verbose
```

Este concepto de *variante* permite algunas personalizaciones predefinidas de alto nivel, pero si toma el hora de leer el manual del sistema Debian Live[9] , descubrirá muchas otras formas de personalizar tomize las imágenes, simplemente cambiando el contenido del subdirectorio apropiado de kali-config . Las siguientes secciones proporcionarán algunos ejemplos.

9.3.3. Cambiar el conjunto de paquetes instalados

Una vez iniciado, live-build instala todos los paquetes enumerados en package-lists / *. List.chroot archivos. La configuración predeterminada que proporcionamos incluye un paquete-lists / kali.list.chroot archivo, que enumera *kali-linux-full* (el metapaquete principal que incluye todos los paquetes de Kali para incluir). usted puede comentar este paquete y poner otro metapaquete de su elección o incluir un Conjunto de otros paquetes. También puede combinar ambos enfoques comenzando con un metapaquete y agregando paquetes suplementarios de su elección.

[8] https://www.xfce.org/
[9] [9] http://debian-live.alioth.debian.org/live-manual/unstable/manual/html/live-manual.en.html

Con las listas de paquetes , solo puede incluir paquetes que ya están disponibles en el Kali oficial repositorio. Pero si tiene paquetes personalizados, puede incluir la imagen en vivo al colocar el archivos .deb en un directorio packages.chroot (por ejemplo, kali-config / config-gnome / packages. chroot si construyes la variante GNOME).

Los metapaquetes son paquetes vacíos cuyo único propósito es tener muchas dependencias de otros paquetes Facilitan la instalación de conjuntos de paquetes que a menudo desea instalar juntos. El paquete fuente kali-meta construye todos los metapaquetes provistos por Kali Linux:

- kali-linux: el sistema base (lo extraen todos los demás metapaquetes)
- kali-linux-full: la instalación predeterminada de Kali Linux
- kali-linux-all: metapaquete de todos los metapaquetes y otros paquetes (casi todos- ¡Lo que Kali proporciona, por lo que es realmente enorme!)
- kali-linux-sdr: herramientas de radio definida por software (SDR)
- kali-linux-gpu: herramientas con GPU (herramientas que hacen uso de la potencia informática disponible en tu tarjeta gráfica)
- kali-linux-wireless: herramientas de análisis y evaluación inalámbricas
- kali-linux-web: herramientas de evaluación de aplicaciones web
- kali-linux-forensic: herramientas forenses (encontrar evidencia de lo que sucedió)
- kali-linux-voip: herramientas de voz sobre IP
- kali-linux-pwtools: herramientas para descifrar contraseñas
- kali-linux-top10: las diez herramientas más populares
- kali-linux-rfid: herramientas RFID

Puede aprovechar estos metapaquetes cuando cree listas de paquetes personalizados para la construcción en vivo . los La lista completa de paquetes de meta disponibles y las herramientas que pueden incluir puede ser http: //tools.kali. org / kali-metapackages

Presentación de Debconf de Paquetes instalados Puede proporcionar archivos predefinidos de Debconf (consulte la sección 4.3.2 , "Crear un archivo presentado " [página 93] para explicaciones) como archivos preseleccionados / *. cfg . Se usarán para configurar los paquetes instalados en el sistema de archivos en vivo.

9.3.4. Usando ganchos para ajustar el contenido de la imagen

Live-build ofrece ganchos que pueden ejecutarse en pasos diferentes del proceso de construcción . Chroothooks son scripts ejecutables que instala como archivos hooks / live / *. chroot en su árbol de configuración y que se ejecutan dentro del chroot. Mientras chroot es el comando que te permite cambiar temporalmente el directorio raíz del sistema operativo a un directorio de su elección, también se usa por extensión para

designar un directorio que aloja un árbol de sistema de archivos completo (alternativo). Este es el caso aquí con live-build , donde el directorio chroot es el directorio donde se está preparando el sistema de archivos en vivo. Dado que las aplicaciones iniciadas en un chroot no pueden ver fuera de ese directorio, lo mismo ocurre con el ganchos chroot: solo puede usar y modificar cualquier cosa disponible en ese entorno chroot. Nosotros confíe en esos ganchos para realizar múltiples personalizaciones específicas de Kali (consulte kali-config / common / ganchos / live / kali-hacks.chroot).

Los ganchos binarios (hooks / live / *. Binary) se ejecutan en el contexto del proceso de compilación (y no chrooteado en cualquier lugar) al final del proceso. Puede modificar el contenido de la imagen ISO construida pero no del sistema de archivos en vivo ya que en este punto, ya se ha generado. Usamos esta característica en Kali para realizar algunos cambios en la configuración predeterminada de isolinux generada por live-build. por ejemplo, vea kali-config / common / hooks / live / persistence.binary donde agregamos el arranque entradas de menú que permiten la persistencia.

9.3.5. Agregar archivos en la imagen ISO o en el sistema de archivos en vivo

Otra personalización muy común es agregar archivos en el sistema de archivos en vivo o en el ISO imagen.

Puede agregar archivos al sistema de archivos en vivo colocándolos en su ubicación esperada antes de-bajo la includes.chroot directorio de configuración. Por ejemplo, proporcionamos kali-config / common / Incluye.chroot / usr / lib / live / config / 0031-root-password , que termina como / usr / lib / live / config / 0031-root-password en el sistema de archivos live.

Live-Boot Hooks Scripts instalados como / lib / live / config / *XXXX* - el*nombre* se ejecuta mediante el script de inicio del paquete live-boot. Reconfiguran muchos aspectos del sistema para adaptarse para un sistema en vivo. Puede agregar sus propios scripts para personalizar su sistema en vivo en tiempo de ejecución: se usa especialmente para implementar un parámetro de arranque personalizado, por ejemplo.

Puede agregar archivos a la imagen ISO colocándolos en su ubicación esperada debajo de las inclusiones. directorio de configuración binaria . Por ejemplo, proporcionamos kali-config / common / includes.binary / isolinux / splash.png para anular la imagen de fondo utilizada por el gestor de arranque Isolinux (que se almacena en /isolinux/splash.png en el sistema de archivos de la imagen ISO).

9.4. Agregar persistencia al ISO en vivo con una llave USB

9.4.1. La característica de persistencia: explicaciones

A continuación, analizaremos los pasos necesarios para agregar persistencia a una llave USB Kali. La naturaleza de una vida El sistema debe ser efímero. Todos los datos almacenados en el sistema en vivo y todos los cambios realizados se pierden cuando reinicies. Para remediar esto, puede usar una característica de *live-boot* llamada persistencia, que es habilitado cuando los parámetros de arranque incluyen la palabra clave de persistencia.

Dado que modificar el menú de arranque no es una tarea trivial, Kali incluye dos entradas de menú por defecto que permiten la persistencia: Live USB Persistence y Live USB Encrypted Persistence, como se muestra en Figura 9.1, " Entradas del menú de persistencia"[Página 241].

Figura 9.1 *Entradas del menú de persistencia*

Cuando esta función está habilitada, *live-boot* escaneará todas las particiones buscando sistemas de archivos etiquetados persistencia (que puede anularse con el parámetro de arranque etiqueta-persistencia = *valor*) y el el instalador configurará la persistencia de los directorios que se enumeran en el archivo persistence.conf encontrado en esa partición (en una línea de directorio). El valor especial "/ unión" permite una persistencia completa de todos los directorios con un *montaje de unión* , una superposición que almacena solo los cambios en comparación con El sistema de archivos subyacente. Los datos de los directorios persistentes se almacenan en el sistema de archivos que contiene el archivo persistence.conf correspondiente .

Página 268

9.4.2. Configuración de la persistencia sin cifrar en una llave USB

En esta sección, suponemos que ha preparado KaliLiveUSBTecla siguiendo las instrucciones en la sección 2.1.4 , "Copiar la imagen en un DVD-ROM o llave USB "[Página 19] y que ha utilizado una memoria USB lo suficientemente grande como para contener la imagen ISO (aproximadamente 3 GB) y los datos de los directorios que querer persistir También suponemos que Linux reconoce la clave USB como / dev / sdb y que solo contiene las dos particiones que forman parte de la imagen ISO predeterminada (/ dev / sdb1 y / dev / sdb2). Tenga mucho cuidado al realizar este procedimiento. Puede destruir fácilmente datos importantes si Vuelva a particionar la unidad incorrecta.

Para agregar una nueva partición, debe conocer el tamaño de la imagen que copió para poder hacer la nueva partición comienza después de la imagen en vivo. Luego use parted para crear realmente la partición. Los siguientes comandos analizan la imagen ISO llamada kali-linux-2016.1-amd64.iso , que es se supone que también está presente en la memoria USB:

```
# parted / dev / sdb print
Modelo: SanDisk Cruzer Edge (scsi)
Disco / dev / sdb: 32,0GB
Tamaño del sector (lógico / físico): 512B / 512B
Tabla de particiones: msdos
Banderas de disco:

Inicio de número Final Talla Tipo Banderas del sistema de archivos
 1 32,8kB 2852MB 2852MB primario arranque oculto
 2 2852MB 2945MB 93,4MB primario
# start = $ (du --block-size = 1MB kali-linux-2016.1-amd64.iso | awk '{print $ 1}')
# echo "El tamaño de la imagen es $ start MB"
El tamaño de la imagen es 2946 MB
# parted -a óptimo / dev / sdb mkpart primary "$ {start} MB" 100%
Información: es posible que deba actualizar / etc / fstab.

# parted / dev / sdb print
Modelo: SanDisk Cruzer Edge (scsi)
Disco / dev / sdb: 32,0GB
Tamaño del sector (lógico / físico): 512B / 512B
Tabla de particiones: msdos
Banderas de disco:

Inicio de número Final Talla Tipo Banderas del sistema de archivos
 1 32,8kB 2852MB 2852MB primario arranque oculto
 2 2852MB 2945MB 93,4MB primario
 3 2946MB 32,0GB 29,1GB primario
```

Con la nueva partición / dev / sdb3 en el lugar , formatee con un sistema de 4 archivos denominado "persistencia" con la ayuda del comando mkfs.ext4 (y su opción -L para establecer la etiqueta). La partición es entonces montado en el / mnt directoryandyouaddtherequired persistence.conf configurationfile. Como

siempre, tenga cuidado al formatear cualquier disco. Podría perder información valiosa si formatea El disco o la partición incorrectos.

```
# mkfs.ext4 -L persistencia / dev / sdb3
mke2fs 1.43-WIP (15-mar-2016)
Creación de un sistema de archivos con 7096832 bloques de 4k y 1777664 inodes
UUID del sistema de archivos: dede20c4-5239-479a-b115-96561ac857b6
Copias de seguridad de superbloque almacenadas en bloques:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Asignación de tablas grupales: hecho
Escribir tablas de inodo: hecho
Creación de diario (32768 bloques): hecho
Escritura de superbloques e información contable del sistema de archivos: hecho
# mount / dev / sdb3 / mnt
# echo "/ union"> /mnt/persistence.conf
# ls -l / mnt
total 20
drwx ------ 2 raíz raíz 16384 10 de mayo 13:31 perdido + encontrado
-rw-r - r-- 1 raíz raíz 8 de mayo 10 13:34 persistence.conf
# umount / mnt
```

La llave USB ya está lista y se puede iniciar con la entrada del menú de inicio "Live USB Persistence".

9.4.3. Configuración de la persistencia cifrada en una llave USB

live-boot también puede manejar sistemas de archivos de persistencia en particiones cifradas. Puedes así proteja los datos de sus directorios persistentes creando una partición cifrada LUKS que contenga Datos de persistencia.

Los pasos iniciales son los mismos hasta la creación de la partición, pero en lugar de formatearla con un sistema de archivos ext4, use `cryptsetup` para inicializarlo como un contenedor LUKS. Luego abre ese contenedor y configure el sistema de archivos ext4 de la misma manera que en la configuración no cifrada, pero en lugar de usar la partición `/ dev / sdb3` , use la partición virtual creada por `cryptsetup` . Esta partición virtual representa el contenido descifrado de la partición cifrada, que está disponible en `/ dev / mapper` bajo el nombre que le asignaste. En el siguiente ejemplo, utilizaremos el nombre kali_persistence. Nuevamente, asegúrese de estar utilizando la unidad y la partición correctas.

```
# cryptsetup --verbose --verify-passphrase luksFormat / dev / sdb3

¡ADVERTENCIA!
========
Esto sobrescribirá los datos en / dev / sdb3 irrevocablemente.

¿Estás seguro? (Escriba mayúscula sí): SÍ
```



```
Ingrese la frase de contraseña:
Verificar frase de contraseña:
Comando exitoso.
# cryptsetup luksOpen / dev / sdb3 kali_persistence
Ingrese la frase de contraseña para / dev / sdb3:
# mkfs.ext4 -L persistencia / dev / mapper / kali_persistence
mke2fs 1.43-WIP (15-mar-2016)
Creación de un sistema de archivos con 7096320 bloques de 4k y 1774192 inodes
Sistema de archivos UUID: 287892c1-00bb-43cb-b513-81cc9e6fa72b
Copias de seguridad de superbloque almacenadas en bloques:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Asignación de tablas grupales: hecho
Escribir tablas de inodo: hecho
Creación de diario (32768 bloques): hecho
Escritura de superbloques e información contable del sistema de archivos: hecho

# mount / dev / mapper / kali_persistence / mnt
# echo "/ union"> /mnt/persistence.conf
```

```
# umount / mnt
# cryptsetup luksClose / dev / mapper / kali_persistence
```

9.4.4. Usar múltiples tiendas de persistencia

Si tiene múltiples casos de uso para su sistema Kali live, puede usar múltiples sistemas de archivos con diferentes ferent etiquetas e indican en la línea de comando de arranque qué (conjunto de) sistemas de archivos deben usarse para la característica de persistencia: esto se hace con la ayuda del parámetro de inicio persistence-label = *label* .

Asumamos que usted es un probador de pluma profesional. Cuando trabajas para un cliente, usas un partición de persistencia cifrada para proteger la confidencialidad de sus datos en caso de que la llave USB esté robado o comprometido. Al mismo tiempo, desea poder mostrar Kali y algunos material de movimiento almacenado en una partición sin cifrar de la misma llave USB. Ya que no quieres para editar manualmente los parámetros de arranque en cada arranque, desea crear una imagen en vivo personalizada con entradas dedicadas al menú de arranque.

El primer paso es crear el ISO en vivo personalizado (siguiendo la sección 9.3 , " Creación de Kali Live personalizado Imágenes ISO "[página 237] y en particular la sección 9.3.4 ,"Usando ganchos para ajustar el contenido de la imagen "[página 239]). La personalización principal es modificar kali-config / common / hooks / live / persistence-menu.binary para que se vea así (tenga en cuenta los parámetros de etiqueta de persistencia):

```
#! / bin / sh

Si [ ! -d isolinux]; entonces
        binario de cd
```



```
fi

gato >> isolinux / live.cfg << FIN

etiqueta de demostración en vivo
        etiqueta de menú ^ USB en vivo con datos de demostración
        linux / live / vmlinuz
        initrd /live/initrd.img
        agregar boot = live username = root hostname = kali persistence-label = demo persistence

etiqueta de trabajo en vivo
        etiqueta de menú ^ USB en vivo con datos de trabajo
        linux / live / vmlinuz
        initrd /live/initrd.img
        agregar boot = live username = root hostname = kali persistence-label = work persistence-
                ¯ cifrado = luks persistencia

FINAL
```

A continuación, crearemos nuestra ISO personalizada y la copiaremos a la tecla USB. Luego crearemos e iniciaremos el dos particiones y archivos ystems que se utilizarán para la persistencia. La primera partición no está encriptada (etiquetado como "demo"), y el segundo está encriptado (etiquetado como "trabajo"). Asumiendo / dev / sdb es nuestro USB clave y el tamaño de nuestra imagen ISO personalizada es de 3000 MB, se vería así:

```
# parted / dev / sdb mkpart primario 3000 MB 55%
# parted / dev / sdb mkpart primary 55% 100%
# mkfs.ext4 -L demo / dev / sdb3
[...]
# mount / dev / sdb3 / mnt
# echo "/ union"> /mnt/persistence.conf
# umount / mnt
# cryptsetup --verbose --verify-passphrase luksFormat / dev / sdb4
[...]
# cryptsetup luksOpen / dev / sdb4 kali_persistence
[...]
# mkfs.ext4 -L work / dev / mapper / kali_persistence
[...]
# mount / dev / mapper / kali_persistence / mnt
# echo "/ union"> /mnt/persistence.conf
# umount / mnt
# cryptsetup luksClose / dev / mapper / kali_persistence
```

Y eso es todo. ¡Ahora puede arrancar la USBkey y seleccionar de las nuevas entradas del menú de arranque según sea necesario!

Página 272

Agregar una contraseña nuclear para mayor seguridad

Kali proporciona un paquete *cryptsetup-nuke-password* que modifica los principios de cryptsetup guiones de arranque para implementar una nueva función: puede establecer una *contraseña nuclear* que, cuando utilizado: destruirá todas las claves utilizadas para administrar la partición cifrada.

Esto puede ser útil cuando viaja mucho y necesita una forma rápida de garantizar sus datos No se puede recuperar. Al iniciar, simplemente escriba la contraseña nuclear en lugar de la real uno y será imposible para cualquier persona (incluido usted) acceder a sus datos.

Antes de usar esa función, es aconsejable hacer una copia de seguridad de su cifrado llaves y guárdelas en un lugar seguro.

Puede configurar una contraseña nuclear con este comando (suponiendo que tenga paquete instalado):

```
# dpkg-reconfigure cryptsetup-nuke-password
```

Puede encontrar más información sobre esta función en el siguiente tutorial:

[2] https://www.kali.org/tutorials/nuke-kali-linux-luks/

9.5. Resumen

En este capítulo, aprendimos sobre cómo modificar los paquetes fuente de Kali, que son la construcción básica bloques de todas las aplicaciones enviadas en Kali. También descubrimos cómo personalizar e instalar el Kali núcleo. Luego discutimos el entorno de construcción en vivo y discutimos cómo construir un entorno personalizado Kali Linux ISO. También demostramos cómo crear Kali USB encriptado y no encriptado instala.

9.5.1. Consejos resumidos para modificar los paquetes de Kali

La modificación de los paquetes de Kali suele ser una tarea para los contribuyentes y desarrolladores de Kali, pero es posible que tenga necesidades específicas no cubiertas por los paquetes oficiales y saber cómo construir un paquete modificado puede ser muy valioso, especialmente si desea compartir sus cambios, implementarlos internamente o Limpie el software de nuevo a un estado anterior.

Cuando necesite modificar una pieza de software, puede ser tentador descargar la fuente, hacer los cambios y use el software modificado. Sin embargo, si su aplicación requiere un sistema completo configuración (por ejemplo, con un paso de instalación), entonces *contaminará* su sistema de archivos con archivos desconocidos para dpkg y pronto creará problemas que las dependencias de paquetes no pueden detectar. Adicionalmente, Este tipo de modificación de software es más tedioso de compartir.

Al crear un paquete modificado, el proceso general es siempre el mismo: tome el paquete fuente. edad, extráigala, realice los cambios y luego cree el paquete. Para cada paso, a menudo hay Múltiples herramientas que pueden manejar cada tarea.

Página 273

Para comenzar a reconstruir un paquete Kali, primero descargue el paquete fuente, que se compone de un * .dsc (*Debian Source Control*) y de archivos adicionales a los que se hace referencia desde ese archivo de control.

Los paquetes fuente se almacenan en espejos accesibles a través de HTTP. La forma más eficiente de obtenerlos es con apt source *source-package-name* , que requiere que agregue una línea deb-src a / etc / apt / sources.list y actualice los archivos de índice con apt update .

Además, puede usar dget (del paquete *devscripts*) para descargar un archivo .dsc directamente junto con sus archivos adjuntos. Para paquetes específicos de Kali cuyas fuentes están alojadas en un Repositorio de Git en gitlab.com/kalilinux/packages[10] , puedes recuperar las fuentes con git clone https://gitlab.com/kalilinux/packages/ *source-package* .git .

Después de descargar las fuentes, instale los paquetes enumerados en las dependencias de compilación del paquete fuente con sudo apt build-dep ./ . Este comando debe ejecutarse desde el directorio fuente del paquete.

Las actualizaciones de un paquete fuente consisten en una combinación de algunos de los siguientes pasos:

- El primer paso requerido es cambiar el número de versión para distinguir su paquete de theoriginalwith dch --local *versión de identificador* , ormodifyotherpackagedetailswith dch .
- Aplicar un parche con patch -p1 < *archivo de parche* o modificar la serie de parches de la colcha .
- Ajustar las opciones de compilación, que generalmente se encuentran en el archivo debian / rules del paquete u otros archivos en el directorio debian /

Después de modificar un paquete fuente, puede compilar el paquete binario con dpkg-buildpackage -us -uc -b del directorio de origen, que generará un paquete binario sin signo. El paquete-age se puede instalar con dpkg -i *package-name_version_arch.deb* .

9.5.2. Sugerencias resumidas para volver a compilar el kernel de Linux

Como usuario avanzado, es posible que desee volver a compilar el núcleo Kali. Es posible que desee adelgazar El núcleo Kali estándar, que está cargado con muchas características y controladores, agrega controladores no estándar o características, o aplicar parches de kernel. Sin embargo, tenga cuidado: un kernel mal configurado puede desestabilizar su sistema y debe estar preparado para aceptar que Kali no puede garantizar actualizaciones de seguridad para su kernel personalizado.

Para la mayoría de las modificaciones del kernel, deberá instalar algunos paquetes con apt install build-esencial libncurses5-dev fakeroot .

El comando apt-cache search ^ linux-source debería enumerar la última versión del kernel empaquetada por Kali, y apt install linux-source- *version-number* instala un archivo comprimido de fuente del núcleo en / usr / src .

[10] https://gitlab.com/kalilinux/packages

Los archivos de origen deben extraerse con tar -xaf en un directorio que no sea / usr / src (como ~ / kernel).

Cuando llegue el momento de configurar su núcleo, tenga en cuenta estos puntos:

- A menos que sea un usuario avanzado, primero debe completar un archivo de configuración del núcleo. El método preferido es tomar prestada la configuración estándar de Kali copiando / boot / config- *version-string* a ~ / kernel / linux-source- *version-number* /.config . Alterna-Puede usar make *architecture* _defconfig para obtener una configuración razonable para La arquitectura dada.
- La herramienta de configuración del kernel make menuconfig basada en texto leerá el archivo .config y presentarle todos los elementos de configuración en un gran menú que puede navegar. Seleccionar un El elemento le muestra su documentación, sus posibles valores y le permite ingresar un nuevo valor.

Cuando se ejecuta desde el directorio de origen del kernel, make clean eliminará los archivos compilados previamente y make deb-pkg generará hasta cinco paquetes Debian. El archivo *linux-image-* version .deb contiene la imagen del kernel y los módulos asociados.

Para usar realmente el kernel construido, instale los paquetes necesarios con dpkg -i *file.deb* . El "linux-imagen "se requiere el paquete; solo tiene que instalar el paquete "linux-headers" si tiene alguna módulos de kernel externos para compilar, que es el caso si tiene instalados algunos paquetes "* -dkms" (verifique con dpkg -l "* -dkms" | grep ^ ii). Los otros paquetes generalmente no son necesarios (un-menos sabes por qué los necesitas!).

9.5.3. Resumen de sugerencias para crear imágenes ISO Kali Live ISO personalizadas

Las imágenes oficiales de Kali ISO se crean con live-build[11] , que es un conjunto de scripts que permite Automatización y personalización completas de todas las facetas de la creación de imágenes ISO.

Su sistema Kali debe estar completamente actualizado antes de usar live-build.

La configuración de creación en vivo de Kali se puede recuperar de los repositorios Git de Kali con dos componentes mands: apt install curl git live-build seguido de git clone https://gitlab.com/kalilinux / build-scripts / live-build-config.git

Para generar una imagen ISO de Kali actualizada pero sin modificar, simplemente ejecute ./build.sh --verbose . los La compilación tardará mucho tiempo en completarse, ya que descargará todos los paquetes para incluir. Cuando terminado, encontrará la nueva imagen ISO en el directorio de imágenes . Si agrega - *variante variante* a la línea de comando, construirá la variante dada de la imagen ISO de Kali. Las diversas variantes

están definidos por sus directorios de configuración kali-config / variant- * . La imagen principal es la variante de gnomo.

Hay varias formas de personalizar su ISO modificando el directorio de configuración de live-build:

[11] http://debian-live.alioth.debian.org/live-build/

- Los paquetes se pueden agregar (o eliminar) a un ISO en vivo modificando las listas de paquetes / *. archivos list.chroot .
- Los paquetes personalizados se pueden incluir en la imagen en vivo colocando los archivos .deb en un paquete. directorio chroot Su instalación se puede preconfigurar con archivos predefinidos / *. Cfg .
- Puede agregar archivos al sistema de archivos en vivo colocándolos en su ubicación esperada debajo del incluye el directorio de configuración chroot.
- Puede ejecutar scripts durante el proceso de configuración de chroot del sistema en vivo instalándolos como hooks / live / *. chroot archivos. También puede ejecutar scripts en el momento del arranque del live generado imagen: youmustarrangeforthemtobeinstalledin / usr / lib / live / config / *XXXX - nombre* , para ejemplo confiando en el directorio de configuración includes.chroot .
- El manual de Debian Live Systems [12] es una excelente referencia para la configuración de construcción en vivo y pruebas.

Configurar la persistencia cifrada y no cifrada en una llave USB: es bastante sencillo crear un Instalación estándar de Kali Live USB. Aunque el proceso puede parecer sintácticamente complejo, es relativamente directo para agregar persistencia cifrada y no cifrada a su portátil instalación para ampliar significativamente su funcionalidad.

En el siguiente capítulo, discutiremos como se muestra en Kalis para la empresa. Discutiremos la configuración administración y mostrarle cómo extender y personalizar Kali Linux de una manera fácil de implementar si tienes un par de máquinas o varios miles.

[12] http://debian-live.alioth.debian.org/live-manual/unstable/manual/html/live-manual.en.html

Palabras clave

Instalación PXE
Configuración
administración
Saltstack
Bifurcando paquetes de Kali
Configuración
paquetes
Repositorio de paquetes

Capítulo

10

Kali Linux en el Empresa

Contenido

Instalación de Kali Linux a través de la red (arranque PXE) 252
Aprovechar la gestión de configuración 255
Ampliación y personalización de Kali Linux 262
Resumen 273

Hasta ahora, hemos visto que Kali es un derivado de Debian extremadamente capaz y seguro.
ing características de seguridad y cifrado de alta resistencia industrial, gestión avanzada de paquetes, multi-
capacidad de plataforma, y (lo que es más conocido para) un área de herramientas de clase mundial para la seguridad
profesional. Lo que podría no ser obvio es cómo Kali escala más allá del escritorio a mediano o grande
escalar implementaciones e incluso a nivel empresarial. En este capítulo, le mostraremos qué tan bien
Kali puede escalar más allá del escritorio, proporcionando administración centralizada y control a nivel empresarial
controlar múltiples instalaciones de Kali Linux. En resumen, después de leer este capítulo, podrá
implemente rápidamente sistemas Kali altamente seguros preconfigurados para sus necesidades específicas y manténgalos
sincronizado gracias a la instalación (semi-automática) de Kali de actualizaciones de paquetes.

Este nivel de escala requiere varios pasos, incluido el inicio de un arranque de red PXE, el uso de un anuncio
herramienta de administración de configuración avanzada (SaltStack), la capacidad de bifurcar y personalizar paquetes,
y la implementación de un repositorio de paquetes. Cubriremos cada paso en detalle, le mostraremos cómo
elimine el "trabajo pesado", e implemente, administre y mantenga multitudes de personalizadas
Instalaciones de Kali Linux con relativa facilidad. Como si eso fuera poco, arrojaremos una multitud de
secuaces para ayudarte a dirigir tu imperio.

10.1 Instalación de Kali Linux a través de la red (arranque PXE)

Como hemos visto en capítulos anteriores, el proceso básico de instalación de Kali Linux es sencillo
una vez que conozca su camino. Pero tenga que instalar Kalionmultiplemachines, el estándar
La configuración puede ser bastante tediosa. Afortunadamente, puede iniciar el procedimiento de instalación de Kali iniciando un
computadora a través de la red. Esto le permite instalar Kali rápida y fácilmente en muchas máquinas
a la vez

Primero, deberá iniciar su máquina de destino desde la red. Esto es facilitado por el Pre-
boot eXecution Environment (PXE), una interfaz cliente / servidor diseñada para arrancar cualquier red ma-
China desde la red, incluso si no tiene un sistema operativo instalado. Configurar PXE
el arranque de red requiere que configure al menos un servidor trivial de protocolo de transferencia de archivos (TFTP) y
un servidor DHCP / BOOTP. También necesitará un servidor web si desea alojar una presentación previa de *debconf*
archivo que se usará automáticamente en el proceso de instalación.

Afortunadamente, *dnsmasq* maneja tanto DHCP como TFTP para que pueda confiar en un solo servicio para configurar
arriba todo lo que necesitas. Y el servidor web Apache está instalado (pero no habilitado) de forma predeterminada en
Sistemas Kali.

Separar DHCP y TFTP demonios

Para configuraciones más complejas, el conjunto de funciones de *dnsmasq* puede ser demasiado limitado o puede desea habilitar el arranque PXE en su red principal que ya ejecuta un demonio DHCP.
En ambos casos, tendrá que configurar demonios DHCP y TFTP separados.

El manual de instalación de Debian cubre la configuración de *isc-dhcp-server* y *tftpd-hpa* para Arranque PXE.

[2] https://www.debian.org/releases/stable/amd64/ch04s05.html

Para configurar *dnsmasq* , primero debe configurarlo a través de /etc/dnsmasq.conf . Un concepto básico
La figuración consta de solo unas pocas líneas clave:

```
# Interfaz de red para manejar
interfaz = eth0
# Opciones de DHCP
# Rango de IP para asignar
```

```
dhcp-range = 192.168.101.100,192.168.101.200,12h
# Gateway para anunciar a los clientes
dhcp-option = opción: enrutador, 192.168.101.1
# Servidores DNS para anunciar a los clientes
dhcp-option = opción: dns-server, 8.8.8.8,8.8.4.4
# Archivo de inicio para anunciar a los clientes
dhcp-boot = pxelinux.0
# Opciones TFTP
enable-tftp
# Directorio de archivos de alojamiento para servir
tftp-root = / tftpboot /
```

Con /etc/dnsmasq.conf configurado, deberá colocar los archivos de arranque de la instalación en / tftpboot / directorio. Kali Linux proporciona un archivo de archivos dedicado a este propósito que puede ser directamente desempaquetado en / tftpboot / . Simplemente seleccione entre 32 bits (i386) y 64 bits (amd64) y métodos de instalación estándar o gráficos (gtk) para su máquina de destino y elija el apropiado archivo:

[2] http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/

netboot / gtk / netboot.tar.gz

[2] http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/

netboot / netboot.tar.gz

[2] http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images/

netboot / gtk / netboot.tar.gz

[2] http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images/

netboot / netboot.tar.gz

Una vez que haya seleccionado el archivo, cree / tftpboot / , descargue el archivo y descomprímalo en ese directorio:

```
# mkdir / tftpboot
# cd / tftpboot
# wget http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images/
        ¯ netboot / netboot.tar.gz
# tar xf netboot.tar.gz
# ls -l
total 25896
drwxrwxr-x 3 raíz root                    4096 6 de mayo 04:43 instalador de Debian
```



```
lrwxrwxrwx 1 raíz raíz                    47 6 de mayo 04:43 ldlinux.c32 -> debian-installer / amd64 / boot
        ¯ -screens / ldlinux.c32
-rw-r - r-- 1 raíz raíz 26507247 6 de mayo 04:43 netboot.tar.gz
lrwxrwxrwx 1 raíz raíz                    33 6 de mayo 04:43 pxelinux.0 -> debian-installer / amd64 /
        ¯ pxelinux.0
lrwxrwxrwx 1 raíz raíz                    35 6 de mayo 04:43 pxelinux.cfg -> debian-installer / amd64 /
        ¯ pxelinux.cfg
-rw-rw-r-- 1 raíz raíz                    71 6 de mayo 04:43 version.info
```

Los archivos desempaquetados incluyen el *gestor de* arranque *pxelinux* , que utiliza los mismos archivos de configuración que *syslinux* e *isolinux* . Debido a esto, puede modificar los archivos de arranque en debian-installer / amd64 / pantallas de arranque / como lo haría al generar imágenes ISO de Kali Linux Live personalizadas .

Por ejemplo, suponiendo que haya elegido el instalador textual, puede agregar parámetros de arranque a preseleccione los valores de idioma, país, mapa de teclas, nombre de host y nombre de dominio. También puedes señalar el instalador a una URL externa preestablecida y configure el tiempo de espera para que el arranque se realice automáticamente tomatically si no se presiona ninguna tecla en 5 segundos. Para lograr esto, primero debe modificar el archivo debian-installer / amd64 / txt.cfg :

```
instalación de etiquetas
        etiqueta de menú ^ Instalar
        kernel debian-installer / amd64 / linux
        anexar vga = 788 initrd = debian-installer / amd64 / initrd.gz ---  lenguaje silencioso = es
                ¯ país = mapa de teclas de EE. UU. = Nombre de host de EE. UU. = Dominio kali = url = http: //192.168.101.1/
                ¯ preseed.cfg
```

Luego, modificaría el archivo debian-installer / amd64 / syslinux.cfg para ajustar el tiempo de espera:

```
# DI config versión 2.0
```

```
# ruta de búsqueda para las bibliotecas de soporte de c32 (libcom32, libutil, etc.)
ruta debian-installer / amd64 / boot-Screens /
incluye debian-installer / amd64 / boot-Screens / menu.cfg
instalador de Debian predeterminado / amd64 / boot-Screens / vesamenu.c32
mensaje 0
tiempo de espera 50
```

Armado con la capacidad de iniciar cualquier máquina desde la red a través de PXE, puede aprovechar todas las características descritas en la sección 4.3 , " Instalaciones desatendidas " [página 91], que le permite hacer Arranque completo, preestablecimiento e instalación desatendida en múltiples computadoras sin arranque físico medios de comunicación. Además, no olvide la flexibilidad del parámetro de arranque preseed / url = http: // *server* / preseed. cfg (ni el uso del alias de url), que le permite configurar un archivo predeterminado basado en la red.

Page 281

10.2 Aprovechando la gestión de la configuración

Con la capacidad de instalar Kali en varias computadoras muy rápidamente, necesitará ayuda en gestionando esas máquinas después de la instalación. Puede aprovechar las herramientas de administración de configuración para administrar máquinas o configurar computadoras de reemplazo para cualquier estado deseado.

Kali Linux contiene muchas herramientas de administración de configuración populares que es posible que desee utilizar (*ansible* , *chef* , *títere* , *saltstack* , etc.) pero en esta sección, solo cubriremos *SaltStack* .

[2] https://saltstack.com

10.2.1. Configurando SaltStack

SaltStack es un servicio de gestión de configuración centralizado: un *maestro de sal* gestiona muchas *minas de sal iones* . Debe instalar el paquete *salt-master* en un servidor al que puedan acceder todos los hosts que desea administrar y *minar sal* en los hosts que desea administrar. Cada minion debe ser le dijeron dónde encontrar a su maestro. Simplemente edite / etc / salt / minion y configure la clave maestra en el DNS nombre (o dirección IP) del maestro de sal. Tenga en cuenta que Salt usa YAML como formato para su configuración archivos.

```
minion # vim / etc / salt / minion
minion # grep ^ master / etc / salt / minion
maestro: 192.168.122.105
```

Cada minion tiene un identificador único almacenado en / etc / salt / minion_id , que por defecto es su host- nombre. Este identificador de minion se usará en las reglas de configuración y, como tal, es importante configúrelo correctamente antes de que el minion abra su conexión con el maestro:

```
minion # echo kali-scratch> / etc / salt / minion_id
minion # systemctl enable salt-minion
minion # systemctl start salt-minion
```

Cuando el servicio *Salt Minion se* está ejecutando, intentará conectarse al Salt Master para intercambiar algunos claves criptográficas En el lado maestro, debes aceptar la clave que el minion está usando para identificarse para permitir que continúe la conexión. Las conexiones posteriores serán automáticas:

```
master # systemctl enable salt-master
master # systemctl start salt-master
master # salt-key - listar todos
Claves aceptadas:
Claves denegadas:
Claves no aceptadas:
kali-scratch
Claves rechazadas:
master # salt-key --aceptar kali-scratch
Se aceptarán las siguientes claves:
```


Página 282

```
Claves no aceptadas:
kali-scratch
¿Continuar? [n / Y] y
```

```
Clave para minion kali-scratch aceptado.
```

10.2.2. Ejecutando comandos en Minions

Tan pronto como los minions estén conectados, puedes ejecutar comandos desde el maestro:

```
master # salt '*' test.ping
kali-scratch:
    Cierto
kali-master:
    Cierto
```

Este comando pide a todos los minions (el '*' es un comodín dirigido a todos los minions) para ejecutar el ping función del módulo de ejecución de prueba. Esta función devuelve un valor Verdadero en caso de éxito y es un Una forma sencilla de garantizar que la conexión funciona entre el maestro y los distintos secuaces.

También puedes apuntar a un súbdito específico dando su identificador en el primer parámetro, o posiblemente un subconjunto de minions utilizando un comodín menos genérico (como '* -scratch' o 'kali- *'). Aquí hay un ejemplo de cómo ejecutar un comando de shell arbitrario en el minion kali-scratch:

```
master # salt kali-scratch cmd.shell 'uptime; uname -a '
kali-scratch:
    05:25:48 hasta 44 min, 2 usuarios, promedio de carga: 0.00, 0.01, 0.05
    Linux kali-scratch 4.5.0-kali1-amd64 # 1 SMP Debian 4.5.3-2kali1 (2016-05-09) x86_64
    GNU / Linux
```

Referencia del módulo de Salt Hay muchos módulos de ejecución disponibles para todo tipo de casos de uso. No lo haremos cúbrelos aquí, pero la lista completa está disponible en https://docs.saltstack.com/ es / latest / ref / modules / all / index.html. También puede obtener una descripción de todos los módulos de ejecución y sus funciones disponibles en un minion dado con la sal comando *minion* sys.doc . La ejecución de este comando devuelve una lista muy larga de funciones pero puede filtrar la lista pasando el nombre de una función o módulo con el prefijo por su módulo padre como parámetro:

```
master # salt kali-scratch sys.doc disk.usage
uso del disco:

    Devolver información de uso para volúmenes montados en este
    minion
```

Uno de los módulos más útiles es pkg, que es una abstracción del administrador de paquetes que se basa en gestor de paquetes apropiado para el sistema (apt-get para Debian y sus derivados como Kali).

El comando pkg.refresh_db actualiza la lista de paquetes (es decir, realiza la actualización de apt-get) mientras pkg.upgrade instala todas las actualizaciones disponibles (realiza apt-get upgrade o apt-get dist-upgrade , según las opciones recibidas). El comando pkg.list_upgrades enumera los operaciones de actualización pendientes (que realizaría pkg.upgrade dist_upgrade = True mando).

El módulo de servicio es una abstracción del administrador de servicios (systemd en el caso de Kali), que permite realiza todas las operaciones habituales de systemctl : service.enable , service.disable , service. inicio , service.stop , service.restart y service.reload :

```
master # salt '*' service.enable ssh
kali-scratch:
    Cierto
kali-master:
    Cierto
master # salt '*' service.start ssh
kali-master:
    Cierto
kali-scratch:
    Cierto
master # salt '*' pkg.refresh_db
kali-scratch:
    ----------
kali-master:
    ----------
master # salt '*' pkg.upgrade dist_upgrade = True
kali-scratch:
    ----------
    cambios:
```

```
          ----------
          archivos base:
              ----------
              nuevo:
                  1: 2016.2.1
              antiguo:
                  1: 2016.2.0
[...]
          zaproxy:
              ----------
              nuevo:
                  2.5.0-0kali1
              antiguo:
                  2.4.3-0kali3
      comentario:
      resultado:
          Cierto
```


Como muestra más concreta, puede configurar fácilmente un escaneo *Nmap* distribuido con *dnmap* . Después Después de instalar el paquete en todos los minions, inicias el servidor en una primera terminal:

```
server # salt '*' pkg.install dnmap
[...]
servidor # vim dnmap.txt
server # dnmap_server -f dnmap.txt
```

Suponiendo que la IP del servidor es 1.2.3.4, puede indicar a todos los secuaces que inicien un proceso de cliente que se conecta al servidor:

```
server # salt '*' cmd.run_bg template = jinja 'dnmap_client -s 1.2.3.4 -a {{grains.id}}'
kali-scratch:
      ----------
      pid:
          17137
[...]
```

Tenga en cuenta que el ejemplo usa cmd.run_bg para ejecutar el comando dnmap_client en segundo plano. No espere hasta que termine, ya que es un proceso de larga duración. Desafortunadamente, no se suicida correctamente cuando interrumpe el servidor para que tenga que limpiarlo:

```
server # salt '*' cmd.shell 'pkill -f dnmap_client'
```

10.2.3. Estados de sal y otras características

Si bien la ejecución remota es un componente importante, es solo una pequeña fracción de lo que SaltStack puede hacer.

Al configurar una nueva máquina, a menudo ejecuta muchos comandos y pruebas para determinar los detalles del sistema antes de la instalación. Estas operaciones se pueden formalizar en una configuración reutilizable plantillas llamadas *archivos de estado* . Las operaciones descritas en los archivos de estado se pueden realizar con un solo estado.aplicar comando salt.

Para ahorrar algo de tiempo, puede confiar en muchos archivos de estado listos para usar que han sido creados por comunidad y que se distribuyen en "Fórmulas de sal":

[2] https://docs.saltstack.com/en/latest/topics/development/conventions/formulas.html

Hay muchas otras características que se pueden combinar:

- Ejecución programada de acciones.
- Definir acciones en respuesta a eventos desencadenados por súbditos.
- Recolectar datos de minions

- Orquestación de una secuencia de operaciones en múltiples secuaces.
- Aplicar estados sobre SSH sin instalar el servicio de minería de sal
- Aprovisionamiento de sistemas en infraestructuras en la nube y su gestión.
- Y más

SaltStack es bastante amplio y no podemos cubrir todas las características aquí. De hecho, hay libros. dedicado por completo a SaltStack y la documentación en línea también es muy extensa. Revisalo si quieres aprender más sobre sus características:

[2] https://docs.saltstack.com/en/latest/

Si gestiona un número significativo de máquinas, le recomendamos que aprenda más sobre SaltStack ya que puede ahorrar una cantidad significativa de tiempo al implementar nuevas máquinas y lo hará ser capaz de mantener una configuración coherente en toda su red.

Para darle una idea de cómo es trabajar con archivos de estado, cubriremos un ejemplo simple: cómo habilitar el repositorio APT e instalar un paquete que cree en la sección 10.3.3, " Creando un repositorio de paquetes para APT "[página 269] y sección 10.3.2 , "Crear paquetes de configuración " [página 263]. También registrará una clave SSH en la cuenta de root para que pueda iniciar sesión de forma remota en caso de problemas

Por defecto, los archivos de estado se almacenan en / srv / salt en el maestro; son archivos estructurados YAML con una extensión .sls . Al igual que para ejecutar comandos, la aplicación de un estado depende de muchos módulos de estado:

[2] https://docs.saltstack.com/en/latest/topics/tutorials/starting_states.html

[2] https://docs.saltstack.com/en/latest/ref/states/all/

Su archivo /srv/salt/offsec.sls llamará a tres de esos módulos:

```
offsec_repository:
    pkgrepo.managed:
        - nombre: deb http://pkgrepo.offsec.com offsec-internal main
        - archivo: /etc/apt/sources.list.d/offsec.list
        - key_url: salt: //offsec-apt-key.asc
        - require_in:
            - pkg: valores predeterminados de offsec

valores predeterminados de offsec:
    paquete instalado

ssh_key_for_root:
    ssh_auth.present:
        - usuario: root
        - nombre: ssh-rsa AAAAB3NzaC1yc2 ... 89C4N rhertzog @ kali
```

El estado offsec_repository se basa en el módulo de estado pkgrepo. El ejemplo utiliza el administrado funcionar en ese módulo de estado para registrar un repositorio de paquetes. Con el atributo key_url, usted

avise a Salt que la clave GPG (blindada ASCII) requerida para verificar la firma del repositorio puede ir a /srv/salt/offsec-apt-key.asc en el maestro de sal. El atributo require_in garantiza que este estado se procese antes de los valores predeterminados de offsec, ya que este último necesita el repositorio configurado correctamente para poder instalar el paquete.

El estado offsec-defaults instala el paquete del mismo nombre. Esto muestra que el nombre de la La clave suele ser un valor importante para los estados, aunque siempre se puede anular con un nombre en- homenaje (como se hizo para el estado anterior). Para casos simples como este, esto es legible y conciso.

El último estado (ssh_key_for_root) agrega la clave SSH dada en el atributo de nombre a /root/.ssh/ Authorizedkeys (el usuario objetivo se establece en el atributo de usuario). Tenga en cuenta que hemos acortado el clave para facilitar la lectura aquí, pero debe poner la clave completa en el atributo de nombre.

Este archivo de estado se puede aplicar a un minion dado:

```
server # salt kali-scratch state.apply offsec
kali-scratch:
----------
          ID: offsec_repository
    Función: pkgrepo.managed
      Nombre: deb http://pkgrepo.offsec.com offsec-internal main
    Resultado: Verdadero
  Comentario: Repo 'deb configurado del paquete http://pkgrepo.offsec.com offsec-internal
              principal '
```

```
          Inicio: 06: 00: 15.767794
        Duración: 4707.35 ms
          Cambios:
                   ----------
                   repo:
                       deb http://pkgrepo.offsec.com offsec-internal main
----------
               ID: valores predeterminados de offsec
         Función: paquete instalado
           Resultado: Verdadero
          Comentario: Se instalaron / actualizaron los siguientes paquetes: offsec-defaults
          Inicio: 06: 00: 21.325184
        Duración: 19246.041 ms
          Cambios:
                   ----------
                   valores predeterminados de offsec:
                       ----------
                       nuevo:
                           1.0
                       antiguo:
----------
               ID: ssh_key_for_root
         Función: ssh_auth.present
```


Página 287

```
                Nombre: ssh-rsa AAAAB3NzaC1yc2 ... 89C4N rhertzog @ kali
              Resultado: Verdadero
            Comentario: se agregó la clave de host autorizada AAAAB3NzaC1yc2 ... 89C4N para el usuario root
            Inicio: 06: 00: 40.582539
          Duración: 62.103 ms
            Cambios:
                     ----------
                     AAAAB3NzaC1yc2 ... 89C4N:
                         Nuevo

Resumen de kali-scratch
------------
Triunfó: 3 (cambiado = 3)
Ha fallado:    0 0
------------
Total de estados ejecutados:    3
Tiempo total de ejecución: 24.015 s
```

También se puede asociar permanentemente al minion al grabarlo en /srv/salt/top.sls archivo, que utiliza el comando state.highstate para aplicar todos los estados relevantes en una sola pasada:

```
servidor # cat /srv/salt/top.sls
base:
    kali-scratch:
        - offsec
server # salt kali-scratch state.highstate
kali-scratch:
----------
               ID: offsec_repository
         Función: pkgrepo.managed
                Nombre: deb http://pkgrepo.offsec.com offsec-internal main
              Resultado: Verdadero
            Comentario: El repositorio de paquetes 'deb http://pkgrepo.offsec.com offsec-internal main' ya
                        configurado
            Inicio: 06: 06: 20.650053
          Duración: 62.805 ms
            Cambios:
----------
               ID: valores predeterminados de offsec
         Función: paquete instalado
           Resultado: Verdadero
          Comentario: el paquete offsec-defaults ya está instalado
          Inicio: 06: 06: 21.436193
        Duración: 385.092 ms
          Cambios:
----------
               ID: ssh_key_for_root
```

```
          Función: ssh_auth.present
                Nombre: ssh-rsa AAAAB3NzaC1yc2 ... 89C4N rhertzog @ kali
              Resultado: Verdadero
            Comentario: la clave de host autorizada AAAAB3NzaC1yc2 ... 89C4N ya está presente para
                        usuario root
              Inicio: 06: 06: 21.821811
            Duración: 1.936 ms
              Cambios:

Resumen de kali-scratch
------------
Triunfó: 3
Ha fallado:           0 0
------------
Total de estados ejecutados:              3
Tiempo total de ejecución: 449.833 ms
```

10.3 Ampliación y personalización de Kali Linux

A veces necesita modificar Kali Linux para que se ajuste a sus necesidades locales. La mejor manera de lograr
Este es un depósito de paquete propio que aloja las versiones modificadas de los paquetes de Kalipa.
que tenías que trabajar, como un paquete de vidrio suplementario que proporciona una configuración personalizada y un índice
software (no proporcionado por Kali Linux).

10.3.1. Forking Kali Packages

Por favor refiérase a la sección 9.1 , " Modificación de paquetes de Kali "[Página 222] para obtener explicaciones sobre este tema.

Todos los paquetes se pueden bifurcar si tiene una buena razón, pero debe saber que bifurcar un paquete
tiene un costo, ya que debe actualizarlo cada vez que Kali publica una actualización. Aquí están algunas
razones por las que es posible que desee bifurcar un paquete:

- Para agregar un parche para corregir un error o agregar una nueva función. Aunque en la mayoría de los casos, querrás
  envíe ese parche a los desarrolladores anteriores para que se corrija el error o se agregue la función
  en la fuente
- Compilarlo con diferentes opciones (suponiendo que haya buenas razones por las cuales Kali no lo hizo).
  compilarlo con esas opciones; de lo contrario, sería mejor discutir esto con los desarrolladores de Kali
  para ver si pueden habilitar las opciones deseadas).

Por el contrario, aquí hay algunas malas razones para bifurcar un paquete junto con sugerencias de cómo manejar
tu problema:

- Para modificar un archivo de configuración. Tienes múltiples opciones mejores, como usar la configuración
  gestión para instalar automáticamente un archivo de configuración modificado o instalar una configuración
  paquete de ración que colocará un archivo en un directorio de configuración (cuando esté disponible) o que
  desviar el archivo de configuración original.
- Actualización a una nueva versión de actualización. De nuevo, es mejor trabajar con desarrolladores hasta la fecha
  El paquete directamente en Debian o Kali. Con el modelo de lanzamiento continuo, las actualizaciones son más bien
  Rápido para llegar a los usuarios finales.

Entre todos los paquetes disponibles, hay algunos que son bloques de construcción de Kali Linux y que
podría ser interesante bifurcar en algunas situaciones:

- *kali-meta* : este paquete de fuentes construye todos los paquetes de *kali-linux-* * metapaquete y notablemente *kali-linux-completo* , que define qué paquetes están instalados en la imagen ISO predeterminada de Kali Linux.
- *escritorio-base* : este paquete fuente contiene varios archivos misceláneos que son utilizados por
  falla en instalaciones de escritorio. Considere bifurcar este paquete si desea mostrar su
  marca de la organización en el fondo predeterminado o cambiar el tema del escritorio.
- *kali-menu* : este paquete define la estructura del menú Kali y proporciona archivos .desktop

para todas las aplicaciones que deberían aparecer en el menú de Kali.

10.3.2. Crear paquetes de configuración

Ahora que hemos tocado el arranque PXE y discutido la gestión de la configuración con Salt-
La bifurcación de la pila y el paquete es hora de resumir estos procesos en un ejemplo práctico y
ampliar el escenario creando un paquete de configuración personalizado para implementar una configuración personalizada
a múltiples máquinas semiautomáticamente.

En este ejemplo, usted creará un paquete personalizado que establece upa y utiliza sus repositorios de paquetes
itory y la clave de firma GnuPG, distribuye una configuración de SaltStack, empuja un fondo personalizado,
y proporciona configuraciones de escritorio predeterminadas de manera unificada para todas sus instalaciones de Kali.

Esto puede parecer una tarea desalentadora (especialmente si echas un vistazo a Debian New Maintainer
Guía[1]) pero afortunadamente para nosotros, un paquete de configuración es principalmente un archivo sofisticado y
convertirlo en un paquete es bastante fácil.

Buscando en una muestra Paquete

Si desea buscar un paquete real que sea básicamente un paquete de configuración, consulte
eche un *vistazo al* paquete *kali-defaults* . No es tan simple como la muestra en esta sección, pero
tiene todas las características relevantes e incluso utiliza algunas técnicas avanzadas (como
`dpkg-divert`) para reemplazar archivos ya proporcionados por otros paquetes.

[1] https://www.debian.org/doc/manuals/maint-guide/

El paquete *offsec-defaults* contendrá algunos archivos:

- `/etc/apt/sources.list.d/offsec.list` : una entrada de `sources.list` para APT, que permite repositorio interno de paquetes de la compañía
- `/etc/apt/trusted.gpg.d/offsec.gpg` : la clave GnuPG utilizada para firmar repositorio de paquetes nal
- `/etc/salt/minion.d/offsec.conf` : aSaltStackconfigurationfiletoindicatewheretofind el maestro de sal
- `/usr/share/images/offsec/background.png` : una buena imagen de fondo con el Logotipo de seguridad ofensiva
- `/usr/share/glib-2.0/schemas/90_offsec-defaults.gschema.override` : un archivo providing configuraciones predeterminadas alternativas para el escritorio GNOME

Primero, cree un `directorio offsec-defaults-1.0` y coloque todos los archivos en ese directorio. Entonces corre
`dh_make --native` (del paquete *dh-make*) para agregar instrucciones de empaquetado de Debian, que
ser almacenado en un `subdirectorio debian` :

```
$ mkdir offsec-defaults-1.0; cd offsec-defaults-1.0
$ dh_make --native
Tipo de paquete: (single, indep, library, python)
[s / i / l / p]? yo
Dirección de correo electrónico : buxy@kali.org
Licencia : gpl3
Nombre del paquete : valores predeterminados de offsec
Nombre del mantenedor : Raphaël Hertzog
Versión : 1.0
Tipo de paquete : indep
Fecha : Jue, 16 jun 2016 18:04:21 +0200
¿Son correctos los detalles? [S / n / q] y
Actualmente no hay Makefile de nivel superior. Esto puede requerir ajustes adicionales
Hecho. Edite los archivos en el subdirectorio debian ahora.
```

Primero, se le solicita un tipo de paquete. En el ejemplo, seleccionamos *indep* , que indica
que este paquete fuente generará un único paquete binario que se puede compartir en todos los archivos
tecturas (Arquitectura: todas). *single* actúa como contraparte y produce un único paquete binario que
depende de la arquitectura de destino (Arquitectura: cualquiera). En este caso, *indep* es más relevante,
ya que el paquete solo contiene archivos de texto y ningún programa binario, por lo que puede usarse de manera similar
en computadoras de todas las arquitecturas. El tipo de *biblioteca* es útil para las bibliotecas compartidas, ya que necesitan

Siga las estrictas normas de embalaje. De manera similar, *python* debería restringirse a los módulos de Python.

Nombre del mantenedor y Dirección de correo electrónico

La mayoría de los programas involucrados en el mantenimiento de paquetes buscarán su nombre y dirección de correo electrónico en las variables de entorno DEBFULLNAME y DEBEMAIL o EMAIL . Definirlos, de una vez por todas, evita volver a escribirlos varias veces. Si tu habitual shell es Bash, es una simple cuestión de agregar las siguientes dos líneas en su ~ / .bashrc archivo. Por ejemplo:

```
export EMAIL = "buxy@kali.org"
export DEBFULLNAME = "Raphael Hertzog"
```

El comando dh_make creó un subdirectorio debian que contiene muchos archivos. Algunos son obligatorios en particular reglas , control , registro de cambios y derechos de autor . Los archivos con la extensión .ex son ex amplios archivos que se pueden usar modificándolos y eliminando la extensión. Cuando no son necesario, recomendamos eliminarlos. El archivo compat debe mantenerse, ya que es necesario para el correcto funcionamiento del conjunto de programas de *debhelper* (todos comenzando con el prefijo dh_) utilizado en varias etapas del proceso de compilación del paquete.

El archivo de copyright debe contener información sobre los autores de los documentos incluidos en el paquete y la licencia relacionada. Si la licencia predeterminada seleccionada por dh_make no le conviene, entonces debes editar este archivo. Aquí está la versión modificada del archivo de copyright:

```
Formato: https://www.debian.org/doc/packaging-manuals/copyright-format/1.0/
Nombre ascendente: valores predeterminados de offsec

Archivos: *
Copyright: 2016 seguridad ofensiva
Licencia: GPL-3.0 +

Licencia: GPL-3.0 +
  Este programa es software libre: puede redistribuirlo y / o modificarlo
  bajo los términos de la Licencia Pública General GNU publicada por
  Free Software Foundation, ya sea la versión 3 de la Licencia, o
  (a su elección) cualquier versión posterior.
  .
  Este paquete se distribuye con la esperanza de que sea útil,
  pero SIN NINGUNA GARANTÍA; sin siquiera la garantía implícita de
  COMERCIABILIDAD o APTITUD PARA UN PROPÓSITO EN PARTICULAR. Ver el
  Licencia pública general de GNU para más detalles.
  .
  Debería haber recibido una copia de la Licencia Pública General de GNU
  junto con este programa. Si no, vea <https://www.gnu.org/licenses/>.
  .
  En sistemas Debian, el texto completo de GNU General
  La licencia pública versión 3 se puede encontrar en "/ usr / share / common-licens / GPL-3".
```


El archivo de registro de cambios predeterminado es generalmente apropiado; reemplazando el "lanzamiento inicial" con un más explicación detallada debería ser suficiente:

```
offsec-defaults (1.0) inestable; urgencia = medio

    * Agregar el archivo de configuración de Salt Minion.
    * Agregue la entrada sources.list de APT y la clave GPG de confianza de APT.
    * Anular el esquema de configuración que define la imagen de fondo.

 - Raphaël Hertzog <buxy@kali.org> jue, 16 jun 2016 18:04:21 +0200
```

En el ejemplo, haremos cambios en el archivo de control . Cambiaremos el campo Sección a *misceláneo* y elimine los campos Página de inicio, Vcs-Git y Vcs-Browser. Por último, completaremos la Descripción

campo:

```
Fuente: offsec-defaults
Sección: misceláneo
Prioridad: opcional
Mantenedor: Raphaël Hertzog <buxy@kali.org>
Build-Depends: debhelper (> = 9)
Versión estándar: 3.9.8

Paquete: offsec-defaults
Arquitectura: todo
Depende: $ {misc: Depende}
Descripción: configuración predeterminada para seguridad ofensiva
  Este paquete contiene múltiples archivos para configurar computadoras
  propiedad de seguridad ofensiva.
  .
  Modifica notablemente:
    - Configuración de APT
    - configuración de salt-minion
    - la configuración de escritorio predeterminada
```

El archivo de reglas generalmente contiene un conjunto de reglas usadas para configurar, construir e instalar el software en un subdirectorio dedicado (llamado así por el paquete binario generado). El contenido de este El subdirectorio se archiva dentro del paquete Debian como si fuera la raíz del sistema de archivos. En este caso, los archivos se instalarán en el subdirectorio debian / offsec-defaults / . Por ejemplo, para terminar con un paquete que instala /etc/apt/sources.list.d/offsec.list , instale el archivo en debian / offsec-defaults / etc / apt / sources.list.d / offsec.list . El archivo de reglas se utiliza como Makefile , con algunos objetivos estándar (incluidos clean y binary, utilizados respectivamente para limpiar el directorio de origen y generar el paquete binario).

¿Qué es un archivo Makefile ? Es posible que haya notado el mensaje sobre el Makefile faltante al final de la salida dh_make y la mención de su similitud con el archivo de reglas . Un Makefile es un archivo de script utilizado por el programa make ; describe las reglas sobre cómo construir un conjunto de archivos el uno del otro en un árbol de dependencias. Por ejemplo, se puede construir un programa a partir de Un conjunto de archivos fuente. El archivo Makefile describe estas reglas en el siguiente formato:

```
destino: fuente1 fuente2 ...
        comando1
        comando2
```

La interpretación de dicha regla es la siguiente: si uno de los archivos fuente * es más reciente que el archivo de destino , entonces el destino debe ser generado, usando command1 y comando2 .

Tenga en cuenta que las líneas de comando deben comenzar con un carácter de tabulación; También tenga en cuenta que cuando una línea de comando comienza con un carácter de guión (-), la falla del comando no interrumpir todo el proceso.

Aunque este archivo es el corazón del proceso, contiene solo el mínimo necesario para ejecutar Un conjunto estándar de comandos proporcionados por la herramienta Debhelper . Tal es el caso de los archivos gene- Ayudado por dh_make . Para instalar la mayoría de sus archivos, le recomendamos configurar el comportamiento de Comando dh_install creando el siguiente archivo debian / offsec-defaults.install :

```
apt / offsec.list etc / apt / sources.list.d /
apt / offsec.gpg etc / apt / Trusted.gpg.d /
salt / offsec.conf etc / salt / minion.d /
images / background.png usr / share / images / offsec /
```

También puede usar esto para instalar el archivo de anulación de gsettings, pero debhelper proporciona un dedicado herramienta para esto (dh_installgsettings) para que pueda confiar en él. Primero, ponga su configuración en debian / offsec-defaults.gsettings-override :

```
[org.gnome.desktop.background]
opciones de imagen = 'zoom'
picture-uri = 'archivo: ///usr/share/images/offsec/background.png'
```

A continuación, anule la llamada dh_installgsettings en debian / rules para aumentar la prioridad a nivel esperado para una anulación de la organización (que es 90 según la página del manual):

```
#! / usr / bin / make -f
```

```
%:
	dh $ @

override_dh_installgsettings:
	dh_installgsettings --priority = 90
```


Page 294

En este punto, el paquete fuente está listo. Todo lo que queda por hacer es generar el paquete binario con el mismo método utilizado anteriormente para reconstruir paquetes: ejecute dpkg-buildpackage -us -uc desde el directorio offsec-defaults-1.0 :

```
$ dpkg-buildpackage -us -uc
dpkg-buildpackage: información: paquete fuente offsec-defaults
dpkg-buildpackage: información: fuente, versión 1.0
dpkg-buildpackage: información: distribución de origen inestable
dpkg-buildpackage: información: fuente modificada por Raphaël Hertzog <buxy@kali.org>
dpkg-buildpackage: información: arquitectura de host amd64
  dpkg-source --before-build offsec-defaults-1.0
  fakeroot debian / reglas limpias
dh limpio
	dh_testdir
	dh_auto_clean
	dh_clean
  dpkg-source -b offsec-defaults-1.0
dpkg-source: info: usando el formato fuente '3.0 (nativo)'
dpkg-source: info: compilando offsec-defaults en offsec-defaults_1.0.tar.xz
dpkg-source: info: compilando offsec-defaults en offsec-defaults_1.0.dsc
  construcción de debian / rules
dh construir
	dh_testdir
	dh_update_autotools_config
	dh_auto_configure
	dh_auto_build
	dh_auto_test
  fakeroot debian / rules binary
dh binario
	dh_testroot
	dh_prep
	dh_auto_install
	dh_install
	dh_installdocs
	dh_installchangelogs
	debian / rules override_dh_installgsettings
make [1]: Entrando en el directorio '/home/rhertzog/kali/kali-book/samples/offsec-defaults-1.0'
dh_installgsettings --priority = 90
make [1]: Saliendo del directorio '/home/rhertzog/kali/kali-book/samples/offsec-defaults-1.0'
	dh_perl
	dh_link
	dh_strip_nondeterminism
	dh_compress
	dh_fixperms
	dh_installdeb
	dh_gencontrol
	dh_md5sums
```


Page 295

```
	dh_builddeb
dpkg-deb: compilando el paquete 'offsec-defaults' en '../offsec-defaults_1.0_all.deb'.
  dpkg-genchanges> ../ offsec-defaults_1.0_amd64.changes
dpkg-genchanges: información: incluye el código fuente completo en la carga
  dpkg-source --after-build offsec-defaults-1.0
dpkg-buildpackage: información: carga completa;  Paquete nativo de Debian (se incluye fuente completa)
```

10.3.3. Crear un repositorio de paquetes para APT

Ahora que tiene un paquete personalizado, puede distribuirlo a través de un repositorio de paquetes APT. Use `reprepro` para crear el repositorio deseado y llenarlo. Esta herramienta es bastante poderosa y es Vale la pena leer la página del manual.

Un repositorio de paquetes generalmente está alojado en un servidor. Para separarlo adecuadamente de otros servicios ejecutándose en el servidor, es mejor crear un usuario dedicado a este servicio. En el usuario dedicado cuenta, podrá alojar los archivos del repositorio y también la clave GnuPG que se utilizará para firmar el repositorio de paquetes:

```
# apt install reprepro gnupg
[...]
# adduser --system --group pkgrepo
Agregando el usuario del sistema 'pkgrepo' (UID 136) ...
Agregar nuevo grupo 'pkgrepo' (GID 142) ...
Añadiendo un nuevo usuario 'pkgrepo' (UID 136) con el grupo 'pkgrepo' ...
Creando el directorio de inicio '/ home / pkgrepo' ...
# chown pkgrepo $ (tty)
# su - -s / bin / bash pkgrepo
$ gpg --gen-key
gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc.
Esto es software libre: usted es libre de cambiarlo y redistribuirlo.
NO HAY GARANTÍA, en la medida permitida por la ley.

gpg: creado el directorio '/home/pkgrepo/.gnupg'
gpg: nuevo archivo de configuración '/home/pkgrepo/.gnupg/dirmngr.conf' creado
gpg: nuevo archivo de configuración '/home/pkgrepo/.gnupg/gpg.conf' creado
gpg: keybox '/home/pkgrepo/.gnupg/pubring.kbx' creado
Nota: Use "gpg --full-gen-key" para un cuadro de diálogo de generación de claves con todas las funciones.

GnuPG necesita construir una identificación de usuario para identificar su clave.

Nombre real: Clave de firma del repositorio de seguridad ofensiva
Dirección de correo electrónico: repoadmin@offsec.com
Seleccionó esta ID DE USUARIO:
        "Clave de firma del repositorio de seguridad ofensiva <repoadmin@offsec.com>"
```



```
¿Cambiar (N) ame, (E) mail o (O) kay / (Q) uit? o
Necesitamos generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra acción (escriba en el teclado, mueva el mouse, utilice el
discos) durante la primera generación; esto da el número aleatorio
Generador una mejor oportunidad de ganar suficiente entropía.
[...]
gpg: /home/pkgrepo/.gnupg/trustdb.gpg: creado trustdb
gpg: clave B4EF2D0D marcada como finalmente confiable
gpg: se creó el directorio '/home/pkgrepo/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación almacenado como '/home/pkgrepo/.gnupg/openpgp-revocs.d/
        ¯ F8FE22F74F1B714E38DA6181B27F74F7B4EF2D0D.rev '
Clave pública y secreta creada y firmada.

gpg: comprobando el trustdb
gpg: marginales necesarios: 3 completos necesarios: 1 modelo de confianza: PGP
gpg: profundidad: 0 válido: 1 firmado: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
pub     rsa2048 / B4EF2D0D 2016-06-17 [S]
        Huella digital clave = F8FE 22F7 4F1B 714E 38DA 6181 B27F 74F7 B4EF 2D0D
uid             [ultimate] Clave de firma del repositorio de seguridad ofensiva <repoadmin@offsec.com>
sub     rsa2048 / 38035F38 2016-06-17 []
```

Tenga en cuenta que cuando se le solicite una frase de contraseña, debe ingresar un valor vacío (y confirmar que no desea proteger su clave privada) ya que desea poder firmar el repositorio no interactivamente. Notas sobre que `gpg` requiere acceso de escritura al terminal para que se pueda promulgar para una frase de contraseña: es por eso que cambió la propiedad de la terminal virtual (que es propiedad por root ya que inicialmente se conectó como ese usuario) antes de iniciar un shell como pkgrepo.

Ahora puede comenzar a configurar el repositorio. Es necesario un directorio dedicado para reprogramar y dentro de ese directorio debe crear un archivo `conf / distributions` que documente qué distribución Las opciones están disponibles en el repositorio de paquetes:

```
$ mkdir -p reprepro / conf
$ cd reprepro
$ cat> conf / distribuciones << FIN
Nombre clave: offsec-internal
AlsoAcceptFor: inestable
Origen: seguridad ofensiva
```

Descripción: Paquetes internos de Offsec
Arquitecturas: fuente amd64 i386
Componentes: principal
Firmar con: F8FE22F74F1B714E38DA6181B27F74F7B4EF2D0D
FINAL

Los campos obligatorios son Nombre clave, que da el nombre de la distribución, Arquitecturas, que indica qué arquitecturas estarán disponibles en la distribución (y aceptadas en el lado de entrada), y Componentes, que indica los diversos componentes disponibles en la distribución (com

Page 297

los componentes son una especie de subsección de la distribución, que se puede habilitar por separado en los APT fuentes.lista). Los campos Origen y Descripción son puramente informativos y se copian tal cual en el archivo de lanzamiento . El campo SignWith le pide a reprepro que firme el repositorio con la clave GnuPG cuyo identificador aparece en la lista (coloque aquí la huella digital completa para asegurarse de usar la clave correcta y no otro que se desplaza sobre el identificador de corta duración). El también Aceptar configuración no es necesario pero los botones es posible procesar archivos .changes cuyo campo Distribución tiene un valor listado aquí (sin esto, solo aceptaría el nombre en clave de la distribución en ese campo).

Con esta configuración básica en su lugar, puede dejar que reprepro genere un repositorio vacío:

```
$ reprepro export
Exportando índices ...
$ encontrar.
.
./db
./db/version
./db/references.db
./db/contents.cache.db
./db/checksums.db
./db/packages.db
./db/release.caches.db
./conf
./conf/distributions
./dists
./dists/offsec-internal
./dists/offsec-internal/Release.gpg
./dists/offsec-internal/Release
./dists/offsec-internal/main
./dists/offsec-internal/main/source
./dists/offsec-internal/main/source/Release
./dists/offsec-internal/main/source/Sources.gz
./dists/offsec-internal/main/binary-amd64
./dists/offsec-internal/main/binary-amd64/Packages
./dists/offsec-internal/main/binary-amd64/Release
./dists/offsec-internal/main/binary-amd64/Packages.gz
./dists/offsec-internal/main/binary-i386
./dists/offsec-internal/main/binary-i386/Packages
./dists/offsec-internal/main/binary-i386/Release
./dists/offsec-internal/main/binary-i386/Packages.gz
./dists/offsec-internal/InRelease
```

Como puede ver, reprepro creó la metainformación del repositorio en un subdirectorio dists . Eso también inicializó una base de datos interna en un subdirectorio db .

Ahora es el momento de agregar su primer paquete. Primero, copie los archivos generados por la compilación de offsec-valores predeterminados paquetes (offsec-defaults_1.0.dsc , offsec-defaults_1.0.tar.xz ,

Page 298

offsec-defaults_1.0_all.deb y offsec-defaults_1.0_amd64.changes) en / tmp en el servidor que aloja el repositorio de paquetes y solicite a reprepro que incluya el paquete:

```
$ reprepro incluye offsec-internal /tmp/offsec-defaults_1.0_amd64.changes
Exportando índices ...
$ encontrar grupo
piscina
```

piscina / principal
piscina / principal / o

pool / main / o / offsec-defaults

pool / main / o / offsec-defaults / offsec-defaults_1.0.dsc

pool / main / o / offsec-defaults / offsec-defaults_1.0.tar.xz

pool / main / o / offsec-defaults / offsec-defaults_1.0_all.deb

Como se puede ver, se añadió a los archivos en su propio almacén de paquetes en una piscina subdirectorio.

Los directorios dists y pool son los dos directorios que debe poner a disposición (públicamente) sobre HTTP para finalizar la configuración de su repositorio APT. Contienen todos los archivos que APT querrá descargar.

Suponiendo que desea alojar esto en un host virtual llamado pkgrepo.offsec.com, puede crear atethefollowingApacheconfigurationfile, guardarlo en / etc / apache2 / sites-available / pkgrepo.

offsec.com.conf , y habilítelo con a2ensite pkgrepo.offsec.com):

```
<VirtualHost *: 80>
        ServerName pkgrepo.offsec.com
        ServerAdmin repoadmin@offsec.com

        ErrorLog /var/log/apache2/pkgrepo.offsec.com-error.log
        CustomLog /var/log/apache2/pkgrepo.offsec.com-access.log "% h% l% u% t \"% r \ "%> s% O"

        DocumentRoot / home / pkgrepo / reprepro

        <Directorio "/ home / pkgrepo / reprepro">
                Opciones Índices FollowSymLinks MultiViews
                Requerir todo otorgado
                Permitir anular todo
        </Directory>
</VirtualHost>
```

Y la entrada correspondiente de sources.list para agregar en máquinas que necesitan paquetes de este el repositorio se vería así:

```
deb http://pkgrepo.offsec.com offsec-internal main

# Habilite la siguiente línea si también desea acceder a los paquetes fuente
# deb-src http://pkgrepo.offsec.com offsec-internal main
```

Su paquete ya está publicado y debería estar disponible para sus hosts en red.

Aunque esta ha sido una configuración larga, el "trabajo pesado" ahora se ha completado. Puedes arrancar tu NetworkedmachinesviaPXE, instala una versión personalizada de Kali Linux sin interacción gracias a una preselección entregada en red, configure SaltStack para administrar sus configuraciones (y controlar minions!), cree paquetes personalizados bifurcados y distribúyalos a través de su propio paquete-repositorio de edad. Esto proporciona gestión centralizada y control a nivel empresarial sobre múltiples Instalaciones de Kali Linux. En resumen, ahora puede implementar rápidamente sistemas preconfigurados de Kali altamente seguros pensado para sus necesidades específicas y mantenerlas sincronizadas gracias a la función de Kali (semiautomática) cancelación de todas las actualizaciones de paquetes.

10.4 Resumen

Kali Linux escala más allá de las implementaciones de escritorio a mediana o gran escala e incluso a nivel de sorpresa En este capítulo, cubrimos cómo centralizar la administración de múltiples instalaciones de Kali con SaltStack, lo que le permite implementar rápidamente sistemas Kali altamente seguros preconfigurados para sus necesidades específicas También revelamos cómo puedes mantenerlos sincronizados gracias a Kali's (semiautomática) instalación de actualizaciones de paquetes.

Hablamos de la bifurcación de paquetes, que le permite crear su propio distribuible personalizado paquetes fuente.

En resumen, repasemos los pasos principales necesarios para establecer Maestros de sal y súbditos, que le permite el control remoto y la configuración de hosts remotos.

Consejos resumidos:

- Arrancar la máquina desde la red con PXE, con al menos un servidor de archivos TFTP, un DHCP / BOOTP servidor (y un servidor web para la preselección de debconf). *dnsmasq* maneja tanto DHCP como TFTP, y el servidor web *apache2* viene preinstalado (pero deshabilitado) en Kali.
- El manual de *instalación de* Debian *cubre la* configuración de *isc-dhcp-server* y *tftpd-hpa para* PXEboot-En g:

[2] https://www.debian.org/releases/stable/amd64/ch04s05.html

• *dnsmasq* se configura a través de /etc/dnsmasq.conf . Una configuración básica consiste solo en algunas líneas clave:

```
# Interfaz de red para manejar
interfaz = eth0
# Opciones de DHCP
# Rango de IP para asignar
dhcp-range = 192.168.101.100,192.168.101.200,12h
# Gateway para anunciar a los clientes
dhcp-option = opción: enrutador, 192.168.101.1
# Servidores DNS para anunciar a los clientes
dhcp-option = opción: dns-server, 8.8.8.8,8.8.4.4
# Archivo de inicio para anunciar a los clientes
```



```
dhcp-boot = pxelinux.0
# Opciones TFTP
enable-tftp
# Directorio de archivos de alojamiento para servir
tftp-root = / tftpboot /
```

• Desempaquete los archivos de arranque de instalación de 32 bits (i386), 64 bits (amd64), estándar o gráfico (gtk) de el archivo Kali en / tftpboot / . Los archivos se pueden encontrar aquí:

[2] http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images / netboot / gtk / netboot.tar.gz

[2] http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/images / netboot / netboot.tar.gz

[2] http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images / netboot / gtk / netboot.tar.gz

[2] http://http.kali.org/dists/kali-rolling/main/installer-i386/current/images / netboot / netboot.tar.gz

```
# mkdir / tftpboot
# cd / tftpboot
# wget http://http.kali.org/dists/kali-rolling/main/installer-amd64/current/
      images / netboot / netboot.tar.gz
# tar xf netboot.tar.gz
```

• Opcionalmente, modifique txt.cfg para parámetros preestablecidos o tiempos de espera personalizados. Ver sección 4.3 , " Instalaciones desatendidas"[Página 91]. A continuación, puede aprovechar la gestión de la configuración. herramientas para administrar máquinas o configurar computadoras remotas a cualquier estado deseado.

• SaltStack es un servicio de administración de configuración centralizado: un maestro de Salt administra muchos Minions de sal. Instale el paquete *salt-master* en un servidor accesible y *salt-minion* en man-anfitriones de edad.

• Edite el archivo de configuración / etc / salt / minion con formato YAML y configure la clave maestra en el DNS nombre (o dirección IP) del maestro de sal.

• Establecer el identificador único de minion en / etc / salt / minion_id :

```
minion # echo kali-scratch> / etc / salt / minion_id
minion # systemctl enable salt-minion
minion # systemctl start salt-minion
```

• Seguirá el intercambio de claves. En el maestro, acepta la clave de identificación de minion. Subsecuente las conexiones serán automáticas:

```
master # systemctl enable salt-master
master # systemctl start salt-master
master # salt-key - listar todos
```



```
Claves aceptadas:
Claves denegadas:
Claves no aceptadas:
```

kali-scratch
Claves rechazadas:
master # **salt-key --aceptar kali-scratch**
Se aceptarán las siguientes claves:
Claves no aceptadas:
kali-scratch
¿Continuar? [n / Y] **y**
Clave para minion kali-scratch aceptado.

• Una vez que los minions están conectados, puedes ejecutar comandos desde el maestro. Examen-
ples:

master # **salt '*' test.ping**
kali-scratch:
Cierto
kali-master:
Cierto
master # **salt kali-scratch cmd.shell 'uptime; uname -a '**
master # **salt kali-scratch sys.doc '**
master # **salt '*' service.enable ssh**
[...]
master # **salt '*' service.start ssh**
[...]
master # **salt '*' pkg.refresh_db**
[...]
master # **salt '*' pkg.upgrade dist_upgrade = True**
server # **salt '*' cmd.shell 'pkill -f dnmap_client'**

• La lista completa de módulos de ejecución se puede encontrar en https://docs.saltstack.com/en/
latest / ref / modules / all / index.html.

• Utilice archivos de estado de Salt (plantillas de configuración reutilizables) para programar acciones, recopilar datos o-
Chestrate secuencias de operaciones en múltiples secuaces, aprovisione sistemas en la nube y traiga
bajo administración, y más. Ahorre tiempo con fórmulas de sal predefinidas:

[2] https://docs.saltstack.com/en/latest/topics/development/conventions/
formulas.html

• Cuando llegue el momento del paquete de trabajo, primero decida que es una falta sin marcar. Allí
Hay ventajas y desventajas significativas. Revíselos cuidadosamente. El *kali-meta* , *escritorio-*
Los paquetes *base* y *kali-menu* son opciones interesantes y probables. El proceso de bifurcar un
El paquete puede ser desalentador y es difícil de resumir.

Página 302

Ahora que hemos cubierto todas las bases en términos de instalación, configuración, personalización,
y despliegue de Kali Linux, pasemos al papel de Kali Linux en el campo de la Información
Seguridad.

Palabras clave

Tipos de evaluaciones
Vulnerabilidad
evaluación
Conformidad
prueba de penetración
Tradicional
prueba de penetración
Solicitud
evaluación
Tipos de ataques.
Negación de servicio
Corrupción de la memoria
Vulnerabilidades web
Ataques de contraseña
Ataques del lado del cliente

Capítulo 11

Introducción a Seguridad Evaluaciones

Contenido

Kali Linux en una evaluación 281
Tipos de evaluaciones 283
Formalización de la evaluación 293
Tipos de ataques 294
Resumen 297

Hemos cubierto muchas características específicas de Kali Linux hasta este punto, por lo que debe tener una sólida comprensión de lo que hace especial a Kali y cómo realizar una serie de tareas complejas.

Sin embargo, antes de utilizar Kali, hay algunos conceptos relacionados con las evaluaciones de seguridad que usted debe comprender. En este capítulo, presentaremos estos conceptos para comenzar y proporcione referencias que lo ayudarán si necesita usar Kali para realizar una evaluación de seguridad.

Para empezar, vale la pena tomarse un tiempo para explorar exactamente qué significa "seguridad" cuando se trata con sistemas de información. Cuando intentas asegurar un sistema de información, te enfocas en tres atributos primarios del sistema:

- *Confidencialidad* : pueden los actores que no deberían tener acceso al sistema o acceso a la información El sistema o la información?
- *Integridad* : ¿se pueden modificar los datos o el sistema de alguna manera que no se pretende?
- *Disponibilidad* : ¿se puede acceder a los datos o al sistema cuándo y cómo se pretende que sea?

Juntos, estos conceptos forman la tríada CIA (Confidencialidad, Integridad, Disponibilidad) y en gran parte, son los elementos principales en los que se centrará al asegurar un sistema como parte del estándar implementación, mantenimiento o evaluación.

También es importante tener en cuenta que, en algunos casos, puede estar mucho más preocupado por un aspecto de la tríada de la CIA que otros. Por ejemplo, si tiene un diario personal que contiene más pensamientos secretos, la confidencialidad de la revista puede ser mucho más importante para usted que

integridad o la disponibilidad. En otras palabras, es posible que no le preocupe tanto si se puede escribir en el diario (en lugar de leerlo) o si el diario es o no siempre accesible. Por otro lado, si está asegurando un sistema que rastrea las recetas médicas, el La integridad de los datos será muy crítica. Si bien es importante evitar que otras personas lean saber qué medicamentos usa alguien y es importante que pueda acceder a esta lista de medicamentos, si alguien pudiera cambiar el contenido del sistema (alterando la integridad), podría provocar resultados que amenazan la vida.

Cuando esté descubriendo un problema de un hombre del sistema, tendrá que considerar cuál de estos tres conceptos, o en qué combinación de ellos, cae el problema. Esto te ayuda a entender el problema de una manera más integral y le permite clasificar los problemas y responder en consecuencia. Es posible identificar vulnerabilidades que afectan a uno o varios elementos de La tríada de la CIA. Para usar una aplicación web con una vulnerabilidad de inyección SQL como ejemplo:

- *Confidencialidad* : una vulnerabilidad de inyección SQL que permite a un atacante extraer el contenido completo carpas de la aplicación web, lo que les permite tener acceso completo para leer todos los datos, pero no capacidad de cambiar la información o deshabilitar el acceso a la base de datos.
- *Integridad* : una vulnerabilidad de inyección SQL que permite a un atacante cambiar la información existente. mation en la base de datos. El atacante no puede leer los datos o impedir que otros accedan la base de datos.

- *Disponibilidad* : una vulnerabilidad de inyección SQL que inicia una consulta de larga duración, que consume un Gran cantidad de recursos en el servidor. Esta consulta, cuando se inicia varias veces, conduce a una situación de denegación de servicio (DoS). El atacante no tiene capacidad para acceder o cambiar datos, pero puede evitar que usuarios legítimos accedan a la aplicación web.
- *Múltiple* : una vulnerabilidad de inyección SQL conduce a un acceso completo de shell interactivo a la operación del host. sistema de borrado que ejecuta la aplicación web. Con este acceso, el atacante puede violar el La confidencialidad del sistema mediante el acceso a los datos que ellos quieran, comprometen la integridad de el sistema al alterar los datos y, si así lo eligen, destruir la aplicación web, lo que lleva a un compromiso de la disponibilidad del sistema.

Los conceptos detrás de la tríada de la CIA no son demasiado complicados, y de manera realista son elementos que usted están trabajando intuitivamente, incluso si no lo reconocen. Sin embargo, es importante tener en cuenta interactúe con los conceptos para ayudarlo a reconocer dónde dirigir sus esfuerzos. Este concepto Foundation lo ayudará con la identificación de los componentes críticos de sus sistemas y la cantidad de esfuerzo y recursos que vale la pena invertir en corregir los problemas identificados.

Otro concepto que abordaremos en detalle es el *riesgo* , y cómo está compuesto de *amenazas* y *vulnerabilidades. bilidades* . Estos conceptos no son demasiado complejos, pero es fácil equivocarse. Cubriremos estos conceptos en detalle más adelante, pero a un alto nivel, es mejor pensar en el *riesgo* como lo que está tratando de evitar que suceda, *amenaza* como quién te lo haría y *vulnerabilidad* como lo que les permite hazlo. Los controles pueden colocarse en el lugar para abordar la vulnerabilidad o amenaza, con el objetivo de emitir el riesgo.

Por ejemplo, cuando visita algunas partes del mundo, puede *correr* un *riesgo* considerable de contraer malaria. Esto se debe a que la *amenaza* de los mosquitos es muy alta en algunas áreas, y usted está casi ciertamente no es inmune a la malaria. Afortunadamente, puedes controlar la *vulnerabilidad* con medicamentos e intente controlar la *amenaza* con el uso de repelente de insectos y mosquiteros. Con controles En lugar de abordar tanto la *amenaza* como la *vulnerabilidad* , puede ayudar a garantizar que el *riesgo* no actualizar.

11.1 Kali Linux en una evaluación

Al prepararse para usar Kali Linux en el campo, primero debe asegurarse de tener un trabajo limpio y funcional instalación. Un error común que cometen muchos profesionales de seguridad novatos es usar un solo instalación en múltiples evaluaciones. Este es un problema por dos razones principales:

- En el transcurso de una evaluación, a menudo instalará manualmente, ajustará o de lo contrario Cambia tu sistema. Estos cambios únicos pueden ponerlo en funcionamiento rápidamente o resolver un problema particular, pero son difíciles de seguir; hacen que su sistema sea más difícil de mantener; y complican las configuraciones futuras.
- Cada evaluación de seguridad es única. Dejar notas, código y otros cambios puede conducir a confusión, o peor, contaminación cruzada de los datos del cliente.

Es por eso que es muy recomendable comenzar con una instalación limpia de Kali y por qué tener una La versión personalizada de Kali Linux que está lista para la instalación automatizada se amortiza rápidamente. Estar seguro para volver a la sección 9.3, " Creación de imágenes ISO de Kali Live personalizadas " [página 237] y sección 4.3 , " Instalaciones desatendidas " [página 91] sobre cómo hacer esto, ya que cuanto más se automatiza hoy, el menos tiempo pierdes mañana.

Todos tienen diferentes requisitos en cuanto a cómo les gusta que Kali Linux se configure cuando están en el campo, pero hay algunas recomendaciones universales que realmente desea seguir. Primero, considere usar una instalación encriptada como se documenta en la sección 4.2.2 , " Instalación en un FullyEncryptedFileSystem"[Página85]. Esto protegerá sus datos en la máquina física, que es un salvavidas si alguna vez le roban su computadora portátil.

Para mayor seguridad durante el viaje, es posible que desee introducir la clave de descifrado (consulte " Agregar una bomba nuclear Contraseña para mayor seguridad "[página 246]) después de haber enviado una copia (encriptada) de la clave a un trabajador en la oficina. De esa manera, sus datos estarán seguros hasta que regrese a la oficina donde pueda restaurar la computadora portátil con la clave de descifrado.

Otro elemento que debe comprobarse dos veces es la lista de paquetes que ha instalado. Considerar qué herramientas podría necesitar para el trabajo que se propone realizar. Por ejemplo, si eres emprender una evaluación de seguridad inalámbrica, puede considerar instalar el *kali-linux-wireless* metapaquete, que contiene todas las herramientas de evaluación inalámbrica disponibles en Kali Linux, o una web se acerca la evaluación de la aplicación, puede instalar todas las pruebas de aplicaciones web disponibles herramientas con el metapaquete *kali-linux-web* . Es mejor asumir que no tendrá acceso fácil a Internet mientras realiza una evaluación de seguridad, así que asegúrese de prepararse lo más posible por adelantado.

Por la misma razón, es posible que desee revisar la configuración de su red (consulte la sección 5.1, " Config-durante la red"[Página 104] y sección 7.3, " Asegurando los servicios de red "[Página 153]). Doble-verifique su configuración de DHCP y revise los servicios que escuchan en su dirección IP asignada. Estas configuraciones pueden tener un impacto crítico para su éxito. No puedes evaluar lo que no puedes ver y los servicios de escucha excesivos pueden marcar su sistema y hacer que se apague antes de recibir empezado.

Si su función implica investigar las intrusiones de la red, preste mucha atención a su conjunto de red: tings es aún más importante y debe evitar alterar los sistemas afectados. Un personalizado la versión de Kali con el metapaquete *kali-linux-forense* iniciado en modo forense no se auto-monte discos de forma matemática o use una partición de intercambio. De esta manera, puede ayudar a mantener la integridad de el sistema bajo análisis mientras hace uso de las muchas herramientas forenses disponibles en Kali Linux.

Es fundamental que prepare adecuadamente su instalación de Kali Linux para el trabajo. Encontrarás que Un entorno Kali limpio, eficiente y efectivo siempre hará que todo lo que sigue sea mucho más suave

11.2 Tipos de evaluaciones

Ahora que se ha asegurado de que su entorno Kali está listo, el siguiente paso es definir exactamente qué tipo de evaluación está realizando. En el nivel más alto, podemos describir cuatro tipos de evaluaciones: una *evaluación de vulnerabilidad* , una *prueba de cumplimiento* , una *prueba de penetración tradicional* y una *aplicación evaluación ción* . Un compromiso puede involucrar varios elementos de cada tipo de evaluación, pero es vale la pena describirlos con cierto detalle y explicar su relevancia para su compilación Kali Linux y medio ambiente.

Antes de profundizar en los diferentes tipos de evaluaciones, es importante notar primero la diferencia entre una vulnerabilidad y un exploit.

Una *vulnerabilidad* se define como una falla que, cuando se aprovecha, comprometerá la confianza. parcialidad, integridad o disponibilidad de un sistema de información. Hay muchos tipos diferentes de vulva Nerabilidades que se pueden encontrar, incluyendo:

- Inclusión de archivos : vulnerabilidades de inclusión de archivos en las aplicaciones web le permite *incluir* el contenido de un archivo local o remoto en el cálculo de un programa. Por ejemplo, una web la aplicación puede tener una función de "Mensaje del día" que lee el contenido de un archivo y

incluye en la página web para mostrar al usuario. Cuando se programa este tipo de característica incorrectamente, puede permitir que un atacante modifique su solicitud web para obligar al sitio a incluir El contenido de un archivo de su elección.

- Inyección SQL: una inyección SQL[2] ataque es uno donde las rutinas de validación de entrada para el se omiten los programas, lo que permite que un atacante proporcione comandos SQL para el programa de destino gramo a ejecutar. Esta es una forma de ejecución de comando que puede conducir a una seguridad potencial cuestiones.
- Desbordamiento de búfer: un desbordamiento de búfer [3] es una vulnerabilidad que omite la ruta de validación de entrada dientes para escribir datos en la memoria adyacente de un búfer. En algunos casos, esa memoria adyacente la ubicación puede ser crítica para la operación del programa objetivo y el control del código ejecutable Se puede obtener precaución mediante la manipulación cuidadosa de los datos de memoria sobrescritos.
- Condiciones de carrera: una condición de carrera [4] es una vulnerabilidad que aprovecha la dependencia del tiempo. deficiencias en un programa. En algunos casos, el flujo de trabajo de un programa depende de un secuencia de eventos a ocurrir. Si puede alterar esta secuencia de eventos, eso puede conducir a una vulnerabilidad.

Un *exploit* , por otro lado, es un software que, cuando se usa, aprovecha una vulnerabilidad específica. capacidad, aunque no todas las vulnerabilidades son explotables. Dado que un exploit debe cambiar una ejecución proceso, obligándolo a realizar una acción no deseada, la creación de exploits puede ser compleja. Además, Hay una serie de tecnologías anti-exploit en las plataformas informáticas modernas que han sido

[1] https://en.wikipedia.org/wiki/File_inclusion_vulnerability
[2] https://en.wikipedia.org/wiki/SQL_injection
[3] https://en.wikipedia.org/wiki/Buffer_overflow
[4] https://en.wikipedia.org/wiki/Race_condition

diseñado para aprovechar las vulnerabilidades de explotación , como DataExecutionPrevention[5] (DEP) y Dirección del espacio de diseño de aleatorización [6] (ASLR). Sin embargo, solo porque no se conoce públicamente explotar para una vulnerabilidad específica, eso no significa que uno no existe (o que uno no puede ser creado). Por ejemplo, muchas organizaciones venden exploits comercializados que nunca se realizan público, por lo que todas las vulnerabilidades deben tratarse como potencialmente explotables.

11.2.1. Evaluación de vulnerabilidad

Una *vulnerabilidad* se considera una debilidad que podría usarse de alguna manera para comprometer la confidencialidad, integridad o disponibilidad de un sistema de información. En una evaluación de vulnerabilidad, su objetivo es crear un inventario simple de vulnerabilidades descubiertas dentro del *entorno objetivo ronment* . Este concepto de un entorno objetivo es extremadamente importante. Debes asegurarte de quedarte dentro del alcance de la red objetivo de su cliente y los objetivos requeridos. Arrastrándose fuera del El alcance de una evaluación puede causar una interrupción del servicio, una violación de la confianza con su cliente o acción legal contra usted y su empleador.

Debido a su relativa simplicidad, una prueba de vulnerabilidad a menudo se completa en entornos más maduros. regularmente como parte de demostrar su debida diligencia. En la mayoría de los casos, una herramienta automatizada, como los del Análisis de vulnerabilidad[7] y aplicaciones web [8] categorías de Kali Tools sitio y menú de aplicaciones de escritorio Kali, se utiliza para descubrir sistemas en vivo en un entorno de destino, Identificar los servicios de escucha y enumerarlos para descubrir tanta información como sea posible. como el software del servidor, la versión, la plataforma, etc.

Esta información es verificada por firmas conocidas de posibles problemas o vulnerabilidades. Estas Las firmas están formadas por combinaciones de puntos de datos que están destinadas a representar problemas conocidos. Se utilizan múltiples puntos de datos, porque cuantos más puntos de datos utilice, más precisa será la identidad. tificación Existe un gran número de puntos de datos potenciales, que incluyen, entre otros:

- Versión del sistema operativo: no es raro que el software sea vulnerable en una operación borrando la versión del sistema pero no en otra. Debido a esto, el escáner intentará determinar, con la mayor precisión posible, qué versión del sistema operativo aloja el objetivo solicitud.
- Nivel de parche: muchas veces, se lanzarán parches para un sistema operativo que no aumentar la información de la versión, pero aún así cambiar la forma en que responderá una vulnerabilidad, o incluso eliminar la vulnerabilidad por completo.
- Arquitectura del procesador: muchas aplicaciones de software están disponibles para múltiples procesadores arquitecturas como Intel x86, Intel x64, múltiples versiones de ARM, UltraSPARC, etc.

[5] https://en.wikipedia.org/wiki/Executable_space_protection#Windows
[6] https://en.wikipedia.org/wiki/Address_space_layout_randomization
[7]

[8] http://tools.kali.org/category/vulnerability-analysis
http://tools.kali.org/category/web-applications

Página 311

En algunos casos, solo existirá una vulnerabilidad en una arquitectura específica, por lo que conocer este bit de información puede ser crítica para una firma precisa.

- Versión del software: la versión del software específico es uno de los elementos básicos que necesita ser capturado para identificar una vulnerabilidad.

Estos, y muchos otros puntos de datos, se utilizarán para crear una firma como parte de una vulnerabilidad. escanear. Como se esperaba, cuanto más puntos de datos coincidan, más precisa será la firma. Cuando Al tratar con coincidencias de firma, puede tener algunos resultados potenciales diferentes:

- Verdadero positivo: la firma coincide y captura una verdadera vulnerabilidad. Estos resultados son los que tendrá que seguir y corregir, ya que estos son los elementos que las personas pueden aprovechar para dañar su organización (o la de su cliente).
- Falso positivo: la firma coincide. Sin embargo, el problema detectado no es una verdadera vulnerabilidad. bilidad En una evaluación, estos a menudo se consideran ruido y pueden ser bastante frustrantes. usted nunca quiera descartar un verdadero positivo como un falso positivo sin una validación más extensa.
- Verdadero negativo: la firma no coincide y no hay vulnerabilidad. Este es el ideal escenario, verificando que no existe una vulnerabilidad en un objetivo.
- Falso negativo: la firma no coincide, pero existe una vulnerabilidad. Tan malo como es un falso positivo, un falso negativo es mucho peor. En este caso, existe un problema pero el el escáner no lo detectó, por lo que no tiene indicios de su existencia.

Como puede imaginar, la precisión de las firmas es extremadamente importante para obtener resultados precisos. Cuantos más datos se proporcionen, mayores serán las posibilidades de obtener resultados precisos de un escaneo automatizado basado en firmas, razón por la cual los escaneos autenticados son a menudo tan populares.

Con un escaneo autenticado, el software de escaneo usará las credenciales proporcionadas para autenticar al objetivo. Esto proporciona un nivel de visibilidad más profundo en un objetivo que el que de otro modo sería posible. ble. Por ejemplo, en un escaneo normal solo puede detectar información sobre el sistema que puede ser derivado de los servicios de escucha y la funcionalidad que proporcionan. Esto puede ser bastante informativo algunas veces, pero no puedo competir con el ClevelandDepthofdatat que se obtendrá autenticarse en el sistema y revisar exhaustivamente todo el software instalado, los parches aplicados, procesos en ejecución, etc. Esta amplitud de datos es útil para detectar vulnerabilidades que otras erwise puede no haber sido descubierto.

Una evaluación de vulnerabilidad bien conducida presenta una instantánea de los problemas potenciales de un organismo Zation y proporciona métricas para medir el cambio en el tiempo. Esta es una evaluación bastante ligera, pero aún así, muchas organizaciones realizarán regularmente escaneos de vulnerabilidad automatizados en horas para evitar posibles problemas durante el día cuando la disponibilidad del servicio y el ancho de banda son más crítico.

Como se mencionó anteriormente, un análisis de vulnerabilidad tendrá que verificar muchos puntos de datos diferentes en Para obtener un resultado preciso. Todas estas comprobaciones diferentes pueden crear carga en el sistema de destino así como consumir ancho de banda. Desafortunadamente, es difícil saber exactamente cuántos recursos se consumirá en el destino, ya que depende de la cantidad de servicios abiertos y los tipos de

Página 312

controles que estarían asociados con esos servicios. Este es el costo de hacer un escaneo; va a ocupar recursos del sistema. Tener una idea general de los recursos que se consumirán y cómo Es importante cargar mucho el sistema de destino cuando se ejecutan estas herramientas.

Escaneado de Hilos mayoría de los escáneres de vulnerabilidad incluyen una opción para establecer *hilos por exploración* , lo que equivale al número de comprobaciones simultáneas que ocurren al mismo tiempo. Aumentando este número tendrá un impacto directo en la carga en la plataforma de evaluación, así como en la red funciona y objetivos con los que estás interactuando. Es importante tener esto en cuenta cuando usa estos escáneres. Es tentador aumentar los hilos para completar los escaneos más rápido, pero recuerde el aumento sustancial de carga asociado con hacerlo.

Cuando finaliza un análisis de vulnerabilidad, los problemas descubiertos generalmente se vinculan a la industria identificadores estándar como el número CVE[9] , EDB-ID [10] , y avisos de proveedores. Esta informacion, junto con las vulnerabilidades CVSS score [11] , se utiliza para determinar una calificación de riesgo. Junto con falso negativos (y falsos positivos), estas clasificaciones de riesgo arbitrarias son problemas comunes que deben ser considerado al analizar los resultados del escaneo.

Dado que las herramientas automatizadas utilizan una base de datos de firmas para detectar vulnerabilidades, cualquier ligera desviación de una firma conocida puede alterar el resultado e igualmente la validez de la vulnerabilidad percibida ity. Un falso positivo marca incorrectamente una vulnerabilidad que no existe, mientras que un falso negativo es efectivamente ciego a una vulnerabilidad y no lo reporta. Debido a esto, a menudo se dice un escáner para ser tan bueno como su base de reglas de firma. Por esta razón, muchos proveedores proporcionan múltiples firmas conjuntos de naturaleza: uno que puede ser gratuito para los usuarios domésticos y otro conjunto bastante caro que es más integral, que generalmente se vende a clientes corporativos.

El otro problema que a menudo se encuentra con los escaneos de vulnerabilidad es la validez de lo sugerido. calificaciones de riesgo. Estas calificaciones de riesgo se definen de forma genérica, considerando muchos factores diferentes como nivel de privilegio, tipo de software y autenticación previa o posterior. Depende de tu medio ambiente, estas clasificaciones pueden o no ser aplicables, por lo que no deben aceptarse a ciegas. Solo aquellos bien versados en los sistemas y las vulnerabilidades pueden validar adecuadamente las clasificaciones de riesgo.

Si bien no existe un acuerdo universalmente definido sobre las calificaciones de riesgo, NIST Publicación especial 800-30 [12] se recomienda como referencia para la evaluación de las clasificaciones de riesgo y su precisión en su entorno. ment. NIST SP 800-30 define el verdadero riesgo de una vulnerabilidad descubierta como *una combinación de probabilidad de ocurrencia y el impacto potencial* .

[9] https://cve.mitre.org
[10] https://www.exploit-db.com/about/
[11] https://www.first.org/cvss
[12] http://csrc.nist.gov/publications/PubsSPs.html#800-30

Página 313

Probabilidad de ocurrencia

Según el Instituto Nacional de Estándares y Tecnología (NIST), la probabilidad de que ocurra rence se basa en la probabilidad de que una amenaza particular sea capaz de explotar una vulnerabilidad particular facilidad de uso, con posibles calificaciones de bajo, medio o alto.

- Alto: el adversario potencial está altamente calificado y motivado y las medidas que tienen implementados para proteger contra la vulnerabilidad son insuficientes.
- Medio: el adversario potencial está motivado y capacitado, pero las medidas implementadas para proteger contra la vulnerabilidad puede impedir su éxito.
- Bajo: el adversario potencial no está calificado o carece de motivación y existen medidas en lugar para protegerse contra la vulnerabilidad que es parcial o completamente efectiva.

Impacto

El nivel de impacto se determina evaluando la cantidad de daño que podría ocurrir si el la nerabilidad en cuestión fue explotada o aprovechada de otra manera.

- Alto: aprovechar la vulnerabilidad podría generar pérdidas financieras muy significativas, daño grave a la misión o reputación de la organización, o incluso lesiones graves, incluida la pérdida de vidas.
- Medio: aprovechar la vulnerabilidad podría conducir a pérdidas financieras, daños a misión o reputación de la organización, o lesiones humanas.
- Bajo: aprovechar la vulnerabilidad podría ocasionar cierto grado de pérdida financiera o impacto en la misión y reputación de la organización.

Riesgo general

Una vez que se ha determinado la probabilidad de ocurrencia e impacto, puede determinar el calificación de riesgo general, que se define como una función de las dos calificaciones. El riesgo general puede ser calificado Bajo, Medio o Alto, que proporciona orientación a los responsables de asegurar y mantener Los sistemas en cuestión.

- Alto: existe un fuerte requisito de que se implementen medidas adicionales para proteger

contra la vulnerabilidad. En algunos casos, se puede permitir que el sistema continúe funcionando pero se debe diseñar e implementar un plan lo antes posible.

- Medio: se requiere la implementación de medidas adicionales para proteger contra la vulnerabilidad. Un plan para implementar las medidas requeridas debe hacerse en un de manera oportuna.

Página 314

- Bajo: el propietario del sistema determinará si se implementarán medidas adicionales para protegerse contra la vulnerabilidad o pueden optar por aceptar el riesgo y abandonar el sistema sin cambios.

En resumen

Con tantos factores que constituyen el verdadero riesgo de una vulnerabilidad descubierta, el riesgo predefinido las clasificaciones de la salida de la herramienta solo deben usarse como punto de partida para determinar el verdadero riesgo para el organización general

Informes creados de manera competente a partir de una evaluación de vulnerabilidad, cuando los analiza un profesional, puede proporcionar una base inicial para otras evaluaciones, como pruebas de penetración de cumplimiento. Como tal, es importante comprender y cómo obtener los mejores resultados posibles de esta evaluación inicial.

Kali es una excelente plataforma para realizar una evaluación de vulnerabilidad y no necesita Cualquier configuración especial. En el menú de aplicaciones de Kali, encontrará numerosas herramientas para evaluaciones de nerabilidad en la recopilación de información, análisis de vulnerabilidad y aplicación web Categorías de análisis. Varios sitios, incluido el mencionado listado de herramientas de Kali Linux[13], el Kali Linux Official Documentation[14], y el Metasploit Unleashed gratuito[15] cursos proporcionan ex recursos excelentes para usar Kali Linux durante una evaluación de vulnerabilidad.

11.2.2. Prueba de penetración de cumplimiento

El siguiente tipo de evaluación en orden de complejidad es una prueba de penetración basada en el cumplimiento. Estas son las pruebas de penetración más comunes, ya que son requisitos obligatorios del gobierno y la industria Se basa en un marco de cumplimiento bajo el cual opera toda la organización.

Si bien hay muchos marcos de cumplimiento específicos de la industria, el más común probablemente ser estándar industria de pagos con tarjeta de datos de seguridad[16] (PCI DSS), un marco dictado por pago compañías de tarjetas que los minoristas que procesan pagos basados en tarjetas deben cumplir. Sin embargo, un número de otros sexistas estándar como la Defensa Información Sistemas Sistemas Agencia Agencia Seguridad Tecnología Guías de implementación de cal[17] (DISA STIG), Programa Federal de Gestión de Riesgos y Autorizaciones[18] (FedRAMP), Ley Federal de Gestión de Seguridad de la Información[19] (FISMA), y otros. En algunos casos, un cliente corporativo puede solicitar una evaluación o solicitar ver los resultados de la evaluación más reciente por varias razones. Cuando se ordenó, estos tipos de evaluación son colectivos

[13] http://tools.kali.org/tools-listing
[14] http://docs.kali.org
[15] https://www.offensive-security.com/metasploit-unleashed/
[16] diecisés https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
[17] http://iase.disa.mil/stigs/Pages/index.aspx
[18] 18 años https://www.fedramp.gov/about-us/about/
[19] http://csrc.nist.gov/groups/SMA/fisma/

Página 315

llamadas pruebas de penetración basadas en el cumplimiento, o simplemente "evaluaciones de cumplimiento" o "cumplimiento cheques ".

Una prueba de cumplimiento a menudo comienza con una evaluación de vulnerabilidad. En el caso del cumplimiento de PCI Auditoría[20], una evaluación de vulnerabilidad, cuando se realiza correctamente, puede satisfacer varias de las bases requisitos, que incluyen: “2. No utilice los valores predeterminados proporcionados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad "(por ejemplo, con herramientas de la categoría del menú Ataques de contraseña), "11. Pruebe regularmente los sistemas y procesos de seguridad ”(con herramientas de la base de datos de evaluación de catálogos egory) y otros. Algunos requisitos, como "9. Restringir el acceso físico a los datos del titular de la tarjeta " y "12. Mantener una política que aborde la seguridad de la información para todo el personal "no parece se prestan a la evaluación de vulnerabilidad tradicional basada en herramientas y requieren creatividad adicional

ity y prueba.

A pesar de que puede no parecer sencillo usar Kali Linux para algunos elementos de una prueba de cumplimiento, el hecho es que Kali encaja perfectamente en este entorno, no solo por la amplia gama de herramientas relacionadas con la seguridad, pero debido al entorno de código abierto de Debian está construido sobre, lo que permite la instalación de una amplia gama de herramientas. Buscando en el administrador de paquetes con palabras clave cuidadosamente elegidas de cualquier marco de cumplimiento que esté utilizando es casi seguro de mostrar múltiples resultados. Tal como está, muchas organizaciones usan Kali Linux como estándar plataforma para este tipo exacto de evaluaciones.

11.2.3. Prueba de penetración tradicional

Una prueba de penetración tradicional se ha convertido en un elemento difícil de definir, y muchos trabajan desde diferentes definiciones diferentes, dependiendo del espacio en el que operan. Parte de esta confusión del mercado es impulsada por el hecho de que el término "Prueba de penetración" se ha utilizado más comúnmente para el mencionó la prueba de penetración basada en el cumplimiento (o incluso una evaluación de vulnerabilidad) donde, por letrero, no está dispuesto a ejecutar la evaluación debido a que iría más allá del mínimo requisitos

Para los propósitos de esta sección, dejaremos de lado ese debate y usaremos esta categoría para cubrir como- evaluaciones que van más allá de los requisitos mínimos; evaluaciones que están diseñadas para realmente Mejorar la seguridad general de la organización.

A diferencia de los tipos de evaluación discutidos anteriormente, las pruebas de penetración a menudo no comienzan con una definición de alcance, pero en su lugar un objetivo como "simular lo que sucedería si un usuario interno es comprometido "o", identificar lo que sucedería si la organización sufriera un ataque focalizado por una parte maliciosa externa ". Un diferenciador clave de este tipo de evaluaciones es que no solo encuentre y valide vulnerabilidades, pero en su lugar aproveche los problemas identificados para descubrir lo peor: de los casos. En lugar de confiar únicamente en conjuntos de herramientas de escaneo de vulnerabilidades pesadas, debe seguir con la validación de los resultados mediante el uso de exploits o pruebas para eliminar los falsos positivos y haz tu mejor esfuerzo para detectar vulnerabilidades ocultas o falsos negativos. Esto a menudo implica explotar

[20] https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf

vulnerabilidades descubiertas inicialmente, explorando el nivel de acceso que proporciona el exploit y utilizando esto aumentó el acceso como palanca para ataques adicionales contra el objetivo.

Esto requiere una revisión crítica del entorno objetivo junto con búsqueda manual, creatividad, y pensar fuera de la caja para descubrir otras vías de vulnerabilidad potencial y, en última instancia, utilizando otras herramientas y pruebas fuera de las encontradas por los escáneres de vulnerabilidades más pesados. Una vez que esto es completado, a menudo es necesario comenzar todo el proceso nuevamente varias veces para hacer un proceso completo y completo trabajo.

Incluso con este enfoque, a menudo encontrará que muchas evaluaciones están compuestas de diferentes etapas. Kali facilita la búsqueda de programas para cada fase a través del menú Kali:

- Recopilación de información: en esta fase, te centras en aprender lo más posible sobre entorno objetivo Por lo general, esta actividad no es invasiva y tendrá un aspecto similar al estándar. Dard actividad del usuario. Estas acciones constituirán la base del resto de la evaluación. y, por lo tanto, debe ser lo más completo posible. La categoría de recopilación de información de Kali tiene docenas de herramientas para descubrir tanta información como sea posible sobre el medio ambiente juzgado.
- VulnerabilityDiscovery: a menudo se denominará "recopilación de información activa", donde usted no ataque, sino que participe en un comportamiento de usuario no estándar en un intento de identificar posibles vulnerabilidades en el entorno objetivo. Aquí es donde las vulnerabilidades discutidas anteriormente El escaneo de la capacidad se realizará con mayor frecuencia. Los programas enumerados en el Análisis de vulnerabilidad, Las categorías de Análisis de aplicaciones web, Evaluación de bases de datos e Ingeniería inversa serán útil para esta fase.
- Explotación: con las posibles vulnerabilidades descubiertas, en esta fase intenta explotar ellos para obtener un punto de apoyo en el objetivo. Las herramientas para ayudarlo en esta fase se pueden encontrar en Análisis de aplicaciones web, evaluación de bases de datos, ataques de contraseña y herramientas de explotación categorías.
- Pivote y exfiltración: una vez que se establece el punto de apoyo inicial, se deben seguir otros pasos terminado. Estos son a menudo privilegios crecientes a un nivel adecuado para lograr su objetivos como atacante, girando hacia otros sistemas que pueden no haber sido previamente accesibles posible para usted, y extrayendo información sensible de los sistemas de destino. Referirse a Ataques con contraseña, herramientas de explotación, olfateo y suplantación de identidad, y categorías posteriores a la explotación

para ayudar con esta fase.

- Informes: una vez que se completa la parte activa de la evaluación, debe documentar ment e informar sobre las actividades que se llevaron a cabo. Esta fase a menudo no es tan técnica como las fases anteriores, sin embargo, es muy importante asegurarse de que su cliente obtenga el valor total del trabajo completado. La categoría Herramientas de informes contiene una serie de herramientas que han demostrado ser útiles en la fase de presentación de informes.

En la mayoría de los casos, estas evaluaciones serán muy únicas en su diseño, ya que cada organización lo hará operar con diferentes amenazas y activos para proteger. Kali Linux es una base muy versátil para

Página 317

este tipo de evaluaciones y aquí es donde realmente puede aprovechar los muchos Kali Linux características de personalización. Muchas organizaciones que llevan a cabo los tipos de evaluaciones mantendrán Versiones altamente personalizadas de Kali Linux para la velocidad de uso interno para la implementación de sistemas antes Una nueva evaluación.

Las personalizaciones que las organizaciones hacen a sus instalaciones de Kali Linux a menudo incluyen:

- Preinstalación de paquetes comerciales con información de licencia. Por ejemplo, puedes tener un paquete como un escáner de vulnerabilidad comercial que le gustaría usar. A evite tener que instalar este paquete con cada compilación, puede hacerlo una vez [21] y hacer que se muestre en cada despliegue de Kali que hagas.
- Redes privadas virtuales (VPN) de conexión y configuración preconfiguradas. Estos son muy útiles en licencia- detrás de dispositivos que le permiten realizar evaluaciones "remotas internas". En la mayoría de los casos, estos sistemas se conectarán de nuevo a un sistema controlado por un evaluador, creando un túnel que el evaluador puede usar para acceder a los sistemas internos. El ISO de Kali Linux de Doom [22] es un ejemplo de este tipo exacto de personalización.
- Herramientas preinstaladas desarrolladas internamente de dos áreas y herramientas. Muchas organizaciones tendrán privacidad conjuntos de herramientas, por lo que configurarlos una vez en una instalación personalizada de Kali [23] ahorra tiempo.
- Configuraciones de SO preconfiguradas, tales como mapeos de host, fondos de escritorio, configuraciones de proxy, etc. Muchos usuarios tienen Kali ajustes específicos [24] que les gusta haber ajustado tan. Si usted es va a hacer un re-despliegue de Kali de forma regular, capturar estos cambios hace mucho de sentido

11.2.4. Evaluación de aplicación

Si bien la mayoría de las evaluaciones tienen un alcance amplio, una evaluación de la aplicación es una especialidad que es narrativa enfocado en una sola aplicación. Este tipo de evaluaciones se están volviendo más comunes Debido a la complejidad de las aplicaciones de misión crítica que usan las organizaciones, muchas de las cuales son casa integrada. La evaluación de la aplicación generalmente se agrega a la evaluación de un negocio, según sea necesario. Las aplicaciones que se pueden evaluar de esta manera incluyen, pero no se limitan a:

- Aplicaciones web: la superficie de ataque externa más común, las aplicaciones web hacer grandes objetivos simplemente porque son accesibles. A menudo, las evaluaciones estándar serán encuentra problemas básicos en aplicaciones web, sin embargo, una revisión más centrada a menudo vale la pena tiempo para identificar problemas relacionados con el flujo de trabajo de la aplicación. El meta de *kali-linux-web* El paquete tiene una serie de herramientas para ayudar con estas evaluaciones.
- Aplicaciones de escritorio compiladas: el software del servidor no es el único objetivo; aplicaciones de escritorio También forman una maravillosa superficie de ataque. En años pasados, muchas aplicaciones de escritorio como

[21] http://docs.kali.org/kali-dojo/02-mastering-live-build
[22] https://www.offensive-security.com/kali-linux/kali-rolling-iso-of-doom/
[23] http://docs.kali.org/development/live-build-a-custom-kali-iso
[24] https://www.offensive-security.com/kali-linux/kali-linux-recipes/

Página 318

Los lectores de PDF o los programas de video basados en la web fueron muy específicos, obligándolos a madurar. Sin embargo, todavía hay una gran cantidad de aplicaciones de escritorio que son muy comunes. habilidades cuando se revisan adecuadamente.

- Aplicaciones móviles: a medida que los dispositivos móviles se vuelvan más populares, las aplicaciones móviles serán- Se trata de una superficie de ataque mucho más estándar en muchas evaluaciones. Este es un movimiento rápido El objetivo y las metodologías aún están madurando en esta área, lo que lleva a nuevos desarrollos

Prácticamente todas las semanas. Las herramientas relacionadas con el análisis de aplicaciones móviles se pueden encontrar en la categoría del menú de Ingeniería inversa.

Las evaluaciones de la aplicación se pueden realizar de diferentes maneras. Como un simple ejemplo, un La herramienta automatizada específica de la aplicación se puede ejecutar contra la aplicación en un intento de identificar problemas potenciales. Estas herramientas usarán lógica específica de la aplicación en un intento de identificar desconocidos problemas en lugar de solo depender de un conjunto de firmas conocidas. Estas herramientas deben tener una función incorporada. comprensión del comportamiento de la aplicación. Un ejemplo común de esto sería una aplicación web escáner de vulnerabilidades como Burp Suite[25] , dirigido contra una aplicación que primero identifica varios campos de entrada y luego envía ataques de inyección SQL comunes a estos campos mientras monitorea la respuesta de la aplicación para indicaciones de un ataque exitoso.

En un escenario más complejo, una evaluación de la aplicación se puede realizar de forma interactiva en *caja negra* o *caja blanca* .

- Evaluación de recuadro negro: la herramienta (o asesor) interactúa con la aplicación sin ninguna especialidad conocimiento o acceso más allá del de un usuario estándar. Por ejemplo, en el caso de una aplicación web plication, el evaluador solo puede tener acceso a las funciones y características que están disponibles a un usuario que no ha iniciado sesión en el sistema. Cualquier cuenta de usuario utilizada sería aquella en la que Un usuario general puede auto-registrar la cuenta. Esto evitaría que el atacante sea capaz de revisar cualquier funcionalidad que solo esté disponible para usuarios que necesitan ser creados por un administrador.

- Evaluación del recuadro blanco: la herramienta (o asesor) a menudo tendrá acceso completo al código fuente, acceso administrativo a la plataforma que ejecuta la aplicación, etc. Esto asegura que Se completa una revisión completa y completa de todas las funcionalidades de la aplicación, independientemente de donde esa funcionalidad vive en la aplicación. La compensación con esto es que la evaluación ment no es en modo alguno una simulación de actividad maliciosa real.

Obviamente hay tonos de gris en el medio. Por lo general, el factor decisivo es el objetivo de evaluación. Si el objetivo es identificar lo que sucedería en caso de que llegara la aplicación bajo un ataque externo enfocado, una evaluación de recuadro negro probablemente sería lo mejor. Si el objetivo es identificar y eliminar tantos problemas de seguridad como sea posible en un período de tiempo relativamente corto, un blanco El enfoque de caja puede ser más eficiente.

[25] https://portswigger.net/burp/

En otros casos, se puede adoptar un enfoque híbrido donde el evaluador no tiene acceso completo a la código fuente de las aplicaciones de la plataforma que ejecuta la aplicación, pero se utilizan aprovisionamientos de cuentas por un administrador para permitir el acceso a la mayor funcionalidad posible de la aplicación.

Kali es una plataforma ideal para todo tipo de evaluaciones de aplicaciones. En una instalación predeterminada, un Se encuentra disponible una gama de diferentes escáneres específicos para cada aplicación. Para evaluaciones más avanzadas, un Existe una amplia gama de herramientas, editores de origen y entornos de secuencias de comandos. Puede encontrar la aplicación web ción [26] e ingeniería inversa[27] secciones de las herramientas de Kali[28] sitio web útil.

11.3 Formalización de la evaluación.

Con su entorno Kali listo y el tipo de evaluación definido, está casi listo para empezar a trabajar. Su último paso es formalizar el trabajo a realizar. Esto es críticamente importante, ya que esto define lo que serán las expectativas para el trabajo y le otorga permiso para llevar a cabo lo que de lo contrario podría ser una actividad ilegal. Cubriremos esto a un alto nivel, pero este es un proceso muy complejo. y un paso importante, por lo que es probable que desee consultar con el representante legal de su organización para asistencia.

Como parte del proceso de formalización, deberá definir las reglas de participación para el trabajo. Esto cubre elementos como:

- ¿Con qué sistemas puedes interactuar? Es importante asegurarse de no acciden- Tally interfiere con cualquier cosa que sea crítica para las operaciones comerciales.
- ¿A qué hora del día y durante qué período de ataque se permite que ocurra la evaluación? Algunos A las organizaciones les gusta limitar los tiempos en que se puede realizar el trabajo de evaluación.
- Cuando descubres una vulnerabilidad potencial, ¿puedes explotarla? Si no, que es El proceso de aprobación? Hay algunas organizaciones que toman un enfoque muy controlado. a cada intento de explotación, mientras que a otros les gustaría un enfoque más realista. Es lo mejor definir estas expectativas claramente antes de comenzar el trabajo.

- Si se descubre un problema importante, ¿cómo se debe manejar? A veces, organizaciones desea ser informado de inmediato, de lo contrario, generalmente se aborda al final de la evaluación ment.
- En caso de emergencia, ¿a quién debe contactar? Siempre es importante saber a quién consultar tacto cuando ocurre un problema de cualquier tipo.
- ¿Quién sabrá sobre la actividad? ¿Cómo se les comunicará? En algunos casos, las organizaciones querrán probar su respuesta a incidentes y el rendimiento de detección como parte de la evaluacion. Siempre es una buena idea saber esto de antemano, para saber si debe tome cualquier grado de sigilo en el enfoque de la evaluación.

[26] http://tools.kali.org/category/web-applications
[27] http://tools.kali.org/category/reverse-engineering
[28] http://tools.kali.org

320

- ¿Cuáles son las expectativas al final de la evaluación? ¿Cómo se comunicarán los resultados? Sepa lo que todas las partes esperan al final de la evaluación. Definir el entregable es el La mejor manera de mantener a todos felices después de que el trabajo se haya completado.

Si bien no está completo, este listado le da una idea de los detalles que deben cubrirse. Sin embargo, debe darse cuenta de que no hay sustituto para una buena representación legal. Una vez que estos artículos son definido, debe adquirir la autorización adecuada para realizar la evaluación, ya que gran parte del la actividad que realizará en el curso de una evaluación puede no ser legal sin la autoridad adecuada de alguien con la autoridad para dar ese permiso.

Con todo eso en su lugar, todavía hay un último paso que querrá tomar antes de comenzar a trabajar: valida- ción Nunca confíes en el alcance que se te proporciona, siempre valídalo. Usa información múltiple fuentes para confirmar que los sistemas dentro del alcance son de hecho propiedad del cliente y que son operado por el cliente también. Con la prevalencia de los servicios en la nube, una organización puede olvidar que en realidad no son dueños de los sistemas que les brindan servicio. Puede encontrar que tiene que obtenga un permiso especial de un proveedor de servicios en la nube antes de comenzar a trabajar. Además, siempre validar bloques de direcciones IP. No cuente con la suposición de una organización de que posee propiedad intelectual completa bloques, incluso si firman en ellos como objetivos viables. Por ejemplo, hemos visto ejemplos de organizaciones que solicitan una evaluación de un rango completo de red de clase C cuando, de hecho, solo poseía un subconjunto de esas direcciones. Al atacar todo el espacio de direcciones de clase C, haríamos han terminado atacando a los vecinos de la red de la organización. La subcategoría OSINT Analysis del menú Recopilación de información contiene una serie de herramientas que pueden ayudarlo con este vali proceso de dación.

11.4 Tipos de ataques

Una vez que el trabajo se está llevando a cabo, ¿cuáles son algunos de los tipos específicos de ataques que se enfrentarán? conductos? Cada tipo de vulnerabilidad[29] tiene sus propias técnicas de explotación asociadas. Esta sección cubrirá las diversas clases de vulnerabilidades con las que interactuará con más frecuencia.

No importa en qué categoría de vulnerabilidad se encuentre, Kali crea estas herramientas y vulnerabilidades. fácil de encontrar. El menú Kali en su interfaz gráfica de usuario se divide en categorías para ayudar hacer que la herramienta correcta sea más fácil de encontrar. Además, el sitio web de Kali Tools[30] tiene listados completos de las diversas herramientas disponibles en Kali, organizadas por categoría y etiquetadas para facilitar la navegación. Cada La entrada contiene información detallada sobre la herramienta, así como ejemplos de uso.

[29] https://www.cvedetails.com/vulnerabilities-by-types.php
[30] http://tools.kali.org/tools-listing

Página 321

11.4.1. Negación de servicio

Los ataques de denegación de servicio aprovechan una vulnerabilidad para crear una pérdida de servicio, a menudo bloqueando el

proceso vulnerable La categoría Stress Testing del menú Kali Linux contiene varias herramientas.
para este propósito.

Cuando muchas personas escuchan el término "ataque de denegación de servicio", inmediatamente piensan en recursos
ataques de consumo que se envían desde múltiples fuentes a la vez contra un solo objetivo. Estas
sería un ataque *distribuido de* denegación de servicios o DDoS. Este tipo de ataques rara vez son parte de un
evaluación de seguridad profesional.

En cambio, un ataque singular de denegación de servicio suele ser el resultado de un intento incorrecto de
explotar una vulnerabilidad. Si un escritor de exploits libera parcialmente funcional o prueba de concepto (PoC)
código y se usa en el campo, esto podría crear una condición de denegación de servicio. Incluso un bien
codedexploitmayonlyworkunderveryspecificcircumstancesbutcauseadenialofserviceunder
circunstancias menores Puede parecer que la solución es usar solo código de explotación seguro y probado,
o para escribir el tuyo. Incluso con esta solución, no hay garantías y esto limita severamente
el evaluador, causando restricciones indebidas, lo que resulta en una evaluación menor. En cambio, la clave es
compromiso. Evite el código PoC y los exploits no probados en el campo y siempre asegúrese de que un abogado tenga
Cubriste otros contratiempos.

Por lo general, los ataques de denegación de servicio no se lanzan intencionalmente. La vulnerabilidad más automatizada
Las herramientas declararán las vulnerabilidades de denegación de servicio como un riesgo menor debido al hecho de que, si bien puede
eliminar un servicio de la operación, ese servicio no puede ser explotado para la ejecución del código. De todos modos, eso
Es importante recordar que no todos los exploits se lanzan públicamente y que la denegación de servicio es más vulnerable.
la habilidad puede enmascarar una amenaza más profunda y grave. Un exploit de ejecución de código para una negación conocida de
El servicio puede existir pero no ser público. El punto es, prestar atención a las vulnerabilidades de denegación de servicio
y aliente a su cliente a repararlo, independientemente de su (a menudo baja) calificación de amenaza.

11.4.2. Corrupción de la memoria

Una corrupción de memoria ocurre cuando una ubicación dentro del espacio de memoria de un proceso es accidental
Tally modificado debido a errores de programación. Los errores de corrupción de memoria generalmente conducen a errores
comportamiento del programa dictable, sin embargo, en muchos casos, estos errores permiten la manipulación de la memoria del proceso.
ción de tal manera que el flujo de ejecución del programa se pueda controlar, permitiendo que el atacante defina
actividad.

Estos ataques generalmente se denominan desbordamientos de búfer, aunque este término es un exceso
simplificación. Los tipos más comunes de corrupción de memoria son muy diferentes de uno y otro.
otros y tienen sus propias tácticas y técnicas requeridas para una explotación exitosa.

- Desbordamiento del búfer en la pila: cuando un programa escribe más datos en un búfer en la pila que allí
  hay espacio disponible para ello, la memoria adyacente puede corromperse, lo que a menudo hace que el programa
  choque.

- Corrupción en el montón: la memoria del montón se asigna en tiempo de ejecución y generalmente contiene datos del
  programa en ejecución Se producen daños en el montón al manipular los datos para sobrescribirlos
  la lista vinculada de punteros de memoria de montón.
- Desbordamiento de enteros: estos desbordamientos se producen cuando una aplicación aplica para crear un valor numérico
  que no puede estar contenido dentro de su espacio de almacenamiento asignado.
- FormatString: cuando un programa acepta usuarioinputa y formatea sin comprobarlo, mem-
  Las ubicaciones de ory se pueden revelar o sobrescribir, según los tokens de formato que se usen.

11.4.3. Vulnerabilidades web

Debido al hecho de que los sitios web modernos ya no son páginas estáticas, sino que se generan dinámicamente
Para el usuario, el sitio web promedio es bastante complejo. Las vulnerabilidades web aprovechan esto
complejidad en un esfuerzo por atacar la lógica de generación de la página de fondo o la presentación a
El visitante del sitio.

Este tipo de ataques son extremadamente comunes, ya que muchas organizaciones han llegado al punto
donde tienen muy pocos servicios externos. Dos de las aplicaciones web más frecuentes
Los tipos de ataque [31] son inyección SQL y scripting entre sitios (XSS).

- Inyección SQL: estos ataques aprovechan las aplicaciones mal programadas que
  no desinfecte adecuadamente la entrada del usuario, lo que permite extraer información del
  base de datos o incluso la toma de control completa del servidor.
- Secuencias de comandos entre sitios: al igual que con la inyección SQL, los ataques XSS son el resultado de una desinfección incorrecta
  de entrada del usuario, lo que permite a los atacantes manipular al usuario o al sitio para que ejecute código en el

contexto de su propia sesión de navegador.
Las aplicaciones web complejas, ricas y complicadas son muy comunes y presentan un ataque bienvenido
superficie para fiestas maliciosas. Encontrará una gran cantidad de herramientas útiles en la aplicación web
Categoría del menú de análisis y el metapaquete *kali-linux-web* .

11.4.4. Ataques de contraseña

Los ataques de contraseña son ataques contra el sistema de autenticación de un servicio. Estos ataques son
a menudo dividido en ataques de contraseña en línea y ataques de contraseña fuera de línea, que encontrará
se desvió en la categoría del menú Ataques de contraseña. En un ataque de contraseña en línea, múltiples contraseñas
se intentan contra un sistema en ejecución. En un ataque de contraseña sin conexión, el hash o encriptado
Se obtienen valores de las contraseñas y el atacante intenta obtener los valores de texto sin cifrar.
La protección contra este tipo de ataque es el hecho de que es computacionalmente costoso trabajar
a través de este proceso, limitando el número de intentos por segundo que puede generar. Sin embargo,

[31] https://www.owasp.org/index.php/Top_10_2013-Top_10

existen soluciones para esto, como el uso de unidades de procesador gráfico (GPU) para acelerar el número
Una serie de intentos que se pueden hacer. El metapaquete *kali-linux-gpu* contiene una serie de herramientas que
aprovechar este poder.

Con mayor frecuencia, los ataques de contraseña apuntan a las contraseñas predeterminadas proporcionadas por el proveedor. Como estos están bien
valores conocidos, los atacantes buscarán estas cuentas predeterminadas, con la esperanza de tener suerte. Otro común
Los ataques incluyen ataques de diccionario personalizados donde se crea una lista de palabras que se ha diseñado para
el entorno de destino y luego un ataque de contraseña en línea contra común, predeterminado o conocido
las cuentas se realizan donde se intenta cada palabra en secuencia.

En una evaluación, es muy importante comprender las posibles consecuencias de este tipo de
ataque. Primero, a menudo son muy ruidosos debido a los repetidos intentos de autenticación. En segundo lugar,
Estos ataques a menudo pueden resultar en una situación de bloqueo de cuenta después de que se hayan intentado demasiados intentos inválidos
realizado contra una sola cuenta. Finalmente, el rendimiento de estos ataques suele ser bastante lento,
resultando en dificultades al intentar usar una lista de palabras completa.

11.4.5. Ataques del lado del cliente

La mayoría de los ataques se realizan contra servidores, pero a medida que los servicios se han vuelto más difíciles de atacar, más fácil
los objetivos han sido seleccionados. Los ataques del lado del cliente son el resultado de esto, donde un atacante apuntará
Las diversas aplicaciones instaladas en la estación de trabajo de un empleado dentro de una organización objetivo.
La categoría del menú Herramientas de ingeniería social tiene una serie de excelentes aplicaciones que pueden ayudar
realizar este tipo de ataques.

Este tipo de ataque es mejor explotado por los ataques Flash, Acrobat Reader y Java que fueron muy
commonintheearly2000s. En estos casos, los atacantes intentarían solicitar un objetivo para visitar el mal
página web. Estas páginas contendrían código especializado que provocaría vulnerabilidades en estos
aplicaciones del lado del cliente, lo que resulta en la capacidad de ejecutar código malicioso en el sistema de destino.

Los ataques del lado del cliente son increíblemente difíciles de prevenir, ya que requieren una gran cantidad de educación del usuario,
actualizaciones constantes de la aplicación y controles de red para mitigar el riesgo de manera efectiva.

11.5 Resumen

En este capítulo, analizamos brevemente el papel de Kali en el campo de la seguridad de la información. Nosotros discutimos
La importancia de una instalación limpia y funcional y el uso de cifrado antes de dirigirse a
el campo para proteger la información de su cliente y la importancia de la representación legal
para protegerlo a usted y a los intereses de su cliente.

Los componentes de la tríada de la CIA (confidencialidad, integridad, disponibilidad) son los elementos principales
en el que se centrará al proteger un sistema como parte de la implementación estándar, mantenimiento o
evaluación. Este fundamento conceptual lo ayudará a identificar los componentes críticos.

componentes de sus sistemas y la cantidad de esfuerzo y recursos que vale la pena invertir en corregir problemas identificados

Discutimos varios tipos de vulnerabilidades, incluida la inclusión de archivos, inyección de SQL, sobrecarga del búfer flujos y condiciones de carrera.

La precisión de las firmas es extremadamente importante para obtener una evaluación útil de vulnerabilidad sults. Cuantos más datos se proporcionen, mayor será la posibilidad de obtener resultados precisos de un escaneo automatizado basado en firmas, razón por la cual los escaneos autenticados son a menudo tan populares.

Dado que las herramientas automatizadas utilizan una base de datos de firmas para detectar vulnerabilidades, cualquier ligera desviación de una firma conocida ahora puede alterarse el resultado y al igual que la validez de la vulnerabilidad percibida.

También discutimos los cuatro tipos de evaluaciones: la *evaluación de vulnerabilidad* , la *prueba de cumplimiento* , la *tradición prueba de penetración nacional* y *evaluación de la aplicación* . Evento cada tipo de evaluación un conjunto básico de herramientas, muchas de las herramientas y técnicas se superponen.

La evaluación de vulnerabilidad es relativamente simple en comparación con los otros tipos de evaluación y a menudo consiste en un inventario automatizado de problemas descubiertos dentro de un entorno objetivo. En En esta sección, discutimos que una vulnerabilidad es una falla que, cuando se explota, comprometerá confidencialidad, integridad o disponibilidad de un sistema de información. Como está basado en firmas, esto tipo de evaluación de semillas y firmas precisas y puede presentar falsos positivos y negativos. usted encontrará las herramientas centrales para este tipo de evaluación en el Análisis de vulnerabilidad y explotación Categorías del menú de herramientas de Kali Linux.

Las pruebas de cumplimiento se basan en requisitos obligatorios del gobierno y la industria (como PCI DSS, DISA STIG y FISMA), que a su vez se basan en un marco de cumplimiento. Esta prueba por lo general comienza con una evaluación de vulnerabilidad.

Una prueba de penetración tradicional es una evaluación exhaustiva de seguridad diseñada para mejorar la postura de seguridad general de una organización basada en ciertas amenazas del mundo real. Este tipo de prueba implica varios pasos (reflejados por la estructura del menú de Kali Linux) y culmina en la explotación de vulnerabilidades y acceso pivotante a otras máquinas y redes dentro del alcance objetivo.

Las evaluaciones de la aplicación (generalmente caja blanca o negra) se centran en una sola aplicación y utilizan Herramientas especializadas como las que se encuentran en Análisis de aplicaciones web, Evaluación de bases de datos, Reverso Categorías de menú de herramientas de ingeniería y explotación.

Se discutieron varios tipos de ataques, incluidos: denegación de servicio, que rompe el comportamiento de una aplicación y la hace inaccesible; corrupción de memoria, que conduce a la manipulación de pro- memoria de cess, a menudo permitiendo la ejecución de un código de atacante; ataques web, que atacan servicios web usando técnicas como inyección SQL y ataques XSS; y ataques de contraseña, que a menudo aprovechan listas de contraseñas para atacar las credenciales del servicio.

Palabras clave

Cambios constantes
Certificaciones
Entrenamientos

Capítulo

12 Conclusión: el Camino por delante

Contenido

Mantenerse al día con los cambios 302
Mostrando su conocimiento recién adquirido 302
Yendo más allá 302

¡Felicidades! Esperemos que ahora esté más familiarizado con su sistema Kali Linux y usted
No debe tener miedo de usarlo para cualquier experimento que se le ocurra. Has descubierto su
características más interesantes, pero también conoce sus límites y varias formas de evitarlos
limitaciones

Si no ha puesto en práctica todas las funciones, guarde este libro con fines de referencia y
actualice su memoria cuando esté a punto de probar una nueva función. Recuerda que no hay nada
ing mejor que la práctica (y perseverancia) para desarrollar nuevas habilidades. Prueba más duro [1] , como la ofensiva
Los entrenadores de seguridad siguen repitiendo.

12.1 Mantenerse al día con los cambios

Con una distribución en constante cambio como *kali-rolling* , algunas partes del libro necesariamente
volverse obsoleto Haremos todo lo posible para mantenerlo actualizado (al menos para la versión en línea) pero para
La mayoría de las partes tratamos de proporcionar explicaciones genéricas que deberían ser útiles durante mucho tiempo.

Dicho esto, debe estar listo para aceptar los cambios y encontrar soluciones a cualquier problema que
podría aparecer. Con una mejor comprensión de Kali Linux y su relación con Debian, usted
puede confiar en las comunidades de Kali y Debian y sus numerosos recursos (rastreadores de errores,
foros, listas de correo, etc.) cuando se estanca.

No tenga miedo de archivar errores (consulte la sección 6.3, "Cómo presentar un buen informe de error " [página 129])! Si usted es
como yo, cuando haya completado los pasos necesarios para presentar un buen informe de error (y
toma un poco de tiempo), habrá resuelto el problema o al menos ha encontrado una buena solución. Y por
En realidad, presentando el error, estará ayudando a otros afectados por el problema.

12.2 Mostrando su conocimiento recién adquirido

¿Estás orgulloso de tus nuevas habilidades de Kali Linux? ¿Le gustaría asegurarse de recordar el
cosas realmente importantes? Si responde afirmativamente a una de esas preguntas, entonces debe considerar
solicitando el programa Kali Linux Certified Professional.

Es una certificación exhaustiva que garantiza que sepa cómo desplegar y usar Kali Linux
en muchos casos de uso realistas. Es una adición a su currículum vitae y sus cosechas vitales ya están listas
para llegar más lejos.

12.3 Ir más lejos

Este libro le enseñó muchas cosas que cualquier usuario de Kali Linux debería saber, pero hicimos algunas cosas difíciles
opciones para mantenerlo breve, y hay muchos temas que no fueron cubiertos.

[1] https://www.offensive-security.com/offsec/say-try-harder/

12.3.1. Hacia la administración del sistema

Si desea obtener más información sobre la administración del sistema, solo podemos recomendarle que
consulte el Manual del administrador de Debian:

[2] https://debian-handbook.info/get/

Encontrará muchos capítulos complementarios que cubren los servicios comunes de Unix que tenemos
completamente omitido en este libro. E incluso para los capítulos que se han reutilizado en el libro de Kali, usted
encontrará muchos consejos complementarios, especialmente sobre el sistema de embalaje (que también está cubierto
más ampliamente en su nivel más bajo).

El libro de Debian obviamente presenta más profundamente a la comunidad de Debian y la forma en que se organiza.
Nized Si bien este conocimiento no es vital, es realmente útil cuando tiene que interactuar con Debian
contribuyentes, por ejemplo a través de informes de errores.

12.3.2. Hacia las pruebas de penetración

Probablemente ya haya notado que este libro no le enseñó las pruebas de penetración. Pero las cosas

Aprendiste que aún son importantes. Ahora está listo para explotar completamente el poder de Kali Linux, el mejor marco de prueba de penetración. Y tienes las habilidades básicas de Linux necesarias para participar en entrenamiento de seguridad ofensiva.

Si cree que aún no está listo para un curso pago, puede comenzar siguiendo el Metasploit Soltado[2] capacitaciones en línea gratuitas. Metasploit es una herramienta de prueba de penetración muy popular y usted tiene que saberlo si se toma en serio sus planes para aprender las pruebas de penetración.

El siguiente paso lógico sería seguir las Pruebas de penetración con Kali Linux[3] en línea curso que lidera el camino a la famosa certificación de "Profesional Certificado en Seguridad Ofensiva". Este curso en línea se puede seguir a su propio ritmo, pero la certificación es realmente difícil, Prueba de penetración práctica de 24 horas de duración, en palabras reales, que se realiza en una red VPN aislada.

¿Estás preparado para el desafío?

[2] https://www.offensive-security.com/metasploit-unleashed/
[3] https://www.offensive-security.com/information-security-training/

Índice

_ _
.config, 235
.d, 195
.htaccess, 116
/ dev, 48
/etc/apt/apt.conf.d/, 195
/ etc / apt / preferencias, 196
/etc/apt/sources.list, 172
/etc/apt/trusted.gpg.d/, 203
/ etc / group, 107
/ etc / gshadow, 107
/ etc / network / interfaces, 105
/ etc / passwd, 107
/ etc / salt / minion, 255
/ etc / shadow, 107
/ etc / ssh / sshd_config, 110
/ proc, 48
/ sys, 48
/ var / lib / dpkg /, 212
/ var / www / html /, 114
CPU de 32 bits, 16
CPU de 64 bits, 16

UNA
a2dismod, 113
a2enmod, 113
a2ensite, 114
ACEPTAR, 155
cuenta
    creación, 107
    desactivar, 109
    modificación, 108
agregar un usuario a un grupo, 108
addgroup, 109
adduser, 108
contraseña de administrador, 72
Herramienta de paquete avanzado, 171
ayudante (paquete Debian), 163
AllowOverride, directiva Apache, 115 , 116
análisis
    vulnerabilidad, 6
    aplicación web, 6
ansible, 255
Apache, 113
    directivas, 115
Directivas de Apache, 116
evaluaciones de solicitudes, 291
aplicaciones
    colección, 10
    menú, 5
aplicando un parche, 227
a propósito, 124
APT, 171
    configuración, 195
    pantalla de encabezado, 185
    configuración inicial, 81
    interfaces, 190
    búsqueda de paquetes, 185
    fijación, 196
    preferencias, 196
apto, 176
apt build-dep, 226
apt dist-upgrade, 179
apt full-upgrade, 179

actividad, monitoreo, 162
apt install, 177

purga apta, 180
apt remove, 180
apto búsqueda, 186
apto espectáculo, 186
apt apt, 223
apt apt, 176
actualización apta, 179
apt-cache, 185
apt-cache dumpavail, 187
apt-cache pkgnames, 187
política de apt-cache, 187
búsqueda de apt-cache, 186
espectáculo apt-cache, 186
apt-cdrom, 172
apt-get, 176
apt-get dist-upgrade, 179
apt-get install, 177
apt-get purge, 181
apt-get remove, 180
apt-get update, 176
apt-get upgrade, 179
apt-key, 203
apt-mark auto, 200
manual de apt-mark, 200
apt-xapian-index, 186
apt.conf.d /, 195
aptitud, 176 , 190
aptitud dist-upgrade, 179
aptitud actualización completa, 179
instalación de aptitud, 177
aptitud markauto, 200
purga de aptitud, 181
aptitud eliminar, 180
aptitud actualización segura, 179
búsqueda de aptitud, 186
programa de aptitud, 186
aptitud unmarkauto, 200
actualización de aptitud, 176
aptitud por qué, 200
arquitectura
  soporte de arco múltiple, 200
Instalaciones ARM, 94
evaluación
  aplicación, 291
  caja negra, 292
  formalización, 293
  vulnerabilidad, 284
  caja blanca, 292
ataques
  lado del cliente, 297
  base de datos, 6
  denegación de servicio, 295
  corrupción de memoria, 295
  contraseña, 6, 296
  tipos de, 294
  web, 296
  inalámbrico, 6
auditoría, seguridad, 5
autenticación
  autenticación de paquete, 202
AuthName, directiva Apache, 116
AuthType, directiva Apache, 116
AuthUserFile, directiva Apache, 116
instalación automática, 91
paquetes instalados automáticamente, 199
efecto avalancha, 163
axi-cache, 186

si
proceso en segundo plano, 57
BackTrack, XXI , 2
bg, 57
BIOS, 24
bloquear el archivo del dispositivo, 49
arranque preestablecido, 92
pantalla de arranque, 67
llave USB de arranque, 19
gestor de arranque, 83
BOOTP, 252
Saltos, campo de encabezado, 209
dependencia rota, 189
Bruce Schneier, 150
ataques de fuerza bruta, 296

buffer
  desbordamiento, 295
  recibir buffer, 156
informe de error, 129
bugs.kali.org, 133
construir dependencias, instalación, 226
opciones de construcción, 229
Build-Depends, 226
edificio
  una imagen ISO en vivo personalizada, 237
  un paquete, 231

C
caché, proxy, 82
  de un grano, 233
prueba de penetración de cumplimiento, 288
componente (de un repositorio), 173
conffiles, 214
confidencialidad
  archivos, 85
config, script de debconf, 214
configuración
  creación de paquetes de configuración, 263
  archivos, 214
  configuración inicial de APT, 81
  gestión, 255
  red
    DHCP, 71

gato, 56
cd, 52
cdimage.kali.org, 14, 175
cdrom preseed, 93
certificación, 302
chage, 108
cadena, 154
archivo de registro de cambios, 266
changelog.Debian.gz, 126
archivo de dispositivo de caracteres, 49
checksecurity, 164
sumas de comprobación, 214
chef, 255
chfn, 108
chgrp, 58
chmod, 58
elección
del país, 69
de lenguaje, 68
chown, 58
chroot, 239
chsh, 108
ataques del lado del cliente, 297
clúster, clúster PostgreSQL, 111, 113
línea de comando, 51
comunidades, 128
comparación de versiones, 185
Compilacion
estático, 71
del grano, 235
configuración del programa, 110
conflictos, 208
Conflictos, campo de encabezado, 208
contrib, sección, 173
control, 206
archivo de control, 266
suma de control, 163
control.tar.gz, 211
copia, imagen ISO, 19
derechos de autor, 127
archivo de copyright, 265
selección de país, 69
cp, 53
createdb, 112
createuser, 112
creación
de una base de datos PostgreSQL, 112
de un usuario de PostgreSQL, 112
de grupos, 109
de cuentas de usuario, 107
credenciales, por defecto, 153
secuencias de comandos entre sitios (XSS), 296
cryptsetup, 243
contraseña nuclear, 246
personalización de imagen ISO en vivo, 237

re
evaluación de la base de datos, 6
servidor de bases de datos, 111
dch, 226
dd, 22
debconf, 214
debconf-get, 97
debconf-get-selections, 94
debconf-set, 97
DEBEMAIL, 265
NOMBRE COMPLETO, 265
Debian
relación con Kali Linux, 4
Manual del administrador de Debian, 303
Directrices de software libre de Debian, 5
Debian GNU / Linux, 2
Política de Debian, 5
debian-archive-keyring, 203
debian-kernel-handbook, 233
debian / changelog, 226 , 266
debian / control, 266
debian / copyright, 265
debian / parches, 225
debian / rules, 229, 267
debuild, 232
contraseñas predeterminadas, 153
default.target, 117
supresión de un grupo, 109
delgroup, 109
denegación de servicio, 295
dependencia, 207
Depende, campo de encabezado, 207
entorno de escritorio, 3
elección durante la construcción de ISO en vivo, 238
base de escritorio, 263
detectar cambios en el sistema de archivos, 162
ataques de diccionario, 296
directivas, Apache, 115 , 116
DirectoryIndex, directiva Apache, 115
deshabilitar una cuenta, 109
disco preestablecido, 93
Discos (programa), 20
diskutil, 23
distribución, Linux, 2
dm-crypt, 86
dmesg, 60
DNAT, 155
dnsmasq, 252
docs.kali.org, 127
documentación, 124, 126
descargar
Imagen ISO, 14
las fuentes, 223
dpkg, 170
base de datos, 212
dpkg --verify, 162
funcionamiento interno, 213
dpkg-buildpackage, 231
dpkg-deb, 232
dpkg-source --commit, 227
unidad, unidad USB, 19
GOTA, 155
dropdb, 112
dropuser, 112
arranque dual, 84

mi
echo, 54
editor, 56
partición encriptada, 85
persistencia cifrada, 243
Ingenieria
reverso, 6

archivo de dispositivo, 49
df, 60
dh-make, 264
dh_install, 267
DHCP, 252
ingeniería social, 7
Mejora, campo de encabezado, 208
medio ambiente
variable de entorno, 54
ExecCGI, directiva Apache, 115

Página 334

módulos de ejecución, sal, 256
ejecución, derecha, 57
experimental, 197
Explicación, 198
herramientas de explotación, 7

F
fail2ban, 152
características, 7
fg, 57
archivo
confidencialidad, 85
archivos de configuración, 214
sistema de archivos, 49
sistema de archivos
jerarquía, 54
regla de filtrado, 154 , 157
encontrar, 56
huella digital, 163
cortafuegos, 153
FollowSymLinks, directiva Apache, 115
forense, 7
modo 8
formalización de la evaluación, 293
formato de disco, 49
foros, 128
forums.kali.org, 128
HACIA ADELANTE, 154
gratis, 60
Freenode, 128
fwbuilder, 160

sol
obtener las fuentes, 223
getent, 108
git clone, 225
Problemas de GitHub, 144
GNOME, 3
gnome-disk-utility, 20
gnome-system-monitor, 162
ÑU
Información, 126
gpasswd, 109
Llave GPG, 17
objetivo gráfico, 117
grep, 56
grupo
agregar un usuario, 108
cambio, 109
creación, 109
deleción, 109
de volúmenes, 86
propietario, 57
groupmod, 109
GRUB, 83
gui-apt-key, 204
partición guiada, 75

H
descubrimiento de hardware, 61
montón de corrupción, 295
historia de Kali Linux, 2
CASA, 55
directorio de inicio, 55
anfitrión, anfitrión virtual, 114
htpasswd, 116
Proxy HTTP, 82
Servidor HTTP, 113
http.kali.org, 174
HTTPS, 114
Hyper-V, 25

yo
ICMP, 156
id, 60 , 109
ifupdown, 105
suplantación, 7
Incluye, directiva Apache, 115
incompatibilidades, 209
Índices, directiva Apache, 115
info, 126
recopilación de información, 6
initrd preseed, 92
ENTRADA, 154

Page 335

instalación, 66
automática, 91
de dependencias de compilación, 226
en dispositivos ARM, 94
instalación de paquete, 176 , 177
solución de problemas, 95
desatendido, 91
preinstalación de instalador, 92
desbordamiento de enteros, 295
Protocolo de mensajes de control de Internet, 156
kali-dev, 4, 174
kali-linux- * metapaquetes, 239
kali-menu, 263
kali-meta, 263
kali-rolling, 4, 173
KDE, 3
grano, 48
compilación, 233
configuración, 235
troncos, 60

ip6tables, 153, 157
iptables, 153 , 157
Canal IRC, 128
isc-dhcp-server, 252
Imagen ISO
autenticación, 16
arranque, 24
copiando, 19
construcción personalizada, 237
descarga, 14
espejos, 14
variantes, 16

J
diario, 60
journalctl, 60

K
Kali Linux
comunidades, 128
documentación, 127
descarga, 14
características, 7
comenzando, 14
historia, 2
metapaquetes, 239
políticas, 9
relación con Debian, 4
repositorios, 173
kali-archive-keyring, 203
borde de sangrado kali, 174 , 197
kali-por defecto, 263
fuentes, 234
llave
Claves de autenticación de APT, 204
Llave USB, 19
distribución del teclado, 70
matar, 57
konqueror, 126
KVM, 25

L
selección de idioma, 68
diseño, teclado, 70
menos, 56
libapache-mod-php, 113
Linux, 48
distribución, 2
grano, 2, 8
fuentes de grano, 234
imagen ISO en vivo, 14
construcción personalizada, 237
arranque en vivo, 240
construcción en vivo, 237
agregar archivos, 240
debconf preseeding, 239
ganchos, 239
paquetes para instalar, 238
cargador
gestor de arranque, 83
LOG, 155
logcheck, 161
tala, 161
Administrador de volumen lógico, 86

inicio de sesión, inicio de sesión remoto, 110
registros
aptitud, 193
dpkg, 188
diario, 60
grano, 60
monitoreo, 161
ls, 52
lsdev, 61
lshw, 61
lspci, 61
lspcmcia, 61
lsusb, 61
LUKS, 86
LVM, 86
LXDE, 3

METRO
máquina, máquina virtual, 24
principal, sección, 173
hacer deb-pkg, 236
Makefile, 267
hombre, 124
administración
gestión de configuración, 255
de servicios, 117
páginas del manual, 124
paquetes instalados manualmente, 199
máscara
máscara de derechos, 59
MASQUERADA, 155
registro maestro de arranque, 84
maestro, maestro de sal, 255
espejos, 14, 81 , 174
mkdir, 53
mkfs, 49
modificación de un paquete, 222
modificación, derecha, 57
monitoreo, 161
actividad, 162
archivos, 163
archivos de registro, 161
más, 56
monte, 49
punto de montaje, 79
Multi-arco, 200
multiusuario.objetivo, 117
MultiViews, directiva Apache, 115
mv, 53

norte
netfilter, 153
configuración de red, 71 , 104
con ifupdown, 105
con NetworkManager, 104
con systemd-network, 106
instalación de red, 252
espejos de red, 81
red preestablecida, 93
servicios de red, 10
asegurando, 153
NetworkManager, 104
newgrp, 58 , 109
NOTICIAS.Debian.gz, 126
no libre, sección, 173
contraseña nuclear, 246

MATE, 3
MD5, 163
md5sums, 214
corrupción de memoria, 295
menú, menú de aplicaciones de Kali Linux, 5
metapaquete, 207 , 209
kali-linux- *, 239
Metasploit desatado, 303
minion, minion de sal, 255

propietario
grupo, 57
usuario, 57

PAGS

paquete
comprobación de autenticidad, 202
paquete binario, 170
construir, 231
configuración, 263
conflicto, 208
inspección de contenido, 184
Paquete Debian, 170
dependencia, 207
lista de archivos, 181
lista de encabezados, 184
incompatibilidad, 209
info, 184
instalación, 176, 177
haciendo cambios, 226
metainformación, 204, 206
modificación, 222
prioridad, 196
purga, 181
mudanza, 177, 180
reemplazo, 210
repositorio, 269
sello, 202
búsqueda, 182 , 185
firma, 202
fuente de, 172
paquete fuente, 170
estado, 182
desembalaje, 177
comparación de versiones, 185
paquete virtual, 209
rastreador de paquetes, 4
Paquetes.xz, 171
embalaje
opciones de construcción, 229
paquetes de configuración, 263
nueva versión aguas arriba, 229
paquete
filtro, 153
IP, 153
PAE (extensión de dirección física), 35
dividido, 242
dividir
encriptado, 85
partición de intercambio, 79
partición, 74
partición guiada, 75
partición manual, 77
passwd, 108
contraseña, 108
ataques, 296
contraseñas predeterminadas, 153
política, 152
ataques de contraseña, 6
parche, 227
aplicación de parche, 227
RUTA, 53
PCI, 288
prueba de penetración
cumplimiento, 288
tradicional, 289
prueba de penetración, 5
curso de prueba de penetración, 303
permisos, 57
persistencia, 240
encriptado, 243
múltiples tiendas, 244
pg_createcluster, 113
pg_ctlcluster, 113
pg_dropcluster, 113
pg_hba.conf, 111
pg_lsclusters, 113
pg_renamecluster, 113
pg_upgradecluster, 113
Clave PGP, 17
PHP, 113
PID, identificador de proceso, 50
Alfiler, 198

O

representación octal de derechos, 59
Seguridad ofensiva, 2
servidor openssh, 110
Opciones, directiva Apache, 115
SALIDA, 154
desbordamiento, buffer, 295
sistema de archivos superpuestos, 241

Prioridad de clavija, 198
pinfo, 126
ping, 156
fijación, fijación APT, 196
punto, punto de montaje, 79
post explotación, 7
redirección, 56
reinstalación, 189
RECHAZAR, 155
Release.gpg, 203
inicio de sesión remoto, 110
retiro de un paquete, 177

PostgreSQL, 111
postinst, 211
postrm, 211
POSTROUTING, 154
pre-dependencia, 207
Predepende, campo de encabezado, 207
preferencias, 196
preinst, 211
prerm, 211
PREROUTING, 154
archivo preestablecido, 93
presentador debian-installer, 92
prioridad
    prioridad del paquete, 196
programa
    configuración, 110
Proporciona, campo de encabezado, 209
proxy, 82
caché proxy, 82
ps, 57
marioneta, 255
purga de un paquete, 181
purgando un paquete, 181
pwd, 52
Bota PXE, 252

Q
QCOW, 30
QEMU, 25

R
leer, derecha, 57
README.Debian, 126
recibir buffer, 156
Recomienda, campo de encabezado, 208
REDIRECTAR, 155
reemplazo, 210
Reemplaza, campo de encabezado, 210
informar un error, 129
reportbug, 139
herramientas de informes, 7
repositorio de paquetes, 269
reprepro, 269
Requerir, directiva Apache, 116
requisitos, instalación mínima requerida
    ments, 66
modo de rescate del instalador, 84
cambiar el tamaño de una partición, 77
recuperar las fuentes, 223
ingeniería inversa, 6
derechos, 57
    máscara, 59
    representación octal, 59
modelo de riesgo, 150
calificaciones de riesgo, 286
rkhunter, 164
rm, 53
rmdir, 53
Rodando, Kali Rodando, 3
raíz, 10
contraseña de root, 72, 153
RTFM, 124
archivo de reglas, 267

S
módulos de ejecución de sal, 256
fórmulas de sal, 258
módulos de estado de sal, 259
estados salinos, 258
clave de sal, 255
pila de sal, 255

samhain, 164
escaneo de hilos, 286
Schneier, Bruce, 150
búsqueda de paquetes, 185
sección
    contrib, 173
    principal, 173
    no libre, 173
arranque seguro, 24
asegurando, 150
    una computadora portátil, 152
    un servidor, 152
    servicios de red, 153
seguridad
    evaluaciones, 280
    auditoría, 5
    política, 150
archivo de servicio, archivo de servicio systemd, 117
gestión de servicios, 117
directorio setgid, 58
setgid, derecha, 58
setuid, derecha, 58
Configuración, 24
sg, 109
SHA1, 163
SHA256SUMS, 16
concha, 52
reducir una partición, 77
    haciendo cambios, 226
sources.list, 172
Fuentes.xz, 171
suplantación de identidad, 7
Inyección SQL, 296
SSH, 110
SSL, 114
módulos de estado, sal, 259
poco pegajoso, 58
sudo, 10
Sugiere, campo de encabezado, 208
permuta, 79
partición de intercambio, 79
SymLinksIfOwnerMatch, directiva Apache, 115
sináptica, 190, 194
administración del sistema, 303
servicios del sistema, 7
sistema, sistema de archivos, 49
systemctl, 117
systemd, 117
systemd-network, 106
resuelto por el sistema, 107

T
objetivo, objetivo systemd, 117
TFTP, 252
tftpd-hpa, 252
modelo de amenaza, 150
TLS, 114

señal, 57
firma
    firma del paquete, 202
SNAT, 155
olfatear, 7
herramientas de ingeniería social, 7
fuente
    de paquetes, 172
    del kernel de Linux, 234
    paquete, 170
    recuperación, 223
paquete fuente
    construir, 231

umask, 59
uname, 60
instalación desatendida, 91
montaje de unión, 241
unidad, unidad systemd, 117
desempacar
    paquete binario, 177
potenciar
    manejo de problemas después de una actualización, 187
    actualización del sistema, 179
Versión aguas arriba, empaquetando una nueva, 229
Llave USB, 19
usuario
    propietario, 57
espacio de usuario, 48

V

variable, ambiente, 54
variantes de imagen ISO en vivo, 238
VDI, 30
versión, comparación, 185
vigr, 107
vipw, 107
host virtual, 114
máquina virtual, 24
memoria virtual, 79
paquete virtual, 209
VirtualBox, 25
VMware, 25
volumen
    grupo, 86
    volumen lógico, 86
    volumen físico, 86
vulnerabilidad
    análisis, 6
    evaluaciones, 284
    lado del cliente, 297
    denegación de servicio, 295
    corrupción de memoria, 295
    contraseña, 296
    exploraciones, 286
    tipos de, 294
    web, 296

W

Wanted By, directiva systemd, 118
Deseos, directiva systemd, 118
restricción de acceso web, 116
análisis de aplicaciones web, 6
ataques web, 296
autenticación web, 115
red de confianza, 17
servidor web, 113
Win32 Disk Imager, 19
ataques inalámbricos, 6
escribir a la derecha, 57

X

XDG, 55
Xen, 25
Xfce, 3

Y

grito, 126