

CP

>> CERTIFICADO DE PROFESIONALIDAD

MF0488_3



90 HORAS DE FORMACIÓN

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

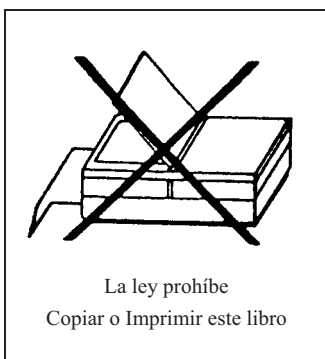


ÁLVARO GÓMEZ VIEITES

SB
STARBOOK



www.starbook.es/cp



GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

© Álvaro Gómez Vieites

© De la Edición Original en papel publicada por Editorial RA-MA

ISBN de Edición en Papel: 978-84-9265-077-4

Todos los derechos reservados © RA-MA, S.A. Editorial y Publicaciones, Madrid, España.

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos (hardware, software, sistemas operativos, etc.) suelen ser marcas registradas. RA-MA ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y solo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

RA-MA es una marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, RA-MA Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

Reservados todos los derechos de publicación en cualquier idioma.

Según lo dispuesto en el Código Penal vigente ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito de RA-MA; su contenido está protegido por la Ley vigente que establece penas de prisión y/o multas a quienes, intencionadamente, reprodujeren o plagiaran, en todo o en parte, una obra literaria, artística o científica.

Editado por:

RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Gustavo San Román Borrueco

Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-331-1

E-Book desarrollado en España en septiembre de 2014

Gestión de Incidentes de Seguridad Informática

Álvaro Gómez Vieites



A mi familia y, muy especialmente, a mi mujer Elena y a nuestra hija Irene.

ÍNDICE

EL AUTOR	11
INTRODUCCIÓN.....	13
CAPÍTULO 1. AMENAZAS A LA SEGURIDAD INFORMÁTICA	15
1.1 CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES	15
1.1.1 <i>Hackers</i>	15
1.1.2 <i>Crackers (blackhats)</i>	16
1.1.3 <i>Sniffers</i>	16
1.1.4 <i>Phreakers</i>	16
1.1.5 <i>Spammers</i>	16
1.1.6 Piratas informáticos.....	17
1.1.7 Creadores de virus y programas dañinos.....	17
1.1.8 <i>Lamers (wannabes): Script-kiddies o Click-kiddies</i>	17
1.1.9 Amenazas del personal interno	18
1.1.10 Ex empleados.....	18
1.1.11 Intrusos remunerados	18
1.1.12 Algunos hackers, crackers y phreakers famosos	18
1.2 MOTIVACIONES DE LOS ATACANTES.....	21
1.3 FASES DE UN ATAQUE INFORMÁTICO.....	22
1.4 TIPOS DE ATAQUES INFORMÁTICOS	24
1.4.1 Actividades de reconocimiento de sistemas	24
1.4.2 Detección de vulnerabilidades en los sistemas	30
1.4.3 Robo de información mediante la interceptación de mensajes	30

1.4.4	Modificación del contenido y secuencia de los mensajes transmitidos	31
1.4.5	Análisis del tráfico	31
1.4.6	Ataques de suplantación de la identidad	32
1.4.7	Modificaciones del tráfico y de las tablas de enrutamiento	37
1.4.8	Conexión no autorizada a equipos y servidores	38
1.4.9	Consecuencias de las conexiones no autorizadas a los sistemas informáticos	38
1.4.10	Introducción en el sistema de <i>malware</i> (código malicioso)	39
1.4.11	Ataques contra los sistemas criptográficos	43
1.4.12	Fraudes, engaños y extorsiones	43
1.4.13	Denegación del Servicio (Ataques DoS – <i>Denial of Service</i>)	45
1.4.14	Ataques de Denegación de Servicio Distribuidos (DDoS)	48
1.4.15	Marcadores telefónicos (<i>dialers</i>)	49
1.5	DIRECCIONES DE INTERÉS	50

CAPÍTULO 2. GESTIÓN DE INCIDENTES DE SEGURIDAD..... 53

2.1	INCIDENTES DE SEGURIDAD	53
2.2	IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA	53
2.3	SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)	57
2.3.1	Características básicas de los IDS	57
2.3.2	Tipos de IDS	59
2.3.3	Arquitecturas de los IDS	62
2.4	IPS (<i>INTRUSION PREVENTION SYSTEMS</i>)	63
2.5	LOS <i>HONEYPOTS</i> Y LAS <i>HONEYNETS</i> (SEÑUELOS)	63
2.6	OTRAS HERRAMIENTAS Y APLICACIONES DE UTILIDAD	67
2.7	DIRECCIONES DE INTERÉS	69

CAPÍTULO 3. RESPUESTA ANTE INCIDENTES DE SEGURIDAD..... 71

3.1	DEFINICIÓN DE UN PLAN DE RESPUESTA A INCIDENTES	71
3.1.1	Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)	72
3.1.2	Procedimientos y actividades a realizar	72
3.2	DETECCIÓN DE UN INCIDENTE DE SEGURIDAD: RECOLECCIÓN DE INFORMACIÓN	73
3.3	ANÁLISIS DE UN INCIDENTE DE SEGURIDAD	75

3.4	CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN	76
3.5	IDENTIFICACIÓN DEL ATACANTE Y POSIBLES ACTUACIONES LEGALES.....	77
3.6	COMUNICACIÓN CON TERCEROS Y RELACIONES PÚBLICAS	79
3.7	DOCUMENTACIÓN DEL INCIDENTE DE SEGURIDAD.....	80
3.8	ANÁLISIS Y REVISIÓN A POSTERIORI DEL INCIDENTE: VERIFICACIÓN DE LA INTRUSIÓN.....	81
3.9	PRÁCTICAS RECOMENDADAS POR EL CERT/CC.....	82
3.9.1	Preparación de la respuesta ante incidentes de seguridad.....	82
3.9.2	Gestión del incidente de seguridad	83
3.9.3	Seguimiento del incidente de seguridad	84
3.10	OBLIGACIÓN LEGAL DE NOTIFICACIÓN DE ATAQUES E INCIDENCIAS	84
3.11	PLAN DE RECUPERACIÓN DEL NEGOCIO	85
3.12	ORGANISMOS DE GESTIÓN DE INCIDENTES	89
3.12.1	CERT/CC (<i>Computer Emergency Response Team/Coordination Center</i>)	89
3.12.2	CERT INTECO	89
3.12.3	Agencia Europea de Seguridad de las Redes y de la Información	90
3.12.4	CSRC (<i>Computer Security Resource Center</i>)	90
3.12.5	US-CERT.....	90
3.12.6	FIRST (<i>Forum of Incident Response and Security Teams</i>)	90
3.12.7	Otros centros de seguridad y respuesta a incidentes.....	91
3.12.8	Bases de datos de ataques e incidentes de seguridad	91
3.13	DIRECCIONES DE INTERÉS	92
CAPÍTULO 4. ANÁLISIS FORENSE INFORMÁTICO		95
4.1	OBJETIVOS DE LA INFORMÁTICA FORENSE	95
4.2	ETAPAS EN EL ANÁLISIS FORENSE DE UN INCIDENTE INFORMÁTICO	96
4.2.1	Captura de las evidencias volátiles y no volátiles.....	97
4.2.2	Preservación de las evidencias digitales: cadena de custodia	99
4.2.3	Análisis de las evidencias obtenidas.....	100
4.3	HERRAMIENTAS DE ANÁLISIS FORENSE	102
4.4	ORGANISMOS Y MEDIOS ESPECIALIZADOS EN INFORMÁTICA FORENSE	102
4.5	DIRECCIONES DE INTERÉS	103

CAPÍTULO 5. CIBERTERRORISMO Y ESPIONAJE EN LAS REDES DE ORDENADORES.....	105
5.1 LA AMENAZA DEL CIBERTERRORISMO Y DE LAS GUERRAS INFORMÁTICAS ...	105
5.2 CONSECUENCIAS DE LOS FALLOS Y ATAQUES EN LAS EMPRESAS	109
5.3 EL ESPIONAJE EN LAS REDES DE ORDENADORES	111
5.3.1 El polémico chip “Clipper” y el papel de la NSA	111
5.3.2 ECHELON.....	112
5.3.3 ENFOPOL (<i>Enforcement Police</i>)	114
5.3.4 CARNIVORE	115
5.4 DIRECCIONES DE INTERÉS	116
BIBLIOGRAFÍA	117
ÍNDICE ALFABÉTICO.....	121

EL AUTOR



Álvaro Gómez Vieites es Doctor en Economía por la UNED (con el Premio Extraordinario de Doctorado), Licenciado en Administración y Dirección de Empresas por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo (con el Premio Extraordinario Fin de Carrera) e Ingeniero en Informática de Gestión por la UNED. Su formación se ha completado con los programas de postgrado *Executive MBA* y *Diploma in Business Administration* de la Escuela de Negocios Caixanova.

En la actualidad, es profesor colaborador de esta entidad y de otras Escuelas de Negocios y Universidades, actividad que compagina con proyectos de consultoría y trabajos de investigación en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

Dirección de correo electrónico de contacto: agomezvieites@gmail.com.

INTRODUCCIÓN

Este libro se dedica al estudio de la gestión de incidentes de seguridad informática.

Para ello, el contenido de esta obra se ha estructurado en cinco capítulos:

- En el primer capítulo se analizan las principales amenazas y tipos de ataques a los sistemas informáticos.
- El segundo capítulo se dedica al estudio de la gestión de incidentes de seguridad.
- En el tercer capítulo se presentan los principales aspectos a tener en cuenta en la respuesta ante incidentes de seguridad y en la definición de planes de continuidad del negocio.
- El cuarto capítulo se centra en el estudio de las principales características y procedimientos incluidos en el análisis forense informático.
- En el quinto capítulo se abordan distintos aspectos relacionados con el ciberterrorismo y el espionaje en las redes y sistemas informáticos.

Con todo ello se pretenden aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.
- Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.
- Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

AMENAZAS A LA SEGURIDAD INFORMÁTICA

1.1 CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES

1.1.1 *Hackers*

Los *hackers* son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno.

El perfil típico de un *hacker* es el de una persona joven, con amplios conocimientos de informática y de Internet (son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos, etcétera), que invierte un importante número de horas a la semana a su afición.

La palabra *hacker* proviene etimológicamente del término anglosajón *hack* (que podríamos traducir por “golpear con un hacha”). Este término se utilizaba de forma familiar para describir cómo los técnicos arreglaban las cajas defectuosas del teléfono, asestándoles un golpe seco.

En el ámbito de la informática el movimiento *hacker* surge en los años cincuenta y sesenta en Estados Unidos, con la aparición de los primeros ordenadores. Los primeros *hackers* eran grupos de estudiantes que se imponían como reto conocer el funcionamiento interno y optimizar el uso de estos caros y poco amigables equipos. De hecho, los pioneros fueron unos estudiantes del MIT (Instituto Tecnológico de Massachussets, en Boston) que tuvieron acceso al TX-0, uno de los primeros ordenadores que empleaba transistores en lugar de las válvulas de vacío.

En la actualidad muchos *hackers* defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que solo pretenden mejorar y poner

a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países, puesto que aunque no se produzca ningún daño, se podría revelar información confidencial.

Por otra parte, la actividad de un *hacker* podría provocar otros daños en el sistema: dejar “puertas traseras” que podrían ser aprovechadas por otros usuarios maliciosos, ralentizar su normal funcionamiento, etcétera. Además, la organización debe dedicar tiempo y recursos para detectar y recuperar los sistemas que han sido comprometidos por un *hacker*.

1.1.1.2 Crackers (blackhats)

Los *crackers* son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etcétera.

A principios de los años setenta comienzan a producirse los primeros casos de delitos informáticos, provocados por empleados que conseguían acceder a los ordenadores de sus empresas para modificar sus datos: registros de ventas, nóminas...

1.1.1.3 Sniffers

Los *sniffers* son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.

1.1.1.4 Phreakers

Los *phreakers* son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los *phreakers* desarrollaron las famosas “cajas azules”, que podían emitir distintos tonos en las frecuencias utilizadas por las operadoras para la señalización interna de sus redes, cuando éstas todavía eran analógicas.

1.1.1.5 Spammers

Los *spammers* son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.

Además, muchos de estos mensajes de correo no solicitados pueden contener código dañino (virus informáticos) o forman parte de intentos de estafa realizados a través de Internet (los famosos casos de *phishing*).

1.1.6 Piratas informáticos

Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

1.1.7 Creadores de virus y programas dañinos

Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos, que distribuyen hoy en día a través de Internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.

En estos últimos años, además, han refinado sus técnicas para desarrollar virus con una clara actividad delictiva, ya que los utilizan para obtener datos sensibles de sus víctimas (como los números de cuentas bancarias y de las tarjetas de crédito, por ejemplo) que posteriormente emplearán para cometer estafas y operaciones fraudulentas.

Así, por ejemplo, a principios de febrero de 2006 se daba a conocer la noticia de que tres expertos informáticos rusos habían desarrollado y posteriormente vendido por 4.000 dólares el código de un virus capaz de explotar la vulnerabilidad del sistema de archivos gráficos WMF de Windows. Este código se expandió rápidamente a través de Internet, al insertarse en comentarios de determinados foros o en algunos programas y utilidades muy populares. Estas aplicaciones infectadas provocaban la instalación de varios programas *spyware* y *adware* en el ordenador de la víctima, así como otros códigos maliciosos.

1.1.8 Lamers (*wannabes*): *Script-kiddies* o *Click-kiddies*

Los *lamers*, también conocidos por *script kiddies* o *click kiddies*¹, son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan.

A pesar de sus limitados conocimientos, son los responsables de la mayoría de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas que se pueden descargar fácilmente de Internet, y que pueden ser utilizadas por personas sin conocimientos técnicos para lanzar distintos tipos de ataques contra redes y sistemas informáticos.

1 Términos que podríamos traducir por “niñatos del script” o “niñatos del clic”.

1.1.9 Amenazas del personal interno

También debemos tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática, ya sea de forma voluntaria o involuntaria. Así, podríamos considerar el papel de los empleados que actúan como "fisgones" en la red informática de su organización, los usuarios incautos o despistados, o los empleados descontentos o desleales que pretenden causar algún daño a la organización.

Por este motivo, conviene reforzar la seguridad tanto en relación con el personal interno (*insiders*) como con los usuarios externos del sistema informático (*outsiders*).

1.1.10 Ex empleados

Los ex empleados pueden actuar contra su antigua empresa u organización por despecho o venganza, accediendo en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización. También pueden provocar la activación de "bombas lógicas" para causar determinados daños en el sistema informático (eliminación de ficheros, envío de información confidencial a terceros...) como venganza tras un despido.

1.1.11 Intrusos remunerados

Los intrusos remunerados son expertos informáticos contratados por un tercero para la sustracción de información confidencial, llevar a cabo sabotajes informáticos contra una determinada organización, etcétera.

1.1.12 Algunos hackers, crackers y phreakers famosos

1.1.12.1 JOHN DRAPER, "CAPITÁN CRUNCH"

Fue conocido por aprovechar los silbatos incluidos como regalo en algunas de las cajas de cereales para realizar llamadas telefónicas gratuitas en Estados Unidos a principios de los años setenta. Estos silbatos generaban tonos de una frecuencia de 2.600 Hz, empleada para la señalización interna en las redes y centralitas del operador de telefonía AT&T en Estados Unidos.



Figura 1.1. John Draper

1.1.12.2 VLADIMIR LEVIN

Matemático ruso que en 1995 consiguió acceder a través de Internet desde San Petersburgo al sistema informático central de Citybank en Nueva York, para realizar transferencias por valor de 10 millones de dólares desde cuentas corporativas de esta entidad financiera a otras abiertas por él en entidades de otros países como Rusia, Finlandia, Alemania, Holanda o Suiza. Finalmente fue arrestado por la Interpol en el aeropuerto londinense de Heathrow en 1995, extraditado a Estados Unidos y condenado a tres años de cárcel y a una multa de 240.000 dólares.



Figura 1.2. Vladimir Levin

1.1.12.3 KEVIN POULSON

Famoso *phreaker* de California, que durante un período de dos años consiguió controlar el sistema de conmutación de su operadora de telefonía local. Gracias a sus conocimientos informáticos pudo intervenir la central de conmutación para que su línea personal de teléfono fuera seleccionada como la ganadora en multitud de concursos y ofertas telefónicas, mientras bloqueaba la de otros usuarios del servicio. De este modo, consiguió ganar dos automóviles deportivos Porsche, dos viajes a Hawai y más de 22.000 dólares en efectivo.

Finalmente fue descubierto por el FBI y acusado de diversos delitos: interceptación de comunicaciones y estafas informáticas, entre otros.



Figura 1.3. Kevin Poulson

1.1.12.4 KEVIN MITNICK

Sin lugar a dudas, Kevin Mitnick es el *cracker* más famoso de la historia de la informática. Conocido también por sus apodos "El Cóndor" y "El Chacal de la Red", inició su carrera en 1980, cuando con apenas 16 años consiguió romper la seguridad del sistema informático de su colegio.



Figura 1.4. Kevin Mitnick

En los años ochenta y principios de los noventa Kevin Mitnick se hizo famoso por realizar continuas incursiones en ordenadores de universidades, empresas de informática y telecomunicaciones, la NASA o el mismísimo Departamento de Defensa de Estados Unidos, consiguiendo acceder a valiosa información confidencial.

Sus “hazañas” costaron muchos millones de dólares al gobierno de los Estados Unidos. Por este motivo, su foto llegó a estar en la lista de los delincuentes más buscados por el FBI, que le persiguió durante tres años hasta que finalmente consiguió detenerlo en febrero de 1995, gracias a la colaboración del experto informático Tsutomu Shimomura, un miembro del Centro de Supercomputación de San Diego que también había sufrido uno de los ataques de Kevin Mitnick.

Tras cumplir una condena en la cárcel, fue puesto en libertad en enero de 2000, si bien Mitnick tuvo absolutamente prohibido el uso de ordenadores, teléfonos móviles, televisores o cualquier equipo electrónico capaz de conectarse a Internet hasta el año 2003. Actualmente se dedica a impartir conferencias y seminarios sobre seguridad informática, escribe artículos y libros sobre seguridad informática e incluso aparece como personaje en videojuegos como *Vampire*.

1.2 MOTIVACIONES DE LOS ATACANTES

El FBI ha acuñado el acrónimo MICE para resumir las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: *Money*, *Ideology*, *Compromise* y *Ego* (Dinero, Ideología, Compromiso y Autorrealización personal).

En general, podemos considerar la siguiente tipología de motivaciones de los atacantes:

- Consideraciones económicas: llevar a cabo operaciones fraudulentas; robo de información confidencial que posteriormente es vendida a terceros; extorsiones (si no se paga un determinado “rescate” se elimina información o se daña de forma irreparable un sistema que haya sido comprometido); intentos de manipulación de las cotizaciones de valores bursátiles; etcétera.
- Diversión: algunos usuarios de Internet realizan estos ataques como una forma de pasar el rato delante de su ordenador.
- Ideología: ataques realizados contra determinadas organizaciones, empresas y *websites* gubernamentales, con un contenido claramente político.

- Autorrealización.
- Búsqueda de reconocimiento social y de un cierto estatus dentro de una comunidad de usuarios.

1.3 FASES DE UN ATAQUE INFORMÁTICO

Los ataques contra redes de ordenadores y sistemas informáticos suelen constar de las etapas o fases que se presentan a continuación:

- Descubrimiento y exploración del sistema informático.
- Búsqueda de vulnerabilidades en el sistema.
- Explotación de las vulnerabilidades detectadas (para ello, se suelen utilizar herramientas específicamente construidas para tal fin, conocidas como *exploits*).
- Corrupción o compromiso del sistema: modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado; etcétera.
- Eliminación de las pruebas que puedan revelar el ataque y el compromiso del sistema: eliminación o modificación de los registros de actividad del equipo (*logs*); modificación de los programas que se encargan de monitorizar la actividad del sistema; etcétera. Muchos atacantes llegan incluso a parchear la vulnerabilidad descubierta en el sistema para que no pueda ser utilizada por otros intrusos.

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque (como podría ser el caso de un fallo en la seguridad del sistema informático elegido).

Estos tres factores constituyen lo que podríamos denominar como el **Triángulo de la Intrusión**, concepto que se presenta de forma gráfica en la siguiente figura:

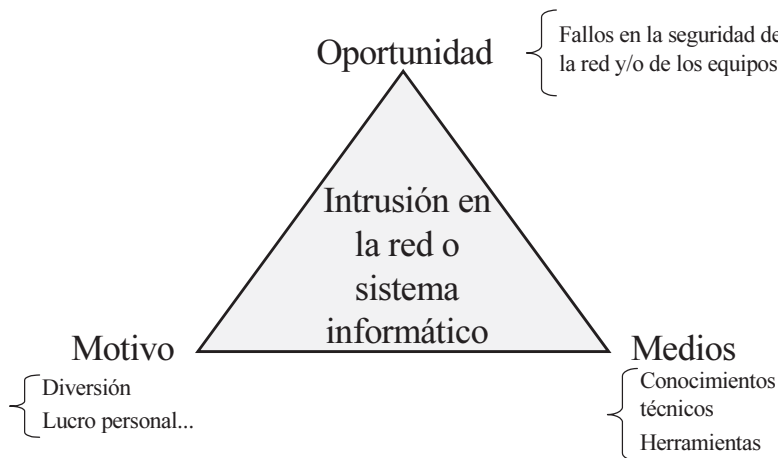


Figura 1.5. El "Triángulo de la Intrusión"

En cuanto a los medios y herramientas disponibles en la actualidad para llevar a cabo sus ataques (*Hacking Tools*), podríamos citar los siguientes:

- Escáneres de puertos: que permiten detectar los servicios instalados en un determinado sistema informático.
- *Sniffers*: dispositivos que capturan los paquetes de datos que circulan por una red. Para ello, también se podría utilizar un equipo conectado a la red con su tarjeta de red (NIC) configurada en "modo promiscuo", para poder procesar todo el tráfico que recibe (aunque vaya dirigido a otros equipos). Por otra parte, existen *sniffers* especializados en la captura de contraseñas u otros datos sensibles (como los números de cuenta o de tarjetas de crédito).
- *Exploits*: herramientas que buscan y explotan vulnerabilidades conocidas.
- *Backdoors kits*: programas que permiten abrir y explotar "puertas traseras" en los sistemas.
- *Rootkits*: programas utilizados por los atacantes para ocultar "puertas traseras" en los propios ficheros ejecutables y servicios del sistema, que son modificados para facilitar el acceso y posterior control del sistema.
- *Auto-rooters*: herramientas capaces de automatizar totalmente un ataque, realizando toda la secuencia de actividades para localizar un sistema, escanear sus posibles vulnerabilidades, explotar una determinada vulnerabilidad y obtener el acceso al sistema comprometido.
- *Password crackers*: aplicaciones que permiten averiguar las contraseñas de los usuarios del sistema comprometido.

- Generadores de virus y otros programas malignos.
- Herramientas que facilitan la ocultación y la suplantación de direcciones IP (técnicas de *spoofing*), dificultando de este modo la identificación del atacante.
- Herramientas de cifrado y protocolos criptográficos (como PGP, SSH, SSL o IPSec): cada vez es más frecuente que el atacante utilice protocolos criptográficos en sus conexiones con los sistemas y máquinas que ha conseguido comprometer, dificultando de este modo su detección y estudio.

1.4 TIPOS DE ATAQUES INFORMÁTICOS

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los **ataques activos**, que producen cambios en la información y en la situación de los recursos del sistema, y los **ataques pasivos**, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

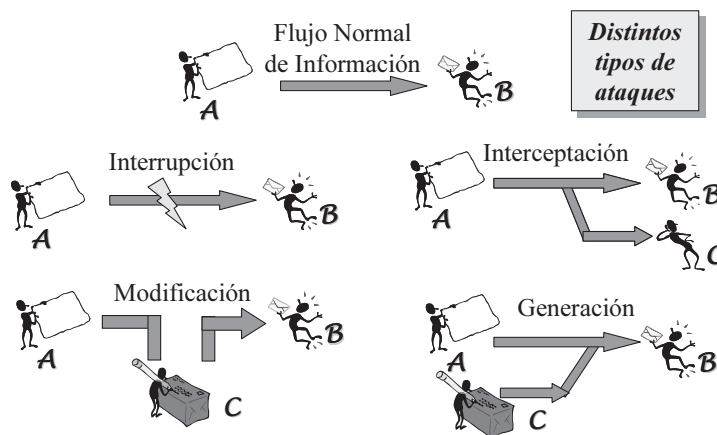


Figura 1.6. Distintos tipos de ataques en una red de ordenadores

Seguidamente se presenta una relación de los principales tipos de ataques contra redes y sistemas informáticos:

1.4.1 Actividades de reconocimiento de sistemas

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando

para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

Así, se puede obtener importante información sobre las organizaciones y empresas presentes en Internet, los nombres de dominio y las direcciones IP que éstas tienen asignadas, por medio de consultas en servicios como *Whois*, que mantiene una base de datos sobre direcciones IP y nombres de dominio necesaria para el correcto funcionamiento de Internet.

Para ello, se podrían consultar las siguientes fuentes de información sobre nombres de dominio y asignación de direcciones IP en Internet:

- Base de datos Whois de InterNIC (Internet Network Information Center): www.internic.net/whois.html.
- Servicio de Información de RIPE-NCC (Réseaux IP Européens Network Coordination Center) para Europa: www.ripe.net.
- Servicio de Información de ARIN (American Registry for Internet Numbers): www.arin.net.
- Servicio de Información de APNIC (Asian Pacific Network Information Center), para la región de Asia-Pacífico: www.apnic.net.
- Servicio de Información de LACNIC (Latin America and Caribbean Internet Addresses Registry): <http://lacnic.net>.

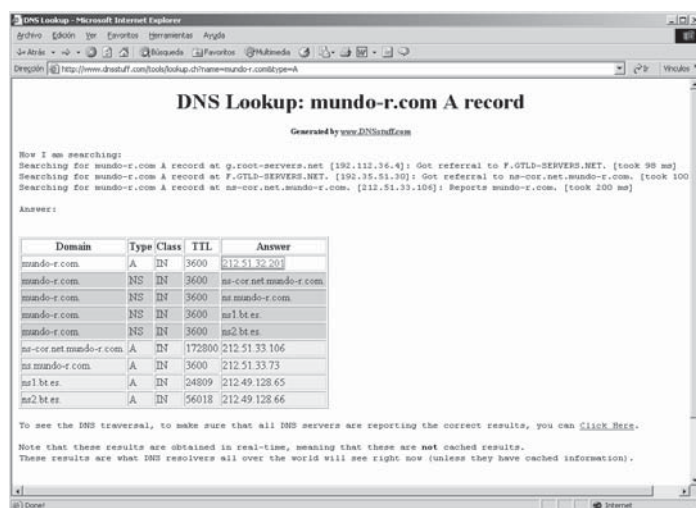


Figura 1.7. Consulta de la ficha de información sobre un determinado nombre de dominio, perteneciente en este caso a un operador de telecomunicaciones

En las consultas a servicios como *Whois* también se puede obtener información relevante sobre las personas que figuran como contactos técnicos y administrativos en representación de una organización (podría facilitar diversos ataques basados en la "Ingeniería Social"); datos para la facturación (*billing address*); direcciones de los servidores DNS de una organización; fechas en que se han producido cambios en los registros; etcétera.

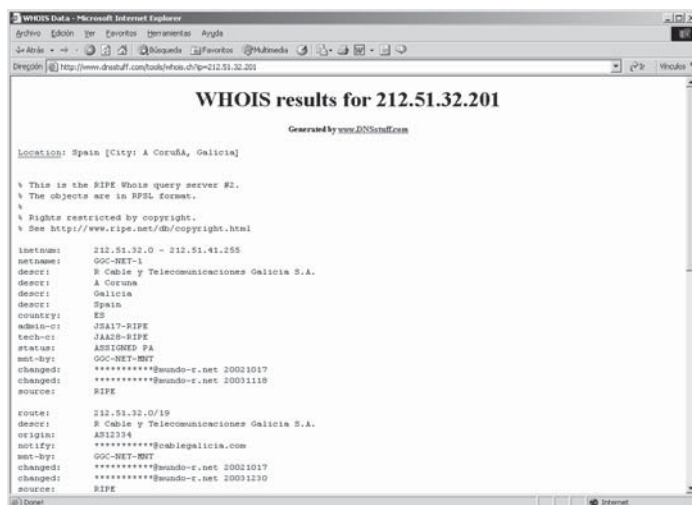


Figura 1.8. Acceso a la base de datos Whois

Por otra parte, se podrían utilizar herramientas que facilitan todos estos tipos de consultas, como podría ser el caso de "DNS Stuff" (www.dnsstuff.com).

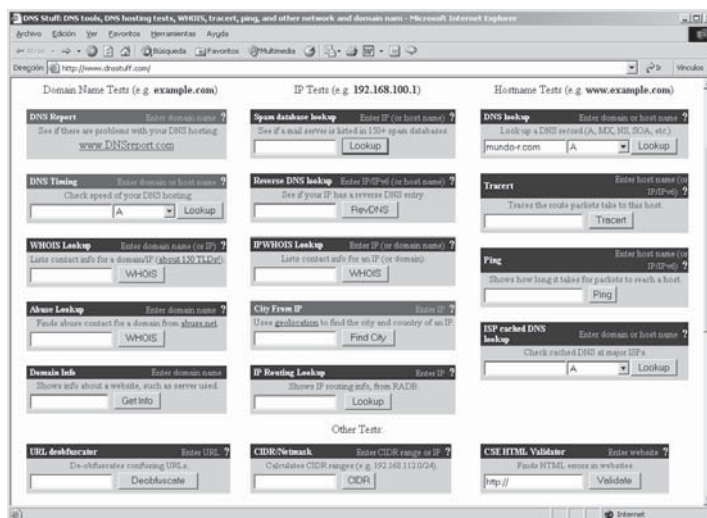


Figura 1.9. DNS Stuff

Los intrusos también podrían recurrir a la información que facilitan los propios servidores de nombre de dominio de la organización (servidores DNS). Para realizar consultas a un servidor DNS se pueden utilizar herramientas como “nslookup”. Si el servicio DNS no se ha configurado adecuadamente, un usuario externo podría realizar una consulta de transferencia de zona completa, obteniendo de este modo toda la información sobre la correspondencia de direcciones IP a nombres de equipos, las relaciones entre equipos de una organización, o el propósito para el que emplean. Así mismo, mediante una consulta al servicio de nombres de dominio se pueden localizar los servidores de correo de una organización (los cuales figuran como registros MX en una base de datos DNS). Por todo ello, conviene configurar los servidores DNS (o filtrar el tráfico hacia estos servidores en los cortafuegos) para evitar este tipo de transferencias hacia equipos externos.

Para detectar cuáles son los ordenadores conectados a una red informática y obtener información adicional sobre su topología se podrían utilizar herramientas como *Ping* o *Traceroute*.

Así, el servicio PING² (*Packet Internet Groper*) permite detectar si un determinado ordenador se encuentra activo y conectado a la red. Para ello, se envía un paquete de control ICMP (paquete “ECHO”) a la dirección IP del equipo y se espera la respuesta por parte de éste (paquete “REPLY”).

Por su parte, la herramienta *Traceroute* proporciona una relación de todos los equipos incluidos en una ruta entre dos equipos determinados. Para ello, se envían una serie de paquetes de control ICMP que permiten determinar el número de saltos (nodos o equipos que hay que atravesar) necesarios para alcanzar un determinado equipo (*host*) destinatario. El número de saltos se determina mediante el campo TTL de la cabecera IP de un paquete, que actúa como un contador de saltos que se va decrementando en una unidad cada vez que el paquete es reenviado por un *router*. Existen herramientas gráficas con una funcionalidad similar a *Traceroute* que permiten visualizar las correspondientes asociaciones de cada elemento IP y su localización en un mapa mundial.

También se puede obtener información interesante sobre una organización recurriendo al análisis de sus páginas web publicadas en Internet, en especial de la revisión del código fuente y de los comentarios incluidos en el propio código de las páginas HTML, ya que permitirán averiguar qué herramientas utilizó el programador para su construcción, así como alguna otra información adicional sobre el sistema (tipo de servidor o base de datos utilizada, por ejemplo).

Para llevar a cabo la identificación de versiones de sistemas operativos y aplicaciones instaladas es necesario obtener lo que se conoce como **huellas identificativas** del sistema: cadenas de texto que identifican el tipo de servicio y su versión, y que se incluyen en las respuestas a las peticiones realizadas por los equipos clientes del servicio en cuestión.

² El nombre de PING proviene del mundo del sonar, siendo en este caso el pulso sonoro enviado para localizar objetos en un medio submarino.

Se conoce con el nombre de *fingerprinting* al conjunto de técnicas y habilidades que permiten extraer toda la información posible sobre un sistema. Los atacantes utilizarán esta información para tratar de explorar las vulnerabilidades potenciales del sistema en cuestión.

En este sentido, muchos ataques comienzan llevando a cabo un análisis de las respuestas que genera un sistema informático a determinadas peticiones en un servicio o protocolo, ya que existen distintas implementaciones de servicios y protocolos TCP/IP (distintas interpretaciones de los estándares propuestos en los documentos que describen el funcionamiento de Internet –RFC–). Para ello, los intrusos se encargan de monitorizar los bits de estado y de control de los paquetes IP, los números de secuencia generados, la gestión de la fragmentación de paquetes por parte del servidor, el tratamiento de las opciones del protocolo TCP (RFC 793 y 1323), etcétera.

En cuanto a las actividades de escaneo de puertos, éstas tienen lugar una vez que se ha localizado e identificado un determinado equipo o servidor conectado a Internet, para descubrir los servicios que se encuentran accesibles en dicho sistema informático (es decir, cuáles son los puntos de entrada al sistema).

Se puede recurrir a distintas técnicas de escaneo, siendo las más conocidas las que se describen a continuación:

- Técnica “TCP Connect Scanning”:

Esta técnica de escaneo es la más sencilla, ya que consiste en el envío de un paquete de intento de conexión al puerto del servicio que se pretende investigar, para comprobar de este modo si el sistema responde aceptando la conexión o denegándola. No obstante, esta técnica es fácilmente detectable, por lo que se puede configurar al sistema informático para que no responda a este tipo de acciones.

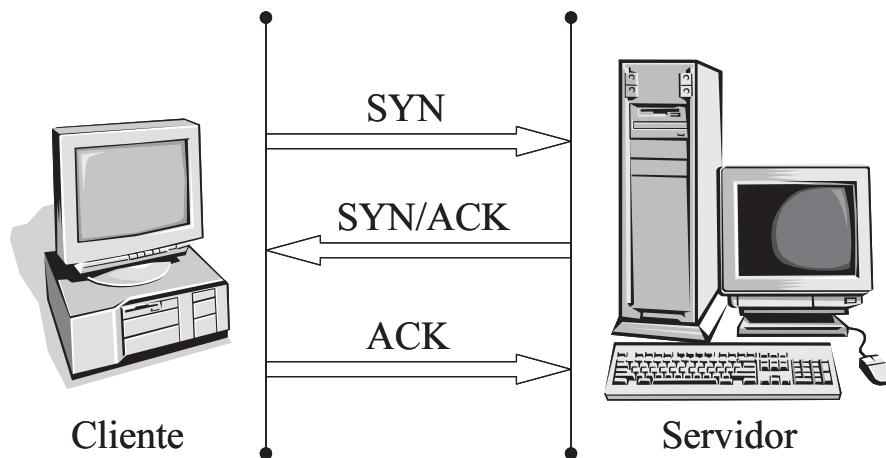


Figura 1.10. Técnica “TCP Connect Scanning”

- Técnica "TCP SYN Scanning":

En esta técnica de escaneo se intenta abrir la conexión con un determinado puerto para a continuación, en cuanto se confirma que el puerto está abierto, enviar un paquete "RST" que solicita terminar la conexión. Esta técnica de escaneo no es registrada por algunos servidores.

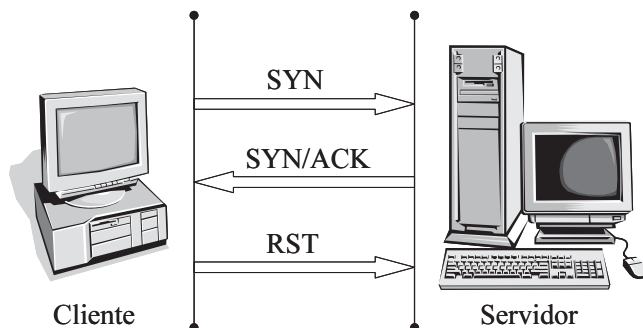


Figura 1.11. Técnica "TCP SYN Scanning"

- Técnica "TCP FIN Scanning":

También conocida como *Stealth Port Scanning* (Escaneo Oculto de Puertos), ha sido propuesta como una técnica de escaneo que trata de evitar ser registrada por los cortafuegos y servidores de una organización.

Se trata, por lo tanto, de una técnica más avanzada que las anteriores, que consiste en el envío de un paquete "FIN" de exploración, de forma que si el puerto está abierto, el servidor ignorará este paquete, mientras que si el puerto está cerrado, el servidor responderá con un paquete "RST". Algunos sistemas, como los de Microsoft, no cumplen de forma estricta el protocolo TCP, respondiendo siempre con un paquete "RST" ante un paquete "FIN", independientemente de si el puerto se encuentra abierto o cerrado (por este motivo, no son vulnerables a este tipo de técnica de escaneo).

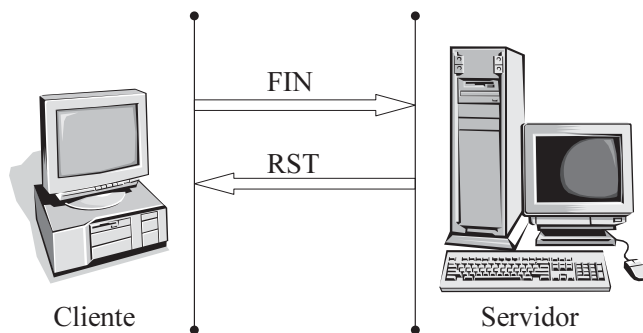


Figura 1.12. Técnica "TCP FIN Scanning"

Otras técnicas de escaneo de puertos:

- **"TCP Null Scanning"**: en esta técnica se envía un paquete TCP con todos los *flags* a cero en su cabecera.
- **"TCP ACK Scanning"**: técnica que permite determinar si un cortafuegos actúa simplemente como filtro de paquetes o mantiene el estado de las sesiones.
- **"TCP Fragmentation Scanning"**: técnica de escaneo que recurre a la fragmentación de paquetes TCP.
- **"TCP Window Scanning"**: permite reconocer determinados puertos abiertos a través del tamaño de ventana de los paquetes TCP.
- **"TPC RPC Scanning"**: en los sistemas UNIX esta técnica permite obtener información sobre puertos abiertos en los que se ejecutan servicios de llamada a procedimientos remotos (RPC).
- **"UDP ICMP Port Unreachable Scanning"**: técnica que emplea paquetes UDP para tratar de localizar algunos puertos abiertos.
- Técnicas que se basan en el análisis de los mensajes de error generados ante paquetes de control ICMP malformados enviados a un equipo: modificación maliciosa de la cabecera del paquete, uso de valores inválidos, etcétera.

Los atacantes pueden utilizar numerosas herramientas disponibles en Internet que facilitan el escaneo de puertos, como podrían ser NMAP para UNIX (www.insecure.org/nmap/) o NetScan Tools para Windows (www.nwpsw.com).

1.4.2 Detección de vulnerabilidades en los sistemas

Este tipo de ataques tratan de detectar y documentar las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como *exploits*).

1.4.3 Robo de información mediante la interceptación de mensajes

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

1.4.4 Modificación del contenido y secuencia de los mensajes transmitidos

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como "ataques de repetición" (*replay attacks*).

1.4.5 Análisis del tráfico

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los *sniffers*. Así, se conoce como *eavesdropping* a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

Una organización podría protegerse frente a los *sniffers* recurriendo a la utilización de redes conmutadas (*switches* en lugar de *hubs*) y de redes locales virtuales (VLAN).

No obstante, en redes locales que utilizan *switches* (es decir, en redes conmutadas), un atacante podría llevar a cabo un ataque conocido como *MAC flooding* para provocar un desbordamiento de las tablas de memoria de un *switch* (tablas denominadas CAM por los fabricantes, *Content Addressable Memory*) para conseguir que pase a funcionar como un simple *hub* y retransmita todo el tráfico que recibe a través de sus puertos (al no poder "recordar" qué equipos se encuentran conectados a sus distintas bocas o puertos por haber sido borradas sus tablas de memoria).

Por otra parte, en las redes VLAN (redes locales virtuales) un atacante podría aprovechar el protocolo DTP (*Dynamic Trunk Protocol*), utilizado para poder crear una VLAN que atravesase varios *switches*, para intentar saltar de una VLAN a otra, rompiendo de este modo el aislamiento físico impuesto por la organización para separar sus distintas redes locales.

También podemos mencionar las técnicas que permiten monitorizar las emisiones electromagnéticas de los equipos (previstas en la normativa TEMPEST) para detectar los datos y comandos que se han introducido a través del teclado, la información visualizada en el monitor o, simplemente, los datos que se han guardado en el propio disco duro del equipo en cuestión.

1.4.6 Ataques de suplantación de la identidad

1.4.6.1 IP SPOOFING

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada *IP Spoofing* ("enmascaramiento de la dirección IP"), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado. En el documento RFC 2267 se ofrece información detallada sobre el problema del *IP Spoofing*.

Los propietarios de las redes y operadores de telecomunicaciones podrían evitar en gran medida el *IP Spoofing* implantando filtros para que todo el tráfico saliente de sus redes llevara asociado una dirección IP de la propia red desde la que se origina el tráfico.

Otro posible ataque sería el secuestro de sesiones ya establecidas (*hijacking*), donde el atacante trata de suplantar la dirección IP de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir. Con el secuestro de sesiones se podrían llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático como, por ejemplo, transferencias desde sus propias cuentas corrientes si en ese momento se encuentra conectado al servidor de una entidad financiera.

Por otra parte, también se han llevado a cabo ataques contra el protocolo ARP (*Address Resolution Protocol*), encargado de resolver las direcciones IP y convertirlas en direcciones físicas en una red local. Mediante estos ataques es posible secuestrar una determinada dirección física³ de la tarjeta de red de un equipo, para hacerse pasar por este equipo ante el resto de los ordenadores conectados a esa red local.

Para ello, el atacante se encarga de enviar paquetes ARP falsos a la víctima en respuesta a sus consultas, cuando trata de averiguar cuál es la dirección física que se corresponde con una determinada dirección IP, antes de que lo haga el equipo legítimo, pudiendo llevar a cabo de este modo un ataque del tipo *man-in-the-middle* ("hombre en el medio"): el equipo del atacante intercepta los paquetes de datos y los reenvía posteriormente a la víctima, sin que los dos equipos que intervienen de forma legítima en la comunicación sean conscientes del problema.

3 También conocida como dirección MAC (Medium Access Control).



Figura 1.13. Ataque man-in-the-middle: el intruso C intercepta la información que el usuario A envía a través de la red, reenviándola posteriormente al usuario B

1.4.6.2 DNS SPOOFING

Los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas web falsas o bien la interceptación de sus mensajes de correo electrónico.

Para ello, en este tipo de ataque los intrusos consiguen que un servidor DNS legítimo acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecerla. De este modo, se persigue “inyectar” información falsa en el base de datos del servidor de nombres, procedimiento conocido como “envenenamiento de la caché del servidor DNS”, ocasionando con ello serios problemas de seguridad, como los que se describen de forma más detallada a continuación:

- Redirección de los usuarios del servidor DNS atacado a *websites* erróneos en Internet, que simulan ser los *websites* reales. De este modo, los atacantes podrían provocar que los usuarios descargasen de Internet software modificado en lugar del legítimo (descarga de código dañino, como virus o troyanos, desde *websites* maliciosos).
- La manipulación de los servidores DNS también podría estar detrás de algunos casos de *phishing*, mediante la redirección de los usuarios hacia páginas web falsas creadas específicamente con la intención de obtener datos confidenciales, como sus claves de acceso a servicios de banca electrónica.
- Otra posible consecuencia de la manipulación de los servidores DNS serían los ataques de Denegación de Servicio (DoS), al provocar la redirección permanente hacia otros servidores en lugar de hacia el verdadero, que de este modo no podrá ser localizado y, en consecuencia, visitado por sus legítimos usuarios.
- Los mensajes de correo podrían ser redirigidos hacia servidores de correo no autorizados, donde podrían ser leídos, modificados o eliminados. Para ello, basta con modificar el registro MX (*Mail Exchanger*) de la tabla de datos del servidor DNS atacado.

Por otra parte, un servidor DNS afectado por este tipo de ataque podría provocar falsas respuestas en los restantes servidores DNS que confíen en él para resolver un nombre de dominio, siguiendo el modelo jerárquico del servicio DNS, extendiendo de este modo el alcance del ataque de *DNS Spoofing*.

El procedimiento seguido en el ataque consiste en engañar a un equipo que trate de acceder a un servidor DNS legítimo. Para ello, el atacante debe identificar cuál es la dirección IP de un servidor DNS real y responder con información falsa antes de que lo haga el verdadero servidor DNS, empleando un identificador adecuado en el mensaje de respuesta (se trata de un identificador asociado a cada consulta realizada al servidor DNS) para que sea dado por válido por el equipo que realiza la consulta, equipo que podría ser el propio servidor DNS interno de la organización, con lo que se estaría introduciendo información falsa en su base de datos.

En una red LAN se puede emplear un *sniffer* para obtener el identificador de la petición en cuestión. El atacante también podría probar aleatoriamente con todos los valores que podría adoptar el identificador, o bien proceder al envío de algunas decenas de consultas DNS para aumentar la oportunidad de alcanzar el identificador de secuencia correcto a partir de alguna predicción anterior.

Así mismo, es posible emplear vulnerabilidades conocidas de predicción de identificadores de consultas DNS. Así, por ejemplo, las versiones antiguas del servidor DNS BIND de UNIX utilizaban un identificador aleatorio para comenzar las consultas y después solo incrementaban el número para identificar las siguientes preguntas, por lo que resultaba muy fácil explotar esta vulnerabilidad.

Otra posible alternativa para llevar a cabo ataques de *DNS Spoofing* sería recurrir a la utilización de virus informáticos que puedan modificar la configuración del protocolo TCP/IP del equipo infectado. Uno de estos virus es el denominado "Qhosts/Delude", dado a conocer en octubre de 2003 y que se caracteriza por realizar una serie de cambios en la configuración TCP/IP del equipo identificado, modificando las direcciones de los servidores de DNS y creando un nuevo archivo HOSTS en el disco duro para que, de esta forma, se puedan redireccionar de forma transparente determinadas peticiones de acceso a servicios de Internet, es decir, el equipo infectado utilizará a partir de ese momento un servidor de nombres ilegítimo, que podría estar bajo el control del creador del virus.

Por otra parte, en octubre de 2005 se daba a conocer la existencia de un nuevo código malicioso, denominado *PremiumSearch*, capaz de engañar a los usuarios de los populares buscadores Google, Yahoo! y MSN, reenviando a los usuarios afectados a enlaces falsos. En este caso, la infección tiene lugar cuando se visita una determinada página web con contenido malicioso, a la que el usuario accede tras haber sido redirigido desde otras páginas con otros contenidos. La infección de *PremiumSearch* comienza con la instalación en el equipo de un fichero BHO (*Browser Helper Object*) malicioso, aprovechando algunas de las vulnerabilidades más utilizadas para la instalación de *spyware*. Como consecuencia de esta acción se lleva a cabo la instalación de una barra de herramientas de Google modificada por terceros (no se trata de la legítima de Google) y se modifica el fichero HOSTS del equipo. La modificación del fichero HOSTS y la instalación del objeto BHO malicioso en el navegador tienen como

consecuencia que los usuarios que soliciten las páginas de los buscadores MSN, Yahoo! y Google obtengan una versión falsa, indistinguible de la original salvo porque muestra una serie de resultados modificados en primer lugar, a los que se añaden a continuación (pero no en primer lugar) los que normalmente mostrarían estos buscadores. Además, las búsquedas realizadas sobre la falsa barra de Google también devuelven los mismos resultados modificados.

Llegado a este punto, conviene destacar un problema adicional de los servidores DNS, y es que se suelen dedicar a esta función equipos antiguos y con un mantenimiento deficiente, ejecutando versiones obsoletas de sistemas operativos, sin los parches y actualizaciones recomendadas por los fabricantes. Además, los administradores suelen prestar poca atención a la configuración y mantenimiento de estos equipos. De hecho, un estudio realizado en 2003 por Men & Mice (www.menandmice.com) revelaba que el 68,4% de los servidores DNS presentaba una configuración insegura, facilitando de este modo los ataques de *DNS Spoofing*.

Una configuración más segura del servicio DNS se podría alcanzar mediante la separación en dos servidores DNS: un servidor interno para responder a las consultas de los equipos pertenecientes a la red local de la organización, mientras que otro servidor DNS externo se encargaría de la información pública del servicio DNS. De este modo, se trataría de evitar el problema de “envenenamiento de la caché” del servidor DNS.

Por último, conviene señalar que se ha desarrollado una nueva versión del servicio DNS, conocida como DNS Seguro (DNSSec), explicada en el RFC 2535 y siguientes (se puede obtener más información sobre DNSSec en la página web <http://www.dnssec.net/>). Esta nueva versión del servicio DNS trata de garantizar la integridad de la información del servidor de nombres, así como su autenticidad, mediante la utilización de algoritmos criptográficos seguros.

1.4.6.3 CAMBIOS EN EL REGISTRO DE NOMBRES DE DOMINIO DE INTERNIC

El registro de nombres de dominio utiliza un sistema de autenticación de usuarios registrados con un bajo nivel de seguridad. Este proceso de autenticación es necesario para poder solicitar cambios ante InterNIC (base de datos central con los nombres de dominio registrados en Internet) o ante alguna de las empresas registradoras de nombres de dominio. Aprovechando esta debilidad en el proceso de autenticación, un usuario malicioso podría tratar de realizar un cambio en el registro de nombres de dominio para provocar una redirección del tráfico destinado a unos determinados dominios hacia otras máquinas, o bien un ataque de Denegación de Servicio contra una determinada organización.

Así, por ejemplo, el 16 de octubre de 1998 alguien envió un mensaje de correo falso a InterNIC, supuestamente en nombre de la empresa America Online, para cambiar la ficha de registro del dominio “aol.com”, provocando la redirección durante unas horas de todo el tráfico destinado a America Online hacia el proveedor Autonet.net.

Debido a este problema de seguridad en el registro de nombres de dominio, en estos últimos años se ha tratado de reforzar el proceso de autenticación de los usuarios antes de aceptar cambios en las fichas de los nombres de dominio.

No obstante, debemos destacar otro posible problema para las organizaciones que, por desgracia, puedan pasar por alto la renovación de los nombres de dominio. Así, la caducidad en la concesión de los nombres de dominio registrados provoca su automática liberación, por lo que podrían ser concedidos a otras empresas o personas físicas que también los hayan solicitado.

1.4.6.4 SMTP SPOOFING

El envío de mensajes con remitentes falsos (*masquerading*) para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario. De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección. Así mismo, este tipo de ataque es muy utilizado por los *spammers*, que envían gran cantidad de mensajes de "correo basura" bajo una identidad falsa.

En la actualidad, falsificar mensajes de correo resulta bastante sencillo porque el protocolo SMTP carece totalmente de autenticación. Así, un servidor configurado para aceptar conexiones SMTP en el puerto 25 podría ser utilizado por un usuario externo a la organización, empleando los comandos propios del protocolo, para que envíe mensajes que aparenten tener un origen seleccionado por el atacante cuando realmente tienen otro distinto. La dirección de origen puede ser una dirección existente o una inexistente con el formato adecuado.

No obstante, los servidores de correo también podrían ser configurados para no aceptar envíos de mensajes desde equipos externos a la red local.

1.4.6.5 CAPTURA DE CUENTAS DE USUARIO Y CONTRASEÑAS

También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como los programas de software espía o los dispositivos hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador⁴ (*keyloggers*). De hecho, es posible localizar soluciones disponibles en el mercado como KeyGhost (www.keyghost.com) o KeyLogger (www.keylogger.com).

⁴ Son dispositivos hardware que se pueden conectar al puerto donde se encuentra conectado el teclado, interceptando de este modo la comunicación entre el teclado y la placa base del ordenador.



Figura 1.14. KeyGhost

Se conoce como *snooping* a la técnica que permite observar la actividad de un usuario en su ordenador para obtener determinada información de interés, como podrían ser sus contraseñas. Los programas que permiten realizar esta actividad se conocen con el nombre de *snoopers*, los cuales pueden ser troyanos u otros “parásitos” que monitorizan dispositivos de entrada como los ratones y los teclados.

Por otra parte, mediante las técnicas de “Ingeniería Social” un usuario podría ser engañado por una persona ajena a la organización para que le facilite sus contraseñas y claves de acceso.

1.4.7 Modificaciones del tráfico y de las tablas de enrutamiento

Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos.

Así, la utilización del encaminamiento fuente (*source routing*) en los paquetes IP permite que un atacante pueda especificar una determinada ruta prefijada, que podría ser empleada como ruta de retorno, saltándose todas las reglas de enrutamiento definidas en la red. De este modo, utilizando además el *IP Spoofing*, un atacante se podría hacer pasar por cualquier máquina en la que el destino pueda confiar, para recibir a continuación los datos correspondientes al equipo que está suplantando.

También es posible llevar a cabo una modificación de las tablas de enrutamiento, utilizando para ello determinados paquetes de control del tráfico, conocidos como paquetes ICMP Redirect⁵, que permiten alterar la ruta a un determinado destino. Otra alternativa sería la de modificar las rutas a través de los propios protocolos de enrutamiento utilizados, como RIP (puerto UDP 520) o BGP.

Al modificar las rutas, el tráfico atravesará otros equipos y redes antes de alcanzar su destinatario final, facilitando de este modo el *sniffing*.

5 Estos paquetes de datos de control se utilizan para informar de rutas alternativas.

1.4.8 Conexión no autorizada a equipos y servidores

Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos destacar las siguientes:

- Violación de sistemas de control de acceso.
- Explotación de “agujeros de seguridad” (*exploits*).
- Utilización de “puertas traseras” (*backdoors*), conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, que permiten acceder o tomar el control del equipo saltándose los controles de seguridad.
- Utilización de *rootkits*, programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo. Los *rootkits*, además de cumplir con las funciones de la herramienta o servicio que reemplazan en el equipo para no despertar sospechas, incorporan otras funciones ocultas que facilitan, entre otras cosas, el control remoto del equipo comprometido.
- *Wardialing*: conexión a un sistema informático de forma remota a través de un módem. Los *wardialers* son dispositivos que permiten realizar de forma automática multitud de llamadas telefónicas para tratar de localizar módems que se encuentren a la espera de nuevas conexiones y que no hayan sido protegidos y configurados de forma adecuada.

Tampoco debemos olvidar las posibles pérdidas o robos de equipos que contienen información sensible y que, por este motivo, puedan caer en manos de personas ajenas a la organización, las cuales podrían tratar de tomar el control de estos equipos para extraer la información que almacenan o para utilizarlos en conexiones remotas a la red de la organización.

1.4.9 Consecuencias de las conexiones no autorizadas a los sistemas informáticos

Las conexiones no autorizadas a los sistemas informáticos pueden acarrear graves consecuencias para la organización afectada por este tipo de ataques e incidentes, entre las que podríamos destacar las siguientes:

- Acceso a información confidencial guardada en un servidor. Los atacantes incluso podrían tener acceso a datos y ficheros que habían sido “borrados” del sistema⁶.
- Utilización inadecuada de determinados servicios por parte de usuarios no autorizados, suponiendo una violación de los permisos establecidos en el sistema.
- Transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización (*mail relaying*). Esto podría facilitar el reenvío masivo de mensajes de *spam* a través de un servidor SMTP configurado de forma inadecuada.
- Utilización de la capacidad de procesamiento de los equipos para otros fines, como, por ejemplo, para tratar de romper las claves criptográficas de otros sistemas.
- Creación de nuevas cuentas de usuario con privilegios administrativos, que faciliten posteriores accesos al sistema comprometido.
- Consumo del ancho de banda de la red de la organización para otros fines.
- Almacenamiento de contenidos ilegales en los equipos: muchos atacantes aprovechan los equipos comprometidos de una organización para guardar y distribuir copias piratas de software, canciones o vídeos, pornografía infantil...
- Modificación o destrucción de archivos y documentos guardados en un servidor.
- *Website vandalism*: modificación del contenido y de la apariencia de unas determinadas páginas web pertenecientes a la organización.

1.4.10 Introducción en el sistema de *malware* (código malicioso)

1.4.10.1 VIRUS INFORMÁTICOS, TROYANOS Y GUSANOS

Entendemos por código malicioso o dañino (*malware*) cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, bombas lógicas, etcétera.

Cabe destacar la rapidez de propagación de estos programas dañinos a través del correo electrónico, las conexiones mediante redes de ordenadores y los servicios de intercambio de ficheros (P2P) o de mensajería instantánea.

⁶ Ficheros o documentos que figuraban como eliminados del Sistema de Ficheros, pero que todavía figuran intactos en el disco duro del equipo.

Hasta ahora algunos técnicos y administradores de redes se centraban en otros problemas de mayor nivel de complejidad, como los ataques contra servidores por parte de *crackers* o el análisis de agujeros de seguridad, relegando la protección contra los virus y códigos dañinos a un segundo plano, ya que se consideraba como una tarea que realizan de forma automática los programas antivirus.

Sin embargo, las nuevas formas de propagación de estos códigos dañinos y los graves problemas que ocasionan a las empresas y a los usuarios obligan a replantearse esta estrategia, prestando una mayor atención a la contención y erradicación de este tipo de ataques e incidentes de seguridad informática.

1.4.10.2 ATAQUES DE “*CROSS-SITE SCRIPTING*” (XSS)

Los ataques de *Cross-Site Scripting* consisten básicamente en la ejecución de código *Script*⁷ (como Visual Basic Script o Java Script) arbitrario en un navegador, en el contexto de seguridad de la conexión a un determinado servidor Web.

Son ataques dirigidos, por lo tanto, contra los usuarios y no contra el servidor Web. Así, mediante *Cross-Site Scripting*, un atacante puede realizar operaciones o acceder a información guardada en un servidor Web en nombre del usuario afectado, suplantando su identidad.

Estos ataques se pueden producir cuando el servidor Web no filtra correctamente las peticiones HTTP de los usuarios, los cuales pueden enviar cadenas de texto a través de formularios o directamente a través de la propia dirección URL de la página web. Estas cadenas de texto podrían incluir código en lenguaje *Script*, que a su vez podría ser reenviado al usuario dentro de una página web dinámica generada por el servidor como respuesta a una determinada petición, con la intención de que este código *Script* se ejecutase en el navegador del usuario, no afectando por lo tanto al servidor Web, pero sí a algunos de los usuarios que confían en él.

Entre las posibilidades de ataque a través de *Cross-Site Scripting* podríamos destacar las siguientes:

- Obtención de *cookies* e identificadores de usuarios, que permiten capturar sesiones y suplantar la identidad de los afectados.
- Modificación de contenidos para engañar al visitante víctima del ataque *Cross-Site Scripting*, con la posibilidad de construir formularios para robar datos sensibles, como contraseñas, datos bancarios, etcétera.

⁷ Lenguaje de programación que se puede utilizar dentro de las páginas HTML para automatizar una serie de tareas, siendo interpretado por el propio navegador del usuario.

El ataque típico de *Cross-Site Scripting* suele llevarse a cabo a través de un enlace que apunta a un servidor Web vulnerable. La dirección URL se construye de forma especial para que incluya un *Script* del atacante, que será transmitido por el servidor afectado al cliente que utilice el enlace para visitar esa dirección Web. De este modo, el código se “originará” aparentemente desde el servidor Web y se ejecutará en su contexto de seguridad, por lo que dicho código podrá acceder a las *cookies* del usuario (incluyendo las de autenticación), además de tener acceso a datos enviados recientemente vía Web, o bien realizar acciones en el *website* afectado actuando en nombre de la víctima.

Así, por ejemplo, en un *website* que permita realizar búsquedas en Internet mediante consultas HTTP del tipo “*http://www.sitio.com/busqueda.asp?busca=texto*”, el atacante podría construir una dirección URL maliciosa que fuera del tipo “*http://www.sitio.com/busqueda.asp?busca=<script_del_atacante>*”. La víctima, al hacer clic en el enlace anterior, ejecutaría el código *Script* en su navegador en el contexto de seguridad del servidor Web de búsquedas. Este enlace malicioso podría estar presente en otra página web, en un mensaje de correo electrónico, en un grupo de noticias, etcétera.

También es posible conseguir una activación automática de los ataques de *Cross-Site Scripting*, aprovechando vulnerabilidades conocidas relacionadas con la forma en que ciertos navegadores Web y lectores de correo electrónico interpretan los tipos MIME de los documentos compuestos.

Por ejemplo, un atacante podría convertir un enlace a una imagen incluido en un documento (mediante la etiqueta HTML , con un enlace aparentemente inofensivo a un fichero gráfico) en una forma de activar un ataque *Cross-Site Scripting*, que pase totalmente inadvertida al usuario víctima, ya que éste ni siquiera tendría que hacer clic en el enlace en cuestión: el navegador, al recibir el documento, se encargaría de realizar la petición para mostrar la imagen correspondiente al enlace incluido. Por otra parte, los mensajes de correo en formato HTML también podrían ser utilizados para desencadenar este tipo de ataques.

Debido a que este tipo de ataques no producen daños en el servidor sino en el usuario, en muchos casos no se les ha prestado toda la atención que requerirían, siendo fáciles de erradicar si se filtrasen de forma adecuada todas las peticiones que recibe un determinado servidor Web.

1.4.10.3 ATAQUES DE INYECCIÓN DE CÓDIGO SQL

SQL, *Structured Query Language* (Lenguaje de Consulta Estructurado), es un lenguaje textual utilizado para interactuar con bases de datos relacionales. La unidad típica de ejecución de SQL es la consulta (*query*), conjunto de instrucciones que permiten modificar la estructura de la base de datos (mediante instrucciones del tipo *Data Definition Language*, DDL) o manipular el contenido de la base de datos (mediante instrucciones del tipo *Data Manipulation Language*, MDL). En los servidores Web se utiliza este lenguaje para acceder a bases de datos y ofrecer páginas dinámicas o nuevas funcionalidades a sus usuarios.

El ataque por inyección de código SQL se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Un usuario malicioso podría incluir y ejecutar textos que representen nuevas sentencias SQL que el servidor no debería aceptar. Este tipo de ataque es independiente del sistema de bases de datos subyacente, ya que depende únicamente de una inadecuada validación de los datos de entrada.

Como consecuencia de estos ataques y, dependiendo de los privilegios del usuario de base de datos bajo el cual se ejecutan las consultas, se podría acceder no solo a las tablas relacionadas con la operación de la aplicación del servidor Web, sino también a las tablas de otras bases de datos alojadas en el mismo servidor Web. También pueden propiciar la ejecución de comandos arbitrarios del sistema operativo del equipo del servidor Web.

Así, como ejemplos de ataques de inyección de código SQL podríamos considerar los siguientes:

Si en el servidor se va a ejecutar una sentencia SQL del tipo: *"UPDATE tabla SET password='\$INPUT[password]' WHERE user= '\$INPUT[user_id]';"*, pensada en principio para actualizar (UPDATE) la contraseña de un determinado usuario registrado en el sistema, se podría llevar a cabo un ataque por inyección de código SQL con una dirección URL preparada de forma malicioso a tal y como sigue: *"http://www.servidor.com/script?pwd=clave&uid=1'+or+uid+like'%25admin%25';"*, la cual tendría como consecuencia que el atacante conseguiría acceder a la base de datos con el perfil de administrador (usuario *admin*).

Si en el servidor se va a ejecutar una sentencia SQL del tipo: *"SELECT nombre FROM productos WHERE id LIKE '%\$INPUT[cod_prod]%'";"*, pensada para devolver el nombre de un producto a partir de su código identificador, se podría producir un ataque por inyección de código SQL con una dirección URL como sigue: *"http://www.servidor.com/script?0';EXEC+master..xp_cmdshell(cmd.exe+/c)"*, la cual tendría como consecuencia que el atacante podría ejecutar una aplicación del sistema operativo del equipo, en este caso el propio intérprete de comandos (*cmd.exe*).

Si en el servidor se va a ejecutar una sentencia SQL del tipo: *"SELECT * FROM usuarios WHERE username = " + username + " AND password = " + password + ";"*, se podría producir un ataque si el usuario especifica lo siguiente:

- Username: ; drop table users;
- Password:

ya que entonces la tabla "usuarios" sería borrada de la base de datos, denegando el acceso a todos los demás usuarios (ataque de Denegación de Servicio).

Este tipo de ataques se podrían evitar filtrando los datos enviados por el usuario antes de que estos sean procesados por el servidor, para evitar que se puedan incluir y ejecutar textos que representen nuevas sentencias SQL.

Así mismo, es conveniente no utilizar las consultas SQL basadas directamente en cadenas de texto enviadas desde el navegador del usuario, sino que se deberían construir todas las consultas en el servidor con sentencias preparadas y/o procedimientos almacenados parametrizados, que encapsulen los parámetros y que deberían evitar los caracteres especiales que hubieran podido ser introducidos dentro de ellos por un usuario malicioso.

1.4.11 Ataques contra los sistemas criptográficos

Los ataques contra la seguridad de los sistemas criptográficos persiguen descubrir las claves utilizadas para cifrar unos determinados mensajes o documentos almacenados en un sistema, o bien obtener determinada información sobre el algoritmo criptográfico utilizado. Podemos distinguir varios tipos de ataques contra los sistemas criptográficos:

- Los “ataques de fuerza bruta”, que tratan de explorar todo el espacio posible de claves para romper un sistema criptográfico.
- Los “ataques de diccionario”, que trabajan con una lista de posibles contraseñas: palabras de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas del calendario, etcétera.
- Los ataques contra el diseño del algoritmo.
- Los ataques contra los dispositivos hardware o las aplicaciones software que lo implementan.
- Las distintas técnicas de criptoanálisis: criptoanálisis lineal, diferencial, técnicas de análisis estadístico de frecuencias, etcétera.

1.4.12 Fraudes, engaños y extorsiones

Los fraudes y estafas financieros a través de Internet se han hecho muy frecuentes en estos últimos años. Se utiliza el término de *phishing* para referirse al tipo de ataques que tratan de obtener los números de cuenta y las claves de acceso a servicios bancarios, para realizar con ellos operaciones fraudulentas que perjudiquen a los legítimos propietarios. Generalmente, se utilizan páginas web falsas que imitan a las originales de los servicios bancarios que pretenden suplantar.

El *pharming* es una variante del *phishing* en la que los atacantes utilizan un virus que conecta a las víctimas desde su ordenador a páginas falsas en lugar de a las legítimas correspondientes a sus propias entidades financieras, para sustraer sus datos (números de cuenta y claves de acceso). El *pharming* y el *phishing* también pueden ser empleados para robar y utilizar de forma fraudulenta números de tarjetas de crédito.

Estos datos podrían ser utilizados para realizar ataques del tipo "salami", consistentes en la repetición de gran cantidad de pequeñas operaciones, como transferencias bancarias de importe reducido, que podrían pasar inadvertidas a nivel individual, pero que en conjunto ocasionan un importante daño económico.

El *clickjacking* es una estratagema que pretende engañar al usuario para que éste haga clic en un enlace o botón que en apariencia es inofensivo, cuando en realidad lo hace sobre otro enlace controlado por terceros. Se trata de una amenaza para la seguridad informática que explota una vulnerabilidad del sistema operativo o el navegador del usuario, presentando una página falsa e invitándole a realizar una acción para tomar el control del sistema.

Por otra parte, se han desarrollado virus y otros programas dañinos para facilitar las extorsiones y estafas a usuarios de Internet. Es lo que se conoce como *ransom-ware*, software malicioso cuyo fin es el lucro de su creador por medio de rescates.

También podemos considerar dentro de este tipo de ataques la difusión de correos electrónicos con ofertas falsas o engañosas, así como la publicación de falsas noticias en foros y grupos de noticias, con distintas intenciones, como podría ser el caso de intentar alterar el valor de las acciones de una empresa (de hecho, ya se han producido varias de estas actuaciones en Estados Unidos y en Europa).

Así mismo, debemos tener en cuenta la proliferación de las extorsiones a los usuarios de Internet. Así, por ejemplo, en febrero de 2003 la revista de seguridad informática *CSO Magazine* informaba de varios casos de extorsión contra profesionales, que eran engañados por otros usuarios que conseguían insertar contenidos pornográficos en sus ordenadores personales. El ataque comenzaba cuando la víctima recibía un correo electrónico aparentemente inofensivo, con una invitación para visitar una determinada página web. Si la víctima activaba el enlace en cuestión, se producía una descarga de ficheros de pornografía infantil desde un *website* de Bulgaria hacia su ordenador personal. Desde ese momento, comenzaba la campaña de extorsión propiamente dicha, mediante el envío de un mensaje amenazante que solicitaba la transferencia de una determinada cantidad de dinero para no revelar el incidente a la empresa para la cual trabajaba la víctima.

En mayo de 2005 se informaba de varios casos de *crackers* que habían conseguido "secuestrar" archivos o páginas web de otros usuarios, solicitando un rescate para proceder a su "liberación". Para ello, los atacantes codificaban los documentos afectados para impedir que su propietario los pudiera abrir, solicitando a continuación un importe de 200 dólares en concepto de "rescate" para devolver al usuario el acceso a sus archivos.

De hecho, los casos de chantaje y extorsión *online* se están extendiendo en países como Estados Unidos, a tenor de los últimos estudios publicados. Así, un 17% de las Pymes norteamericanas había sufrido algún tipo de extorsión por la red, según un estudio de la Universidad Carnegie Mellon dado a conocer en septiembre de 2005. En muchos de estos casos, los chantajistas aseguran tener información confidencial sobre la empresa y amenazan con difundirla si no reciben una determinada cantidad de dinero. Se ha podido comprobar que un porcentaje elevado de estas amenazas eran realizadas por un antiguo empleado de la

propia empresa con acceso a datos internos o, incluso, alguien de la competencia. Además, muchas de las empresas amenazadas terminan pagando para evitar mayores problemas.

También han aumentado los casos de extorsión a particulares a través de Internet, consistentes en la publicación o amenaza de publicación de alguna información difamatoria sobre la víctima, utilizando algún medio de la Red (páginas web, foros, grupos de noticias...). En marzo de 2006 se anunciaba la propagación de un nuevo tipo de virus a través de Internet, capaz de bloquear el equipo informático de sus víctimas, solicitando un "rescate" de 300 dólares para revelar la clave para liberar el equipo en cuestión.

1.4.13 Denegación del Servicio (Ataques DoS – *Denial of Service*)

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Para ello, existen varias posibilidades de conseguirlo:

- Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las máquinas afectadas: procesador, memoria y/o disco duro, provocando una caída en su rendimiento. Entre ellas podríamos citar el establecimiento de múltiples conexiones simultáneas, el envío masivo de ficheros de gran tamaño o los ataques lanzados contra los puertos de configuración de los *routers*.
- Provocar el colapso de redes de ordenadores mediante la generación de grandes cantidades de tráfico, generalmente desde múltiples equipos.
- Transmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.
- Sabotajes mediante *routers* "maliciosos", que se encarguen de proporcionar información falsa sobre tablas de enrutamiento que impidan el acceso a ciertas máquinas de la red.
- Activación de programas "bacteria", cuyo objetivo es replicarse dentro de un sistema informático, consumiendo la memoria y la capacidad del procesador hasta detener por completo al equipo infectado.
- Envío masivo de miles mensajes de correo electrónico (*mail bombing*), provocando la sobrecarga del servidor de correo y/o de las redes afectadas.
- "Ataque reflector" (*reflector attack*), que persigue generar un intercambio ininterrumpido de tráfico entre dos o más equipos para disminuir su rendimiento o incluso conseguir su completo bloqueo dentro de una red informática.

- Incumplimiento de las reglas de un protocolo. Para ello, se suelen utilizar protocolos no orientados a conexión, como UDP o ICMP, o bien el protocolo TCP sin llegar a establecer una conexión completa con el equipo atacado.

En relación con esta última posibilidad, el incumplimiento de las reglas de un protocolo, podemos enumerar varios tipos de ataques que han ocasionado numerosos problemas a distintos tipos de sistemas informáticos en los últimos años:

- “El ping de la muerte”: mediante el comando “*ping -l 65510 direccion_equipo_victima*”, que envía un paquete IP de un tamaño superior a los 65.536 bytes, provocando el reinicio o “cuelgue” del equipo víctima que lo recibe (si no ha sido protegido frente a esta eventualidad).
- *Land Attack*: debido a un error en la implementación del protocolo TCP/IP en algunos sistemas Windows, se consigue “colgar” un equipo vulnerable mediante el envío de una serie de paquetes maliciosamente contruidos, en los que la dirección y el puerto de origen son idénticos a la dirección y el puerto de destino.
- *Supernuke* o *Winnuke*: ataque contra algunos sistemas Windows, que se quedan “colgados” o disminuyen drásticamente su rendimiento al recibir paquetes UDP manipulados (fragmentos de paquetes *Out-Of-Band*) dirigidos contra el puerto 137.
- *Teardrop*: tipo de ataque consistente en el envío de paquetes TCP/IP fragmentados de forma incorrecta. Los equipos vulnerables que no hayan sido convenientemente parcheados se “cuelgan” al recibir este tipo de paquetes maliciosos.
- *SYN Flood*: este ataque se basa en un incumplimiento de las reglas básicas del protocolo TCP por parte del cliente. Al establecer la conexión mediante el procedimiento *three-way handshake*, se envía una petición de conexión al equipo víctima, pero no se responde a la aceptación de la conexión por parte de este equipo (generalmente se facilita una dirección IP falsa). El equipo víctima deja la conexión en estado de “semiabierta”, consumiendo de este modo recursos de la máquina. Las conexiones “semiabiertas” caducan al cabo de un cierto tiempo, liberando sus recursos. No obstante, si se envían muchas peticiones de conexión siguiendo el ataque de *SYN Flood*, se colapsarán los recursos del equipo víctima, que no podrá atender nuevas conexiones legítimas.

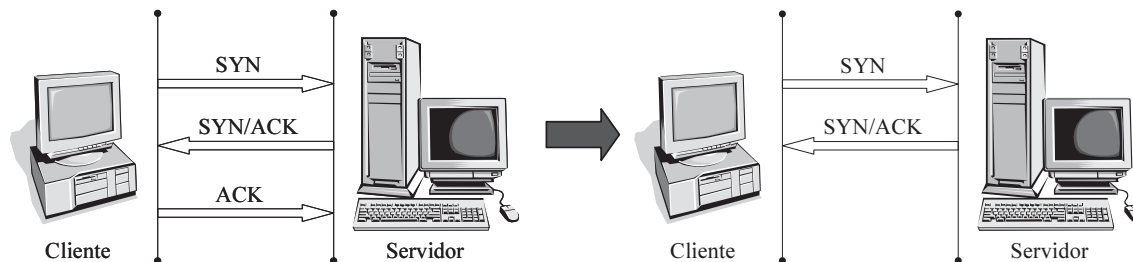


Figura 1.15. Ataque del tipo "SYN Flood"

Así mismo, podemos señalar otros tipos de ataques de Denegación de Servicio (DoS) que se han hecho famosos en los últimos años:

- *Connection Flood*: tipo de ataque que consiste en intentar establecer cientos o miles de conexiones simultáneas contra un determinado servidor víctima del ataque, con lo que se consumen sus recursos y se degrada de forma notable su respuesta ante usuarios legítimos. Este tipo de ataques se han lanzado con éxito contra los *websites* de algunas empresas, como en el caso de la tienda de juguetes *online* eToys, cuyo Website llegó a estar colapsado durante varios días por un ataque coordinado llevado a cabo desde cientos de equipos.
- *Net Flood*: ataque similar al que se ha expuesto anteriormente, consiste en el envío de tráfico masivo contra una determinada red conectada a Internet, para tratar de degradar su funcionamiento.
- *Smurf* ("pitufo"): ataque DoS que se lleva a cabo mediante el envío de una gran cantidad de mensajes de control ICMP (*Internet Control Message Protocol*) de solicitud de eco dirigidos a direcciones de difusión (direcciones *broadcast*), empleando para ello la dirección del equipo víctima del incidente, que se verá desbordado por la cantidad de mensajes de respuesta generados en la red de equipos sondeados, que actúa como una red amplificadora del ataque.
- Bomba UDP: se considera un ataque del tipo *reflector attack* ("ataque reflector"), en el que se emplea el protocolo UDP (*User Datagram Protocol*) y uno de los muchos servicios que responden a los paquetes que reciben para crear una congestión en la red que provoque el DoS, generando un flujo de paquetes UDP continuo entre dos sistemas seleccionados. Así, por ejemplo, se podría elegir en el primer equipo el servicio "chargen" (es una herramienta de pruebas disponible en el puerto 9, que genera una serie de caracteres), mientras que en el segundo equipo se podría hacer uso del servicio "echo" (servicio disponible en el puerto 7, que responde a cada uno de los paquetes que recibe), para de este modo conseguir un intercambio interminable de paquetes UDP entre los dos equipos, generando una especie de "tormenta de paquetes UDP". Para evitar este tipo de ataques conviene desactivar estos servicios en los equipos de la red, así como filtrar este tráfico a través de un cortafuegos.

- *Snork UDP*: ataque similar al anteriormente descrito ("bomba UDP"), dirigido contra sistemas Windows. En este caso se emplea un paquete de datos UDP con origen en el puerto 7 (servicio "echo") o el puerto 19 (servicio "chargen"), utilizando como puerto de destino el 135, en el que se ubica el servicio de localización de Microsoft a través del protocolo NetBIOS. De este modo, se consigue un intercambio de paquetes UDP innecesario que reduce el rendimiento de los equipos y de la red afectada. Se trata, por tanto, de otro ataque del tipo *reflector attack*.

También se han llevado a cabo ataques DoS contra sesiones TCP previamente establecidas, aprovechando una vulnerabilidad en el diseño del protocolo TCP dada a conocer por el CERT/CC a finales de abril de 2004, que afecta a aquellos servicios que se basan en la utilización de sesiones TCP permanentes, sin ningún tipo de autenticación entre los dos extremos de la comunicación. Así, teniendo en cuenta esta vulnerabilidad, un atacante remoto podría forzar el cierre de las sesiones TCP establecidas, mediante un paquete TCP manipulado que sea aceptado por el ordenador destinatario, originando de este modo el ataque DoS.

Uno de los protocolos que podría verse más afectado por esta vulnerabilidad en TCP es BGP (*Border Gateway Protocol*), utilizado para el intercambio de información de enrutamiento entre las redes de los proveedores de acceso a Internet, provocando la desconexión de todas las redes que dependan de un *router* vulnerable al ataque.

Para evitar muchos de los problemas de los ataques de Denegación de Servicio, se puede utilizar algún sistema que permita autenticar los dos extremos de la comunicación, como podría ser el protocolo IPSec con el servicio AH (*Authentication Header*), que permite autenticar todos los paquetes TCP enviados.

Así mismo, es conveniente escanear las redes conectadas a Internet para determinar si son vulnerables al ataque *Smurf*. Un recurso de gran ayuda sobre esta cuestión podría ser el *website* de Powertech, que mantiene en la dirección <http://www.powertech.no/smurf/> una información actualizada de rangos de direcciones IP con debilidades ante el ataque "*Smurf*".

Hay que tener en cuenta que en los ataques de Denegación del Servicio (DoS) el atacante suele ocultar su verdadera dirección mediante técnicas de *IP Spoofing*. Además, en numerosas ocasiones se han empleado este tipo de ataques para encubrir otros ataques simultáneos que pretendían comprometer un sistema o red informático.

1.4.14 Ataques de Denegación de Servicio Distribuidos (DDoS)

Los Ataques de Denegación de Servicio Distribuidos (DDoS) se llevan a cabo mediante equipos zombi. Los equipos zombi son equipos infectados por virus o troyanos, sin que sus propietarios lo hayan advertido, que abren puertas traseras y facilitan su control remoto por parte de usuarios remotos. Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y usuarios legítimos lleguen a ser conscientes del problema, para tratar de

colapsar las redes y los servidores objeto del ataque. Generalmente los equipos zombi cuentan con una conexión ADSL u otro tipo de conexión de banda ancha, de tal modo que suelen estar disponibles las 24 horas.

Para luchar de forma eficaz contra este tipo de ataques es necesario contar con la colaboración de los proveedores de acceso a Internet, para filtrar o limitar el tráfico procedente de los equipos que participan en el ataque. En este sentido, cabría destacar una iniciativa pionera llevada a cabo a finales de mayo de 2005 por la FTC (Comisión Federal de Comercio estadounidense) para tratar de identificar y poner en cuarentena a los clientes de los proveedores de acceso a Internet cuyos ordenadores se hayan convertido (seguramente sin su conocimiento) en una máquina zombi.

Los equipos zombi también están siendo utilizados por los *spammers* para la difusión masiva de sus mensajes de correo no solicitados.

Incluso en algunos países ya se han dado casos de alquiler de redes zombi (conocidas como *botnets*) para poder llevar a cabo ataques de Denegación de Servicio Distribuidos (DDoS). Así, por ejemplo, en el Reino Unido varios jóvenes *crackers* alquilaban redes con 30.000 ordenadores zombi por un precio de 100 dólares la hora para realizar ataques masivos de denegación de servicio. Y en el verano de 2004 un empresario de Massachussets pagó a tres *crackers* menores de edad para realizar ataques con una red zombi de 10.000 equipos contra los servidores de las empresas de la competencia.

Así mismo, la disponibilidad de herramientas como TFN (*Tribe Flood Net*) y TFN2K facilita el desarrollo de este tipo de ataques. En concreto, esta herramienta mejora la comunicación y control de los equipos zombi utilizando paquetes TCP, UDP o ICMP, así como técnicas criptográficas (como el algoritmo CAST-256) para dificultar la detección del atacante. TFN2K permite programar distintos tipos de ataques (*flooding*, *smurf*...) y cambia de forma frecuente las cabeceras de los paquetes que envía a los equipos zombi para dificultar su detección por los Sistemas de Detección de Intrusiones (IDS).

Un informe de Microsoft hecho público en 2010 situaba a España como el país europeo donde se estaban produciendo un mayor número de infecciones relacionadas con equipos zombi, hasta el punto de que solo en el período comprendido entre abril y julio de 2010 unos 382.000 ordenadores españoles se convirtieron en zombis.

1.4.15 Marcadores telefónicos (*dialers*)

Los *dialers* o marcadores telefónicos son pequeños programas que se encargan de marcar números telefónicos que dan acceso a algún tipo de servicio, con una tarifa telefónica muy superior a la normal.

En un principio, este tipo de aplicaciones eran distribuidas por proveedores de acceso a Internet para facilitar a sus clientes el proceso de conexión con el servidor. También se han

desarrollado otro tipo de servicios de pago a través de *dialers*, relacionados en su gran mayoría con la descarga de contenidos pornográficos.

Sin embargo, el problema surgió con la proliferación en Internet de páginas web preparadas para descargar, instalar y ejecutar *dialers* de conexión a números de tarifas especiales de forma automática y sin informar al usuario afectado. Así mismo, posteriormente hicieron su aparición nuevos tipos de virus informáticos capaces de instalar los *dialers* y propagarse rápidamente a través de Internet.

Estos virus son capaces de crear un nuevo acceso telefónico a redes en el ordenador infectado que se configura como el predeterminado para la conexión a Internet, o bien pueden modificar el acceso telefónico a redes que el usuario utiliza habitualmente para sus conexiones a Internet de tal manera que, cada vez que sea ejecutado, el número marcado no sea el correspondiente al proveedor de servicios de Internet del usuario, sino un número de tarifa especial, ocasionando un grave problema económico a la víctima, quien detectará la situación anormal al recibir sus próximas facturas del servicio telefónico.

1.5 DIRECCIONES DE INTERÉS

Información sobre nombres de dominio, páginas web y direcciones IP:



- Base de datos Whois de InterNIC (Internet Network Information Center): <http://www.internic.net/whois.html>.
- Servicio de Información de RIPE-NCC (Réseaux IP Européens Network Coordination Center) para Europa: <http://www.ripe.net/>.
- Servicio de Información de ARIN (American Registry for Internet Numbers): <http://www.arin.net/>.
- Servicio de Información de APNIC (Asian Pacific Network Information Center), para la región de Asia-Pacífico: <http://www.apnic.net/>.
- Servicio de Información de LACNIC (Latin America and Caribbean Internet Addresses Registry): <http://lacnic.net/>.
- DNS Stuff: <http://www.dnsstuff.com/>.

Herramientas para el reconocimiento de sistemas y escaneo de puertos:

- NMAP (para UNIX): <http://www.insecure.org/nmap/>.
- NetScan Tools (para Windows): <http://www.nwpsw.com/>.

Ataques informáticos:

- IP Spoofing: <ftp://ftp.rfc-editor.org/in-notes/rfc2267.txt>, <ftp://ftp.rfc-editor.org/in-notes/rfc2827.txt>.
- DNS Seguro: <http://www.dnssec.net/>.
- KeyGhost: <http://www.keyghost.com/>.
- KeyLogger: <http://www.keylogger.com/>.
- Ataque de Denegación de Servicio Smurf: <http://www.powertech.no/smurf/>.

Otras direcciones de interés:

- Dshield: <http://www.dshield.org/>.
- Security Focus: <http://www.securityfocus.com/>.
- Internet Storm Center: <http://isc.sans.org/>.
- Internet Health Monitoring: <http://www.internetpulse.net/>.

Páginas especializadas en los hackers:

- Hacker Watch: <http://hackerwatch.org/>.
- Revista 2600 de la comunidad hacker: <http://www.2600.com/>.
- Astalavista – The Underground: <http://www.astalavista.com/>.
- Chaos Computer Club, mayor comunidad de hackers de europa: <http://www.ccc.de/>.
- HACKHiSPANO: <http://www.hackhispano.com/>.
- Revista Phrack: <http://www.phrack.org/>.
- The Hacker's Defense Foundation: <http://www.hackerz.org/>.
- AntiOnline: <http://www.antionline.com/>.

GESTIÓN DE INCIDENTES DE SEGURIDAD

2.1 INCIDENTES DE SEGURIDAD

Por **Incidente de Seguridad** entendemos cualquier evento que pueda provocar una interrupción o degradación de los servicios ofrecidos por el sistema, o bien afectar a la confidencialidad o integridad de la información.

Un incidente de seguridad puede ser causado por un acto intencionado realizado por un usuario interno o un atacante externo para utilizar, manipular, destruir o tener acceso a información y/o recursos de forma no autorizada. Aunque un incidente también podría ser la consecuencia de un error o trasgresión (accidental o deliberada) de las políticas y procedimientos de seguridad, o de un desastre natural o del entorno (inundación, incendio, tormenta, fallo eléctrico...).

En España, la Ley Orgánica de Protección de Datos define una incidencia como "cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos", en el contexto de los ficheros con datos de carácter personal.

2.2 IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA

Los *logs* de los equipos informáticos (en especial, de los servidores) y de los dispositivos de red facilitan el registro de posibles incidentes y funcionamientos anómalos, la existencia de fallos en la configuración de una aplicación, la posible desconexión de algún dispositivo del sistema, los cambios realizados en la configuración de los equipos, la utilización de recursos sensibles por parte de los usuarios del sistema, etcétera. Además, proporcionan estadísticas que permiten evaluar el rendimiento del sistema informático.

No obstante, en algunos casos se podría estar registrando información que podría afectar a la privacidad de los usuarios, por lo que será necesario tener en cuenta las posibles consideraciones desde el punto de vista legal (obligación de informar a los usuarios que se está registrando su actividad en el sistema).

En lo que se refiere a los *logs* del sistema operativo, se podrían configurar para registrar los procesos en ejecución dentro del sistema, los inicios y cierres de sesión por parte de los usuarios, las llamadas al sistema, las aplicaciones ejecutadas por los usuarios, los accesos a ficheros y a otros recursos (impresoras...), los posibles problemas de seguridad (intentos de acceso no autorizado a los recursos o fallos de las aplicaciones), etcétera.

Así, por ejemplo, en los sistemas UNIX se podría utilizar la herramienta "System log", mientras que en los sistemas Windows se puede recurrir al registro de eventos (*event log*). También será necesario configurar los *logs* de los dispositivos de red (*routers*, cortafuegos...), de los servidores y de las aplicaciones instaladas en algunos equipos.

Para garantizar la adecuada protección de los *logs*, será necesario almacenarlos de forma segura en un entorno distinto al del sistema protegido, para evitar que los intrusos los puedan modificar o eliminar: grabación de los registros en discos WORM (*Write Once Read More*), generación de una copia en papel, etcétera.

En algunos casos se puede recurrir a una gestión centralizada de los *logs*, mediante un servidor de *logs* que se encargue de guardar copias de todos los registros enviados por los dispositivos de red y los servidores. Para ello, se podrían utilizar aplicaciones como *Syslog* para centralizar los registros. De este modo, se refuerza la seguridad frente a intrusos que pretendan eliminar su rastro manipulando los *logs* de los equipos.

Además, un servidor centralizado de *logs* permite conservar los registros durante un mayor período de tiempo, lo que puede facilitar el análisis detallado de estos registros, incluyendo el estudio de la relación entre eventos incluidos en los *logs* de distintos equipos y dispositivos (elementos de red, herramientas de seguridad...).

Para poder comparar los distintos *logs* conviene mantener todos los relojes de los equipos y dispositivos perfectamente sincronizados. Para ello, se podría utilizar el protocolo NTP (*Network Time Protocol*, www.ntp.org).

En los servidores Web se emplea el formato CLF (*Common Log Format*) o el ELF (*Extended Log Format*), registrando los siguientes datos de cada petición realizada por un cliente remoto:

Tabla 2.1. Registro de las conexiones a un servidor Web

-
- Dirección IP o nombre de dominio de la máquina remota (cliente) que se conecta al servidor Web.
 - Identificación remota del cliente.
 - Nombre de autenticación del usuario.
 - Fecha y hora de la conexión.
 - Petición formulada por el cliente (por ejemplo: "GET/index.html HTTP/1.0").
 - Estado HTTP devuelto por el servidor al cliente.
 - Número de bytes enviados al cliente.
 - Agente de usuario (tipo de navegador utilizado): campo ELF.
 - URL de procedencia (referrer log): campo ELF.
-

Los administradores de la red tienen a su disposición una serie de herramientas para analizar toda la información registrada en los *logs*, entre las que se encuentran distintos tipos de filtros y aplicaciones que permiten detectar de forma automática patrones de ataques o situaciones de potencial peligro.

En este sentido, se debería considerar el problema de que el exceso de información registrada en el sistema pueda llegar a desbordar a sus administradores, provocando una situación bastante habitual en muchas organizaciones: que los datos de los registros de actividad no sean analizados de forma adecuada.

Por otra parte, suele ser muy recomendable realizar un estudio previo del tráfico en la red para facilitar la posterior detección de situaciones anómalas: consumo de ancho de banda por usuarios y departamentos, patrones horarios del tráfico, servicios y protocolos utilizados... El protocolo de gestión de red SNMP se podría utilizar para recabar parte de esta información de los dispositivos de red.

En los servidores Windows se pueden utilizar tres tipos de registros:

- **Registro de Aplicación:** muestra los mensajes, la información del estado y los sucesos generados desde las aplicaciones y servicios instalados en el sistema.
- **Registro del Sistema:** incluye los errores, advertencias y sucesos generados por el propio sistema operativo y sus servicios esenciales.
- **Registro de Seguridad:** muestra los registros de éxito y de fracaso de los servicios auditados, es decir, cuando un usuario intenta acceder a un recurso auditado y se le concede (éxito) o se le deniega (fracaso) el acceso.

Mediante el Visor de Sucesos es posible acceder a la información de estos tres registros.

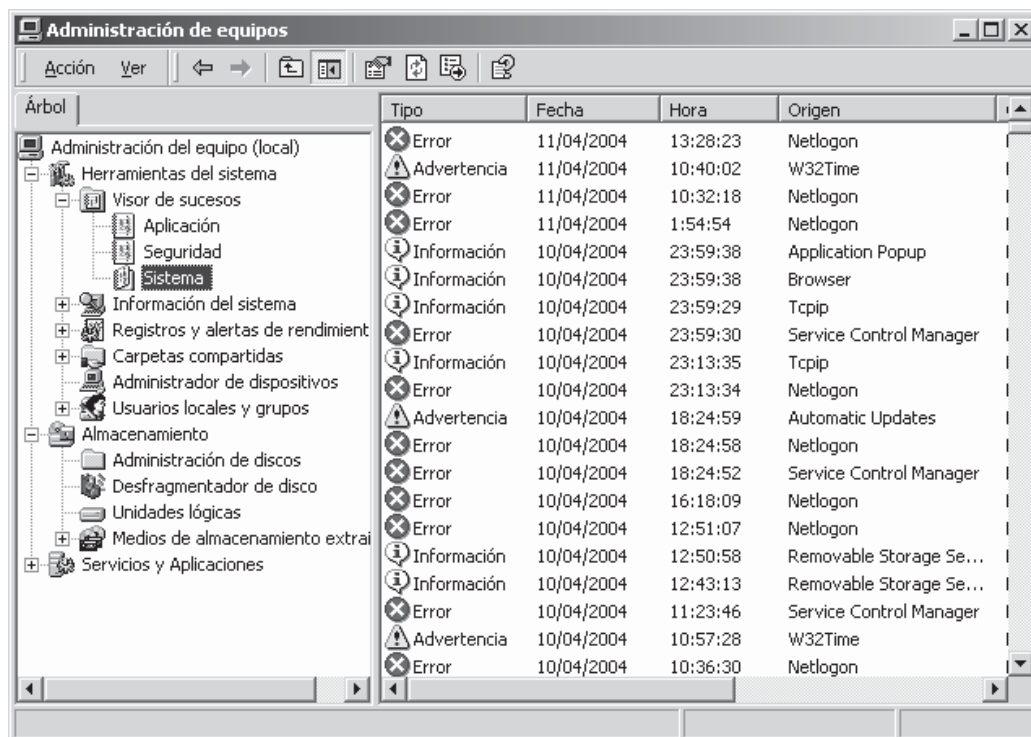


Figura 2.1. Visor de Sucesos en un equipo Windows

El Registro de Seguridad en Windows permite auditar varias clases de actividades o sucesos:

Tabla 2.2. Sucesos que se pueden registrar en un equipo Windows

- Eventos de inicio de sesión interactivo.
- Eventos de inicio de sesión en el dominio.
- Gestión de cuentas.
- Acceso a objetos.
- Acceso al Directorio Activo.
- Utilización de privilegios.
- Seguimiento de procesos.
- Eventos de sistema.
- Cambios de política de seguridad.

2.3 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

2.3.1 Características básicas de los IDS

Los **Sistemas de Detección de Intrusos** (*Intrusion Detection Systems*, IDS) son los sistemas encargados de detectar y reaccionar de forma automatizada ante los incidentes de seguridad que tienen lugar en las redes y equipos informáticos.

Para ello, estos sistemas se encargan de monitorizar el funcionamiento de los equipos y de las redes en busca de indicios de posibles incidentes o intentos de intrusión, avisando a los administradores del sistema informático ante la detección de cualquier actividad sospechosa mediante una serie de alarmas e informes.

En la arquitectura de un IDS podemos distinguir los siguientes elementos funcionales básicos:

- Una fuente de información que proporciona eventos del sistema o red informática.
- Una base de datos de patrones de comportamiento considerados como normales, así como de los perfiles de distintos tipos de ataque.
- Un motor de análisis encargado de detectar evidencias de intentos de instrucción.
- Un módulo de respuesta capaz de llevar a cabo determinadas actuaciones a partir de las indicaciones del motor de análisis.

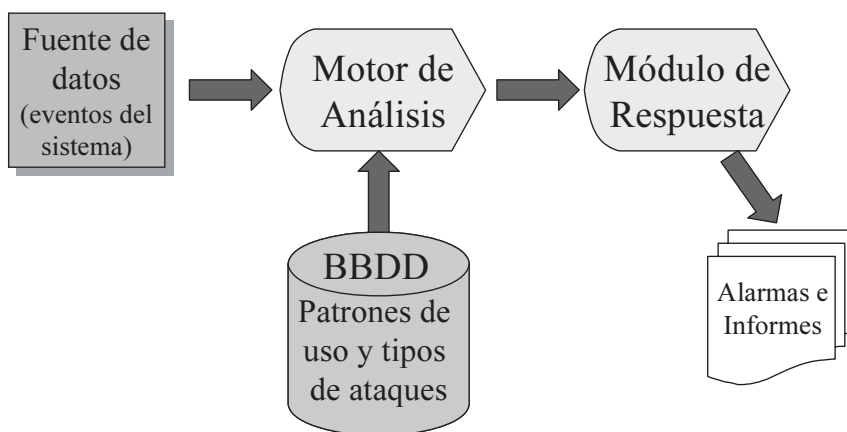


Figura 2.2. Arquitectura de un Sistema de Detección de Intrusiones (IDS)

Por otra parte, un IDS puede utilizar dos modelos de detección:

- **Detección de un mal uso** (*misuse*): tipos ilegales de tráfico, secuencias utilizadas para realizar ataques contra los equipos (*exploits*), escaneo de puertos, etcétera.
- **Detección de un uso anómalo**: análisis estadístico del tráfico en la red, monitorización de procesos y del comportamiento de los usuarios, con el fin de poder detectar aquellos comportamientos que se puedan considerar anómalos según los patrones de uso registrados hasta el momento: franjas horarias, utilización de puertos y servicios...

Se trataría, por lo tanto, de detectar cambios de comportamiento no justificados en lo que se refiere a ficheros accedidos, aplicaciones utilizadas en el trabajo, cantidad de tráfico cursado en la red, conexiones de usuarios en horarios poco habituales, etcétera.

Gracias a su módulo de respuesta, un IDS es capaz de actuar de forma automática a los incidentes detectados. Las **respuestas pasivas** se limitan a registrar las posibles intrusiones o usos anómalos, así como a generar informes y alertas dirigidas a los administradores de la red (correos electrónicos, mensajes SMS...).

Por su parte, mediante las **respuestas activas** el IDS podría responder a la situación anulando conexiones o bloqueando el acceso a determinados equipos o servicios de la red, para tratar de limitar las consecuencias del incidente.

Tabla 2.3. Ejemplos de respuestas activas de un IDS

- Anular las conexiones TCP inyectando paquetes de reinicio en las conexiones del atacante.
 - Reconfiguración de los cortafuegos de la red para filtrar el tráfico que pueden estar causando el incidente.
 - Desconexión automática de servidores y dispositivos de red.
 - Bloqueo de cuentas o prohibición de la ejecución de determinados comandos.
 - Localización del origen del ataque y notificación a los proveedores de acceso a Internet u organizaciones implicadas.
-

No obstante, los sistemas IDS también presentan una serie de problemas y limitaciones, como podrían ser la generación de falsas alarmas, ya sean éstas **falsos negativos**, que se producen cuando el IDS no es capaz de detectar algunas actividades relacionadas con incidentes de seguridad que están teniendo lugar en la red o en los equipos informáticos, o bien **falsos positivos**, que se producen cuando el IDS registra y genera alertas sobre determinadas actividades que no resultan problemáticas, ya que forman parte del funcionamiento normal del sistema o red informático.

Por otra parte, en los entornos conmutados, es decir, en las redes locales que utilizan *switches*, resulta más difícil monitorizar el tráfico de la red. Por este motivo, en estos casos resulta conveniente la instalación en la red de *switches* dotados de puertos especiales, conocidos como *spanning ports* o *mirrored ports*, que faciliten la captura de todo el tráfico cursado por parte de un sistema IDS.

Así mismo, es necesario tener en cuenta la imposibilidad de analizar las comunicaciones cifradas (conexiones que empleen protocolos como SSH, SSL, IPsec...). Por este motivo, resulta conveniente examinar los datos una vez hayan sido descifrados por los equipos destinatarios dentro de la red de la organización.

Los sistemas IDS también pueden tener un cierto impacto en el rendimiento de la red y podrían ocasionar una sobrecarga de tareas administrativas si generasen un elevado número de informes y registros de actividad.

Entre los principales IDS disponibles en el mercado, podríamos citar SNORT, Real Secure de Internet Security Systems, SentiVist de la empresa NFR, NetRanger de Cisco, etcétera.

2.3.2 Tipos de IDS

2.3.2.1 HIDS (*HOST IDS*)

Los *Host IDS* pueden detectar las intrusiones a nivel de *host*, es decir, a nivel de un equipo informático, observando para ello si se han producido alteraciones significativas de los archivos del sistema operativo o analizando los *logs* del equipo en busca de actividades sospechosas.

Un *Host IDS* requiere de la instalación de un dispositivo sensor, conocido como "agente", en el equipo informático objeto de monitorización. Este sensor software trabaja a bajo nivel, interceptando las llamadas a las funciones básicas del sistema operativo. Además, se encarga de analizar cada actividad y proceso en ejecución dentro del equipo, razón por la que también presenta el inconveniente de disminuir el rendimiento del equipo.

Las principales tareas realizadas por un *Host IDS* son las que se presentan a continuación:

- Análisis de los registros de actividad (*logs*) del núcleo (*kernel*) del sistema operativo, para detectar posibles infiltraciones.
- Verificación de la integridad de los ficheros ejecutables. Para ello, es necesario mantener una base de datos con el estado exacto de cada uno de los archivos del sistema y de las aplicaciones instaladas, a fin de detectar posibles modificaciones

de los mismos (*integrity check*). Herramientas como *Tripwire* (www.tripwire.org) facilitan esta función.

- Exploración periódica/planificada de programas privilegiados ("setuid" de sistemas UNIX/LINUX).
- Auditoría periódica de los permisos asignados a los recursos del sistema.
- Búsqueda y evaluación periódica de vulnerabilidades de software conocidas.
- Revisión detallada del proceso de instalación de nuevas aplicaciones en el sistema, a fin de poder detectar caballos de Troya u otros códigos malignos.

2.3.2.2 MHIDS (*MULTIHOST IDS*)

Este tipo de IDS permiten detectar actividades sospechosas en base a los registros de actividad de diferentes equipos informáticos (*hosts*). Por este motivo, también se les conoce como sistemas "IDS Distribuidos" (DIDS, *Distributed IDS*).

2.3.2.3 NIDS (*NETWORK IDS*)

Los *Network IDS* se instalan en una red de ordenadores para monitorizar el tráfico de red en busca de cualquier actividad sospechosa: escaneo de puertos; intentos de explotación de agujeros de seguridad en los servicios instalados en los equipos de la red; ataques conocidos contra determinados protocolos; intentos de ejecución de *scripts* CGI vulnerables en los servidores; etcétera.

Para ello, un *Network IDS* trata de detectar el tráfico anómalo que suele acompañar a los intentos de intrusión, analizando para ello el contenido de los paquetes de datos que se transmiten a través de la red de la organización.

Entre las distintas situaciones de tráfico anómalo, podríamos citar las siguientes:

- Enrutamiento anormal de los paquetes de datos.
- Fragmentación de paquetes deliberada.
- Utilización de una dirección IP no válida o en desuso en uno de los tramos de red internos (*IP Spoofing*).
- Afluencia de paquetes DNS con identificadores consecutivos, que incluyen la supuesta respuesta a una misma encuesta (situación típica de un ataque de *DNS Spoofing*).

- Invasión de paquetes TCP SYN desde una o varias direcciones (situación típica de un ataque de denegación de servicio del tipo de *SYN Flooding*).
- Invasión de paquetes ICMP o UDP de eco (típicos de ataques como *Smurf* y *Fraggle*).
- Falsa correspondencia entre las direcciones MAC conocidas y las direcciones IP de los equipos.
- Tormentas de tráfico ARP, que podrían revelar un intento de “envenenamiento de las tablas ARP” (situación típica de un ataque de *ARP Spoofing*).

Uno de los sistemas NIDS más conocidos es SNORT. Este sistema decide qué paquetes de los que circulan por una red resultan sospechosos, empleando para ello una base de datos de reglas que se aplican teniendo en cuenta el contenido y los formatos de cabecera de los paquetes de datos.

Además, se pueden descargar nuevas reglas directamente desde bases de datos disponibles en Internet, que permiten catalogar nuevos tipos de incidentes, *exploits* y vulnerabilidades de sistemas.

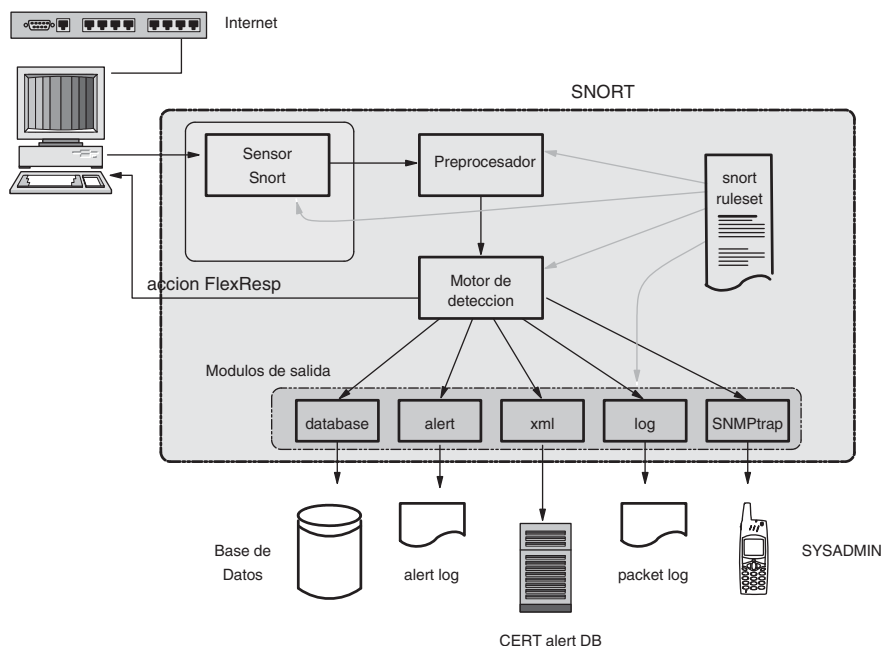


Figura 2.3. Arquitectura del IDS Snort

2.3.3 Arquitecturas de los IDS

Las arquitecturas de los IDS se han propuesto con el objetivo de facilitar la interoperabilidad y reutilización de módulos, así como la reducción de la complejidad en la gestión y configuración de los IDS.

Gracias a la aprobación de protocolos de comunicación específicos, es posible lograr el intercambio de datos entre elementos de distintos fabricantes que pueden formar parte de un IDS. De este modo, se facilita la captura de eventos generados por distintas fuentes, proporcionando una imagen más amplia y detallada de las actividades maliciosas en un determinado entorno.

En una arquitectura de IDS se distinguen los elementos Agentes (que se encargan de monitorizar la actividad en el sistema objeto de estudio), los elementos Transceptores (se encargan de la comunicación), los elementos Maestros (centralizan y analizan los datos) y una Consola de Eventos (módulo de interfaz con los usuarios).

Las arquitecturas de IDS más importantes son CIDF e IDWG.

CIDF (*Common Intrusion Detection Framework*) es una arquitectura promovida por la Agencia Federal de Estados Unidos DARPA (*Defense Advanced Research Projects Agency*) y finalizada en 1999, que ha tenido una escasa aceptación comercial.

Esta arquitectura está constituida por los siguientes elementos:

- **Generador de eventos:** obtención y descripción de eventos mediante objetos denominados GIDO (*Generalized Intrusion Detection Objects*).
- **Analizador de eventos:** incorpora los algoritmos de detección de ataques.
- **Base de datos de eventos:** se utiliza el lenguaje CISL (*Common Intrusion Specification Language*) para expresar los diferentes eventos.
- **Unidades de respuesta:** se encargan de cerrar las conexiones, terminar procesos, bloquear el acceso a los servidores, etcétera.

Por su parte, la arquitectura **IDWG** (*Intrusion Detection Working Group*) propone el formato IDEF (*Intrusion Detection Exchange Format*) para facilitar el intercambio de información sobre los incidentes de seguridad.

En este caso se distinguen los módulos Sensor, Analizador, Fuente de Datos y Manager:

- El **Analizador** es el componente que analiza los datos recolectados por el Sensor, buscando señales de actividad no autorizada o indeseada.

- El **Sensor** recolecta datos de la **Fuente de Datos**: paquetes de red, *logs* de auditoría del sistema operativo, *logs* de aplicaciones... (información que el IDS emplea para detectar cualquier actividad indeseada o no autorizada).
- El **Manager** es el componente desde el cual se administran los restantes elementos del IDS: se encarga de la configuración de los sensores y analizadores, de la consolidación de datos, de la generación de informes, etcétera.

La arquitectura IDWG ha definido un modelo de datos orientado a objetos basado en lenguaje XML para describir los eventos, conocido como IDMEF (*Intrusion Detection Message Exchange Format*). Así mismo, IDWG prevé dos mecanismos de comunicaciones: el protocolo IAP (*Intrusion Alert Protocol*), para intercambiar datos de alertas de intrusiones de forma segura entre las entidades de detección, y el protocolo IDXP (*Intrusion Detection Exchange Protocol*), que permite intercambiar datos en general entre las entidades de detección de intrusiones.

2.4 IPS (*INTRUSION PREVENTION SYSTEMS*)

Un sistema IPS (*Intrusion Prevention System*) es un sistema que permite prevenir las intrusiones. Se trata, por tanto, de un tipo de sistema que pretende ir un paso más allá de los IDS, ya que puede bloquear determinados tipos de ataques antes de que estos tengan éxito.

2.5 LOS *HONEYPOTS* Y LAS *HONEYNETS* (SEÑUELOS)

Un *honeypot* es un servidor configurado y conectado a una red para que pueda ser sondeado, atacado e incluso comprometido por intrusos. Se trata, por lo tanto, de un equipo o sistema que actúa a modo de señuelo o trampa para los intrusos.

El concepto de sistema trampa ya fue propuesto hace algunos años por Cliff Stoll en su libro *Cuckoo's Egg*.

Por su parte, una *honeynet* (red señuelo) es una red completa que ha sido configurada y conectada a otras redes para que pueda ser sondeada, atacada e incluso comprometida por intrusos.

Los *honeypots* y *honeynets* proporcionan varios mecanismos para la monitorización, registro y control de las acciones de los intrusos. De este modo, permiten analizar cómo los intrusos emplean sus técnicas y herramientas para intentar entrar en un sistema o en una red informática (cómo consiguen analizar y explotar sus vulnerabilidades) y comprometer su

seguridad (cómo pueden alterar o destruir los datos, instalar programas dañinos o controlar de forma remota los equipos afectados). Además, estas actividades de monitorización y registro se realizan tratando de pasar de forma inadvertida para los intrusos.

Tal y como afirmaba el general chino Sun Tzu en su libro *El Arte de la Guerra* (siglo V A.C.), “lo que posibilita a un gobierno inteligente y a un mando militar sensato vencer a los demás y lograr triunfos extraordinarios es la información previa”. Además, también en palabras de este famoso estratega, “la mejor forma de protegerse es saber cómo me van a atacar”.

Por lo tanto, los *honeypots* y las *honeynets* entrarían dentro de las aplicaciones del tipo *know your enemy* (“conoce a tu enemigo”), que permiten aprender de las herramientas y técnicas de los intrusos para proteger mejor a los sistemas reales de producción, construyendo una base de datos de perfiles de atacantes y tipos de ataques. También podrían facilitar la captura de nuevos virus o códigos dañinos para su posterior estudio.

Así mismo, estos sistemas permiten desviar la atención del atacante de los verdaderos recursos valiosos de la red de la organización.

En cuanto al diseño de una *honeynet*, se han propuesto dos arquitecturas conocidas como GenI (año 1999) y GenII (año 2002), siendo la segunda más fácil de implementar y más segura para la organización.

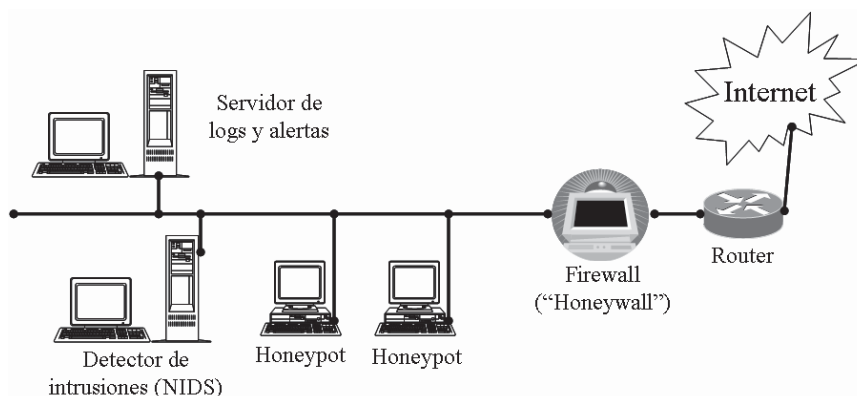


Figura 2.4. Diseño de una honeynet

Los elementos integrantes de una *honeynet*, según el esquema anterior, serían uno o varios *honeypots* (servidores que actuarían de señuelos), un sistema de detección de intrusiones en red (NIDS), un servidor de *logs*, un dispositivo que se haría pasar por un cortafuegos (*honeywall*) y un *router*.

También se podría considerar la posibilidad de incorporar un dispositivo que aplique la técnica de *bait and switch*, según la cual se monitoriza el tráfico procedente de Internet y se desvía aquel que pudiera ser considerado como “hostil” hacia el sistema trampa (*honeynet*), dejando que el resto del tráfico “normal” pueda dirigirse a la red interna de la organización.

En definitiva, podemos considerar que los sistemas basados en señuelos (*honeynets* y *honeypots*) ofrecen los siguientes servicios y funciones:

- Conexión segura de la red corporativa a Internet.
- Captura de datos sobre los intrusos: en el cortafuegos, en el NIDS y en los propios registros (*logs*) de los *honeypots*.
- Centralización de la información capturada en un servidor de *logs*, por motivos de seguridad.
- Control de las acciones del intruso, ya que éste debe quedar confinado dentro de la *honeynet*, sin que pueda atacar a otras redes o equipos.

En los *honeypots* se suelen instalar versiones modificadas del intérprete de comandos (*shell* en un sistema Unix/Linux o "cmd.exe" en un sistema Windows), como "ComLog", un troyano que reemplaza al "cmd.exe" para registrar y reenviar los comandos tecleados por el usuario, así como otras herramientas que permitan registrar las actuaciones de los intrusos (SpyBuddy, KeyLogger, etcétera).

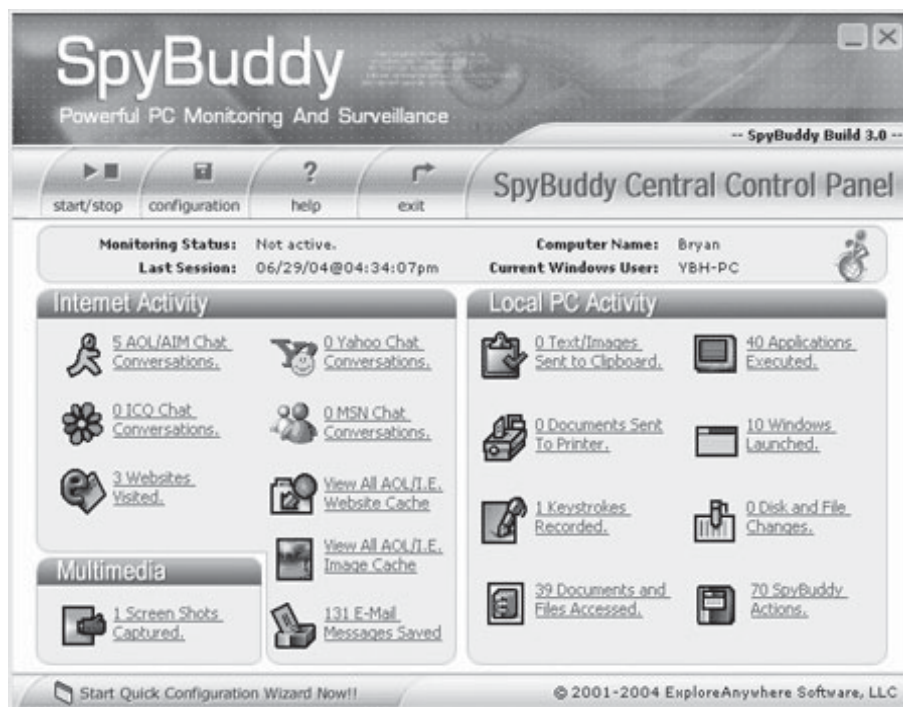


Figura 2.5. SpyBuddy

SpyBuddy es una herramienta comercial que permite registrar las teclas pulsadas por el usuario del equipo; monitorizar la creación, acceso, modificación y eliminación de ficheros y directorios; realizar un seguimiento de los programas que se ejecutan en el equipo; etcétera.

En estos últimos años se ha propuesto el desarrollo de *honeynets* virtuales, en una configuración en la que todos los equipos y servicios se ejecutan en un único ordenador, recurriendo para ello a un software de virtualización, como VMWare (www.vmware.com). Este software de virtualización permite la ejecución simultánea de varios sistemas operativos, con distintos tipos de servicios y aplicaciones, en un mismo equipo físico, de tal modo que, a pesar de compartir los recursos de este ordenador (conocido como *host* anfitrión), aparenten estar ejecutándose en máquinas distintas e independientes.

Una *honeynet* virtual presenta como ventaja unos menores costes y espacio requerido que en una red física, facilitando la gestión centralizada de todos los servicios y aplicaciones incluidos en la *honeynet*.

Por otra parte, debemos tener en cuenta otras consideraciones acerca del uso de estas herramientas, ya que se trata de proyectos de elevado riesgo, debido a las amenazas y tipos de ataques que se van a producir contra los equipos y redes de la organización. Por este motivo, en los equipos y redes señuelo no se deberían incluir datos o información sensible, ni servicios en producción.

Además, los posibles ataques contra estos equipos y redes no deberían comprometer a los usuarios y clientes de la red informática de la organización y, mucho menos, podrían afectar a terceros. Para ello, es necesario establecer las medidas de control y bloqueo de los posibles ataques e intentos de intrusión llevados a cabo contra redes y equipos de terceros desde los equipos que hayan sido comprometidos en la *honeynet*, ya que de lo contrario la organización podría incurrir en responsabilidades legales por los daños ocasionados a terceros desde sus propios equipos y redes informáticas.

Otra cuestión legal que se podría contemplar surge en torno a la discusión de hasta qué punto es lícito emplear estas herramientas para espiar a los intrusos, sin que estos hayan sido advertidos previamente de que sus actividades están siendo registradas por la organización.

Para concluir este apartado, podemos citar algunos ejemplos de herramientas y proyectos de interés relacionados con los *honeypots* y las *honeynets*.

Así, podemos encontrar en Internet aplicaciones que permiten simular determinados servicios para registrar los posibles intentos de ataque e intrusión, como *BackOfficer Friendly*, *Specter*, *Honeyd*, *Decoy Server* de Symantec, *Deception Toolkit*, etcétera.

Por su parte, el proyecto HoneyNet (www.honeynet.org) se remonta a junio del año 2000, con el objetivo de "estudiar las técnicas, tácticas y motivaciones de la comunidad de atacantes y compartir las lecciones aprendidas". En la actualidad este proyecto está integrado por profesionales de distintos perfiles y áreas de conocimiento: informáticos, psicólogos, ingenieros de redes, etcétera.

2.6 OTRAS HERRAMIENTAS Y APLICACIONES DE UTILIDAD

Podemos destacar otras herramientas y aplicaciones que pueden resultar de ayuda para gestionar y supervisar la seguridad en las redes de ordenadores.

Así, por ejemplo, podríamos citar en primer lugar determinadas herramientas y comandos incluidos en el propio sistema operativo de un ordenador, entre las que destacan las siguientes⁸:

- **Netstat**: comando que muestra el estado de las conexiones de red.
- **NBTStat**: muestra el estado de las conexiones actuales que utilizan NetBIOS sobre TCP/IP.
- **IpConfig**: informa sobre la configuración de las tarjetas de red del equipo.
- **Ping**: envía un *ping* al equipo especificado para comprobar si se encuentra activo en la red.
- **Tracert**: informa de la ruta seguida para alcanzar un determinado equipo conectado a la red.
- **Route**: muestra y manipula las tablas de enrutamiento del equipo.
- **ARP**: muestra y modifica las tablas de conversión de direcciones IP a direcciones físicas (direcciones MAC).
- **Nslookup**: inspecciona los contenidos de los archivos de un servidor DNS.
- **Finger**: muestra información sobre un determinado usuario del sistema.
- **Whois**: relaciona nombres de dominio con direcciones IP.
- **Telnet**: permite iniciar una sesión remota en otro servidor, emulando un terminal virtual.
- **FTP**: permite enviar y descargar ficheros de otro servidor, a través del protocolo FTP.

⁸ En Windows se pueden ejecutar desde el intérprete de comandos.

```

C:\ Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Alvaro Gómez Vieites>netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    DELL_ALVARO:epmap     0.0.0.0:0             LISTENING
TCP    DELL_ALVARO:microsoft-ds 0.0.0.0:0             LISTENING
TCP    DELL_ALVARO:1026      0.0.0.0:0             LISTENING
TCP    DELL_ALVARO:31595     0.0.0.0:0             LISTENING
UDP    DELL_ALVARO:microsoft-ds *:*:
UDP    DELL_ALVARO:isakmp    *:*:
UDP    DELL_ALVARO:4500      *:*:
UDP    DELL_ALVARO:ntp       *:*:
UDP    DELL_ALVARO:1900      *:*:
UDP    DELL_ALVARO:18001     *:*:
UDP    DELL_ALVARO:18002     *:*:

C:\Documents and Settings\Alvaro Gómez Vieites>

```

Figura 2.6. Ejecución de la herramienta Netstat en un sistema Windows

Por otra parte, los *wrappers* son programas que permiten controlar el acceso y utilización de otros programas y servicios que se ejecutan en un ordenador.

A su vez, los analizadores de protocolos y *sniffers* son programas “husmeadores”, que interceptan y analizan el tráfico en la red, recurriendo para ello a la utilización de dispositivos de escucha del tráfico en la red (*network taps*), que actúan en modo promiscuo y que son difíciles de detectar ya que no tienen asociada una dirección IP.

Así, por ejemplo, podríamos citar *sniffers* y analizadores de protocolos como Nmap, Ntop, NetScanTools, LANSleuth o Ethereal, que permiten detectar protocolos y servicios no autorizados por la organización, además de llevar a cabo un completo análisis del tráfico habitual en la red de una organización (protocolos y servicios utilizados, cantidad de información transmitida, evolución de la situación por franjas horarias y por días de la semana, comportamiento por segmentos de la red...), ya que de este modo será más fácil la detección de situaciones anómalas a posteriori.

Los sistemas anti-*sniffers* son herramientas capaces de detectar la existencia de tarjetas de red que se encuentren funcionando en modo promiscuo para capturar todo el tráfico de la red.

También pueden resultar de gran ayuda las herramientas para la evaluación de vulnerabilidades. Estas herramientas, entre las que podríamos citar a Nessus o a Internet Security Scanner, se encargan de llevar a cabo un análisis automático de un sistema informático, para tratar de localizar algunas de las vulnerabilidades más conocidas.

Además, el sondeo de seguridad complementa al análisis de vulnerabilidades con tareas como la detección y la revisión de la instalación y configuración de los equipos de seguridad (cortafuegos, antivirus, IDS, etcétera).

En este caso, se podrían realizar pruebas de intrusión (tests de penetración), en las que no solo se detectasen las vulnerabilidades, sino que se tratasen de explotar aquellas que hayan sido identificadas y que pudieran comprometer el sistema, así como otros sistemas accesibles desde el afectado. Esta tarea se puede completar posteriormente con un análisis de riesgos en el sistema informático, en el que se pretende determinar cuál es el nivel de riesgo a partir del análisis de posibles amenazas y vulnerabilidades.

También podemos considerar las herramientas que se encargan de monitorizar de forma permanentemente la actividad en la red de la empresa, para evitar que determinada información o documentos "sensibles" puedan ser enviados al exterior sin la adecuada autorización, debido a distintos factores: virus informáticos, actuaciones de empleados desleales, explotación de algún agujero de seguridad en un equipo informático de la organización, etcétera.

Por último, podemos destacar que en los últimos años se han presentado en el mercado distintas soluciones integradas "todo en uno", constituidas por dispositivos que incorporan varios servicios de seguridad como el programa antivirus, el filtrado de contenidos, el filtrado de correo basura (*spam*), una herramienta para el análisis de vulnerabilidades del sistema, un Sistema de Detección de Intrusos (IDS), un cortafuegos para la seguridad perimetral y/o un servidor VPN para crear túneles seguros y habilitar las conexiones remotas. Además, estos dispositivos, que se instalan en el punto de conexión de la red corporativa de la empresa con el exterior, cuentan con un servicio de actualización y mantenimiento remoto por parte del fabricante.

Como ejemplo destacado de estos dispositivos integrados podríamos citar la gama de productos FortiGate de la empresa Fortinet (www.fortinet.com).

2.7 DIRECCIONES DE INTERÉS



Cortafuegos:

- Firewall-1 de CheckPoint: <http://www.checkpoint.com/>.
- PIX de Cisco: <http://www.cisco.com/>.
- Netscreen Firewall: <http://www.juniper.net/>.
- Watchguard Firebox: <http://www.watchguard.com/>.
- Symantec Raptor: <http://www.symantec.com/>.
- ZoneAlarm: <http://www.zonealarm.com/>.
- Fortigate de la empresa Fortinet: <http://www.fortinet.com/>.

Sistemas IDS:

- Tripwire: <http://www.tripwire.org/>.
- Snort: <http://www.snort.org/>.
- Specter: <http://www.specter.com/>.

Honeypots y honeynets:

- VMWare: <http://www.vmware.com/>.
- Honeyd: <http://www.honeyd.org/>.
- HoneyNet Project: <http://www.honeynet.org/>.

Otras herramientas y aplicaciones de interés:

- Nessus: <http://www.nessus.org/>.

RESPUESTA ANTE INCIDENTES DE SEGURIDAD

3.1 DEFINICIÓN DE UN PLAN DE RESPUESTA A INCIDENTES

La definición e implantación de un Plan de Respuesta a Incidentes debería tener en cuenta una serie de actividades y tareas, entre las cuales podríamos destacar todas las que se presentan en la siguiente relación:

Tabla 3.1. Actividades contempladas en un Plan de Respuesta a Incidentes

- Constitución de un Equipo de Respuesta a Incidentes.
 - Definición de una Guía de Procedimientos.
 - Detección de un incidente de seguridad.
 - Análisis del incidente.
 - Contención, erradicación y recuperación.
 - Identificación del atacante y posibles actuaciones legales.
 - Comunicación con terceros y relaciones públicas.
 - Documentación del incidente de seguridad.
 - Análisis y revisión a posteriori del incidente.
-

3.1.1 Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)

El **Equipo de Respuesta a Incidentes de Seguridad Informática** (CSIRT, *Computer Security Incident Response Team*) está constituido por las personas que cuentan con la experiencia y la formación necesaria para poder actuar ante las incidencias y desastres que pudieran afectar a la seguridad informática de una organización.

Generalmente solo las grandes organizaciones cuentan con un equipo de personas contratadas para cumplir con esta función. En la mayoría de las organizaciones que no cuentan con un Equipo de Respuesta formalmente constituido, será necesario identificar quiénes son las personas responsables de acometer cada una de las tareas que se hayan definido en el Plan de Respuesta a Incidentes, definiendo claramente las responsabilidades, funciones y obligaciones de cada persona implicada en dicho Plan.

La organización deberá mantener actualizada la lista de direcciones y teléfonos de contacto para emergencias, para poder localizar rápidamente a las personas clave.

En algunos casos será necesario contratar a las personas con la necesaria experiencia y cualificación profesional (conocimientos técnicos, habilidades de comunicación...). La experiencia es un factor determinante para poder actuar de forma correcta evitando errores a la hora de responder de forma rápida y eficaz ante los incidentes de seguridad.

Así mismo, conviene prestar especial atención a la formación continua de los miembros del Equipo de Respuesta a Incidentes (o de las personas que deban asumir esta responsabilidad si no existe el equipo como tal), contemplando tanto los aspectos técnicos como los aspectos legales (delitos informáticos).

Estas personas deben contar con la dotación de medios técnicos y materiales necesarios para poder cumplir con eficacia su misión. Para comprobar la idoneidad de los medios disponibles, el entrenamiento de los miembros del equipo y las actividades definidas en el Plan de Respuesta a Incidentes, conviene llevar a cabo simulacros de forma periódica en la organización.

3.1.2 Procedimientos y actividades a realizar

Como parte integrante del Plan de Respuesta a Incidentes, la organización debe definir una guía de actuación clara y detallada con los procedimientos y acciones necesarias para la restauración rápida, eficiente y segura de la capacidad de procesamiento informático y de comunicaciones de la organización, así como para la recuperación de los datos dañados o destruidos.

El objetivo perseguido con la Guía de Procedimientos es conseguir una respuesta sistemática ante los incidentes de seguridad, realizando los pasos necesarios y en el orden adecuado para evitar errores ocasionados por la precipitación o la improvisación.

Una buena Guía de Procedimientos permitirá minimizar los daños ocasionados y facilitar la recuperación del sistema afectado.

Además, esta guía debe completar la adquisición de información detallada sobre cada incidente de seguridad para mejorar los procedimientos de actuación ante futuros incidentes y reforzar la protección actual de los sistemas informáticos de la organización.

Por supuesto, también debe tratar de forma adecuada las cuestiones legales que se pudieran derivar de cada incidente de seguridad, así como los aspectos relacionados con la imagen y reputación de la organización y las relaciones públicas.

3.2 DETECCIÓN DE UN INCIDENTE DE SEGURIDAD: RECOLECCIÓN DE INFORMACIÓN

La organización debería prestar especial atención a los posibles indicadores de un incidente de seguridad, como una actividad a contemplar dentro del Plan de Respuesta a Incidentes. Seguidamente se presenta una relación de los principales indicadores de posibles incidentes de seguridad:

- Precursores de un ataque: actividades previas de reconocimiento del sistema informático, como el escaneo de puertos, el escaneo de vulnerabilidades en servidores, el reconocimiento de versiones de sistemas operativos y aplicaciones...
- Alarmas generadas en los Sistemas de Detección de Intrusos (IDS), en los cortafuegos o en las herramientas antivirus.
- Registro de actividad extraña en los *logs* de servidores y dispositivos de red o incremento sustancial del número de entradas en los *logs*.
- Aparición de nuevas carpetas o ficheros con nombres extraños en un servidor, o modificaciones realizadas en determinados ficheros del sistema (*librerías*, *kernel*, aplicaciones críticas...), que se pueden detectar mediante herramientas de revisión de la integridad de ficheros.
- Caída o mal funcionamiento de algún servidor: reinicios inesperados, fallos en algunos servicios, aparición de mensajes de error, incremento anormal de la carga del procesador o del consumo de memoria del sistema...
- Notable caída en el rendimiento de la red o de algún servidor, debido a un incremento inusual del tráfico de datos.

- Cambios en la configuración de determinados equipos de la red: modificación de las políticas de seguridad y auditoría, activación de nuevos servicios, puertos abiertos que no estaban autorizados, activación de las tarjetas de red en modo promiscuo (para poder capturar todo el tráfico que circula por la red interna mediante *sniffers*), etcétera.
- Existencia de herramientas no autorizadas en el sistema.
- Aparición de nuevas cuentas de usuario o registro de actividad inusual en algunas cuentas⁹: conexiones de usuarios en unos horarios extraños (por ejemplo, por las noches o durante un fin de semana), utilización de la misma cuenta desde distintos equipos a la vez, bloqueo reiterado de cuentas por fallos en la autenticación, ejecución inusual de determinados servicios desde algunas cuentas, etcétera.
- Informes de los propios usuarios del sistema alertando de algún comportamiento extraño o de su imposibilidad de acceder a ciertos servicios.
- Detección de procesos extraños en ejecución dentro de un sistema, que se inician a horas poco habituales o que consumen más recursos de los normales (tiempo de procesador o memoria)¹⁰.
- Generación de tráfico extraño en la red: envío de mensajes de correo electrónico hacia el exterior con contenido sospechoso, inusual actividad de transferencia de ficheros, escaneo de otros equipos desde un equipo interno...
- Notificación de un intento de ataque lanzado contra terceros desde equipos pertenecientes a la propia organización.
- Desaparición de equipos de la red de la organización.
- Aparición de dispositivos extraños conectados directamente a la red o a algunos equipos de la organización (en este último caso podrían ser, por ejemplo, dispositivos para la captura de pulsaciones de teclado en los equipos).

Conviene tener en cuenta que los ataques informáticos se están volviendo cada vez más sofisticados, por lo que es difícil conseguir detectarlos a tiempo. Incluso existen herramientas que facilitan este tipo de ataques ocultando su actividad y que se pueden obtener de forma gratuita en Internet.

Por otra parte, la gran cantidad de información que se genera en los *logs* y en las distintas herramientas de seguridad puede dificultar su posterior estudio, debido sobre todo a la pérdida de tiempo provocada por los "falsos positivos". Por este motivo, es necesario contar con herramientas y filtros que faciliten la detección y clasificación de los incidentes.

9 Para ello, se pueden utilizar aplicaciones como *finger* y *who* en sistemas UNIX/LINUX, que muestran los usuarios que se encuentran conectados al sistema, desde qué terminal o equipo están conectados y en qué momento iniciaron su sesión.

10 Para ello, podría resultar de utilizar el comando "*ps*" en sistemas UNIX/LINUX, que muestra la relación de procesos en ejecución en el sistema.

3.3 ANÁLISIS DE UN INCIDENTE DE SEGURIDAD

El Plan de Respuesta a Incidentes debe definir cómo el equipo de respuesta debería proceder al análisis de un posible incidente de seguridad en cuanto éste fuese detectado por la organización, determinando en primer lugar cuál es su alcance: ¿qué equipos, redes, servicios y/o aplicaciones se han podido ver afectados? ¿Se ha podido comprometer información confidencial de la organización o de sus usuarios y clientes? ¿Ha podido afectar a terceros?

Seguidamente, el equipo de respuesta debería determinar cómo se ha producido el incidente: qué tipo de ataque informático (si lo ha habido) ha sido el causante, qué vulnerabilidades del sistema han sido explotadas, qué métodos ha empleado el atacante, etcétera.

Se podría utilizar una **Matriz de Diagnóstico** para facilitar la actuación del equipo en momentos de máximo estrés, evitando que se puedan tomar decisiones precipitadas que conduzcan a errores, constituyendo además un valioso apoyo para el personal con menos experiencia en la actuación frente a incidentes de seguridad.

Tabla 3.2. Ejemplo de Matriz de Diagnóstico

Síntoma	Código malicioso	Denegación de servicio (DoS)	Acceso no autorizado
Escaneo de puertos	Bajo	Alto	Medio
Caída de un servidor	Alto	Alto	Medio
Modificación de ficheros de un equipo	Alto	Bajo	Alto
Tráfico inusual en la red	Medio	Alto	Medio
Ralentización de los equipos o de la red	Medio	Alto	Bajo
Envío de mensajes de correo sospechosos	Alto	Bajo	Medio

Así mismo, conviene realizar una valoración inicial de los daños y de sus posibles consecuencias, para a continuación establecer un orden de prioridades en las actividades que debería llevar a cabo el equipo de respuesta, teniendo para ello en consideración aspectos como el posible impacto del incidente en los recursos y servicios de la organización y en el desarrollo de su negocio o actividad principal.

En este sentido, los documentos RFC 1244 y RFC 2196 (del IETF, *Internet Engineering Task Force*) proponen la siguiente priorización de las actividades a realizar por parte de un equipo de respuesta a incidentes:

- **Prioridad uno:** proteger la vida humana y la seguridad de las personas.
- **Prioridad dos:** proteger datos e información sensible de la organización.
- **Prioridad tres:** proteger otros datos e información de la organización.
- **Prioridad cuatro:** prevenir daños en los sistemas informáticos (pérdida o modificación de ficheros básicos para las aplicaciones y los servidores).
- **Prioridad cinco:** minimizar la interrupción de los servicios ofrecidos a los distintos usuarios (internos y externos).

3.4 CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Dentro del Plan de Respuesta a Incidentes, el equipo de respuesta debe elegir una determinada estrategia de **contención** del incidente de seguridad. Una primera opción sería llevar a cabo una rápida actuación para evitar que el incidente pueda tener mayores consecuencias para la organización: apagar todos los equipos afectados, desconexión de estos equipos de la red informática, desactivación de ciertos servicios, etcétera. Esta estrategia de contención es la más adecuada cuando se puedan ver afectados servicios críticos para la organización, se pueda poner en peligro determinada información confidencial, se estén aprovechando los recursos de la organización para lanzar ataques contra terceros o cuando las pérdidas económicas puedan ser considerables.

Una segunda alternativa sería retrasar la contención para poder estudiar con más detalle el tipo de incidente y tratar de averiguar quién es el responsable del mismo. Esta estrategia se puede adoptar siempre y cuando sea posible monitorizar y controlar la actuación de los atacantes, para de este modo reunir las evidencias necesarias que permitan iniciar las correspondientes actuaciones legales contra los responsables del incidente. No obstante, se corre el riesgo de que el incidente pueda tener peores consecuencias para la organización o para terceros (y en este último caso la organización podría ser considerada culpable por no haber actuado a tiempo).

Por otra parte, en algunos tipos de ataque las medidas de contención adoptadas podrían desencadenar mayores daños en los sistemas informáticos comprometidos. Así, por ejemplo, un equipo controlado por un *cracker* podría estar ejecutando un servicio que se encargaría de realizar *pings* periódicos a determinados servidores o comprobar el estado de las conexiones de red, de tal modo que si se detectase una desconexión del equipo del resto de la red, se desencadenaría otro proceso encargado de eliminar todas las pruebas del disco duro del equipo.

También hay que tener en cuenta que en los ataques de Denegación de Servicio (DoS) puede resultar necesario contar con la colaboración de las empresas proveedoras de acceso a Internet o de administradores de las redes de otras organizaciones para contener el ataque.

Por su parte, la **erradicación** es la etapa del Plan de Respuesta a Incidentes en la que se llevan a cabo todas las actividades necesarias para eliminar los agentes causantes del incidente y de sus secuelas, entre las que podríamos citar posibles “puertas traseras” instaladas en los equipos afectados, *rootkits*¹¹ u otros códigos malignos (virus, gusanos...), contenidos y material inadecuado que se haya introducido en los servidores, cuentas de usuario creadas por los intrusos o nuevos servicios activados en el incidente. También será conveniente llevar a cabo una revisión de otros sistemas que se pudieran ver comprometidos a través de las relaciones de confianza con el sistema afectado.

Por último, la **recuperación** es la etapa del Plan de Respuesta a Incidentes en la que se trata de restaurar los sistemas para que puedan volver a su normal funcionamiento. Para ello, será necesario contemplar tareas como la reinstalación del sistema operativo y de las aplicaciones partiendo de una copia segura, la configuración adecuada de los servicios e instalación de los últimos parches y actualizaciones de seguridad, el cambio de contraseñas que puedan haber sido comprometidas, la desactivación de las cuentas que hayan sido utilizadas en el incidente, la revisión de las medidas de seguridad para prevenir incidentes similares y la prueba del sistema para comprobar su correcto funcionamiento.

3.5 IDENTIFICACIÓN DEL ATACANTE Y POSIBLES ACTUACIONES LEGALES

Dentro del Plan de Respuesta a Incidentes, la identificación del atacante es necesaria para poder emprender acciones legales para exigir responsabilidades y reclamar indemnizaciones. No obstante, conviene tener en cuenta que generalmente solo se podrá identificar la máquina o máquinas desde las que se ha llevado a cabo el ataque, pero no directamente al individuo responsable de su utilización.

¹¹ Un rootkit es un programa dañino que simula actuar como una herramienta o servicio legítimo del sistema infectado. Para ello, el atacante se encarga de reemplazar el fichero original del programa que pretende suplantar.

La identificación del atacante puede ser una tarea que consuma bastante tiempo y recursos, por lo que no debería interferir en la contención y erradicación del incidente. Algunas organizaciones optan por no perseguir legalmente a los atacantes por el esfuerzo necesario: costes, trámites judiciales, publicación en los medios...

Además, los ataques realizados desde otros países con ciertas lagunas legales en el tratamiento de los delitos informáticos pueden dificultar las reclamaciones judiciales, ya que se complica en gran medida el proceso de extradición de los responsables¹².

Existen distintas técnicas para determinar la dirección IP del equipo (o equipos) desde el que se ha llevado a cabo el ataque contra el sistema informático: utilización de herramientas como *ping*, *traceroute* o *whois*; consulta en los registros inversos de servidores DNS; etcétera.

No obstante, es necesario tener en cuenta una serie de obstáculos que pueden dificultar esta tarea:

- Mediante técnicas de *IP Spoofing* se podría enmascarar la dirección en algunos tipos de ataque.
- El atacante podría estar utilizando equipos de terceros para realizar sus acciones, situación que se produce con bastante frecuencia hoy en día.
- El atacante podría haber empleado una dirección IP dinámica, asignada a su equipo por un proveedor de acceso a Internet.
- El equipo del atacante podría estar situado detrás de un servidor *proxy* con el servicio NAT activo (traducción de direcciones internas a una dirección externa), compartiendo una dirección IP pública con otros equipos de la misma red.

Por este motivo, en muchos casos será necesario solicitar la colaboración de los responsables de otras redes y de los proveedores de acceso a Internet que pudieran haber sido utilizados por los atacantes.

Una tarea que también podría contribuir a la identificación del atacante es el análisis de las actividades de exploración (escaneos de puertos y de vulnerabilidades en el sistema) que suelen anteceder a un ataque, sobre todo si éstas han podido ser registradas por los *logs* de los equipos afectados o por el Sistema de Detección de Intrusiones (IDS).

En cuanto a la ejecución de acciones contra el atacante, se recomienda presentar una denuncia ante las unidades policiales especializadas en este tipo de incidentes o ataques informáticos, para poder emprender de este modo las correspondientes actuaciones policiales y judiciales.

¹² En estos casos se requiere de la existencia de un tratado de cooperación judicial entre los países involucrados en el proceso.

Conviene destacar que si la organización decidiese actuar por su propia cuenta, “tomando la justicia por su mano”, es decir, realizar ataques a modo de represalia contra los equipos desde los que aparentemente se está produciendo un intento de intrusión contra sus propios equipos y redes informáticas, esta actuación podría tener graves consecuencias para la organización. Si el atacante ha utilizado técnicas de enmascaramiento (como *IP Spoofing*), la organización podría lanzar un ataque contra equipos y redes inocentes, con las correspondientes responsabilidades legales que se derivan de esta actuación, por lo que podría ser denunciada por las organizaciones propietarias de estos equipos atacados a modo de represalia.

3.6 COMUNICACIÓN CON TERCEROS Y RELACIONES PÚBLICAS

El Plan de Respuesta a Incidentes tiene que contemplar cómo la organización debería comunicar a terceros la causa y las posibles consecuencias de un incidente de seguridad informática.

Así, dentro de este Plan de Respuesta deberían estar previstos los contactos con organismos de respuesta a incidentes de seguridad informática (como el CERT), con las fuerzas de seguridad (Policía o Guardia Civil en España), con agencias de investigación y con los servicios jurídicos de la organización.

También podría ser necesario establecer contactos con proveedores de acceso a Internet, ya sea el proveedor de la propia organización o el proveedor o proveedores que dan servicio a equipos desde los que se ha originado un ataque contra la organización.

Del mismo modo, en algunos casos sería recomendable contactar con los fabricantes de hardware y/o software que se hayan visto involucrados en el incidente, debido a una vulnerabilidad o una mala configuración de sus productos.

En el Plan de Respuesta a Incidentes también se deben contemplar los contactos con terceros que pudieran haber sido perjudicados por el incidente de seguridad, como en el caso de que se hubieran utilizado ordenadores de la organización para realizar un ataque contra sistemas y redes de otras entidades. De este modo, se podrían limitar las responsabilidades legales en las que podría incurrir la organización por culpa del incidente de seguridad.

Por otra parte, hay que tener en cuenta el cumplimiento de la normativa existente ya en algunos países, que obliga a la notificación de los incidentes de seguridad a determinados organismos de la Administración, así como a los ciudadanos (generalmente clientes de la organización) que pudieran verse afectados por dicho incidente. En los contactos con los clientes de la organización, el personal debería poder transmitir seguridad y tranquilidad, indicando en todo momento que “la situación está controlada”.

Por último, también será conveniente definir un Plan de Comunicación con los Medios: agencias de noticias, prensa, emisoras de radio y TV... Para ello, la organización debería establecer quién se encargará de hablar con los medios y qué datos se podrán facilitar en cada momento.

El interlocutor debería estar preparado para responder a preguntas del estilo: ¿quién ha sido el responsable del ataque o incidente?; ¿cómo pudo suceder?; ¿hasta qué punto se ha extendido por la organización?; ¿qué medidas están adoptando para contrarrestarlo?; ¿cuáles pueden ser sus consecuencias técnicas y económicas?; etcétera.

En la comunicación con los medios, la organización debería procurar no revelar información sensible, como los detalles técnicos de las medidas adoptadas para responder al incidente de seguridad, y evitar en la medida de lo posible las especulaciones sobre las causas o los responsables del incidente de seguridad.

3.7 DOCUMENTACIÓN DEL INCIDENTE DE SEGURIDAD

El Plan de Respuesta a Incidentes debería establecer cómo se tiene que documentar un incidente de seguridad, reflejando de forma clara y precisa aspectos como los que se presentan en la siguiente relación:

Tabla 3.3. Documentación de un incidente de seguridad

- Descripción del tipo de incidente.
 - Hechos registrados (eventos en los logs de los equipos).
 - Daños producidos en el sistema informático.
 - Decisiones y actuaciones del equipo de respuesta.
 - Comunicaciones que se han realizado con terceros y con los medios.
 - Lista de evidencias obtenidas durante el análisis y la investigación.
 - Comentarios e impresiones del personal involucrado.
 - Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en el futuro.
-

La *Trans-European and Education Network Association* (TERENA) ha desarrollado un estándar para facilitar el registro e intercambio de información sobre incidentes de seguridad: el estándar RFC 3067, con recomendaciones sobre la información que debería ser registrada en cada incidente (*Incident Object Description and Exchange Format Requirements*).

Conviene destacar que una correcta y completa documentación del incidente facilitará el posterior estudio de cuáles han sido sus posibles causas y sus consecuencias en el sistema informático y los recursos de la organización. Por supuesto, será necesario evitar que personal no autorizado pueda tener acceso a esta documentación sensible.

3.8 ANÁLISIS Y REVISIÓN A POSTERIORI DEL INCIDENTE: VERIFICACIÓN DE LA INTRUSIÓN

Dentro del Plan de Respuesta a Incidentes se tiene que contemplar una etapa para el análisis y revisión a posteriori de cada incidente de seguridad, a fin de determinar qué ha podido aprender la organización como consecuencia del mismo.

Con tal motivo, será necesario elaborar un informe final sobre el incidente, en el que se puedan desarrollar los siguientes aspectos de forma detallada:

- Investigación sobre las causas y las consecuencias del incidente:
- Estudio de la documentación generada por el equipo de respuesta a incidentes.
- Revisión detallada de los registros de actividad (*logs*) de los ordenadores y dispositivos afectados por el incidente.
- Evaluación del coste del incidente de seguridad para la organización: equipos dañados, software que se haya visto afectado, datos destruidos, horas de personal dedicado a la recuperación de los equipos y los datos, información confidencial comprometida, necesidad de soporte técnico externo, etcétera.
- Análisis de las consecuencias que haya podido tener para terceros.
- Revisión del intercambio de información sobre el incidente con otras empresas e instituciones, así como con los medios de comunicación.
- Seguimiento de las posibles acciones legales emprendidas contra los responsables del incidente.
- Revisión de las decisiones y actuaciones del equipo de respuesta a incidentes:
- Composición y organización del equipo.
- Formación y nivel de desempeño de los miembros.

- Rapidez en las actuaciones y decisiones: ¿cómo respondió el personal involucrado en el incidente?; ¿qué tipo de información se obtuvo para gestionar el incidente?; ¿qué decisiones se adoptaron?
- Análisis de los procedimientos y de los medios técnicos empleados en la respuesta al incidente:
 - Redefinición de aquellos procedimientos que no hayan resultado adecuados.
 - Adopción de las medidas correctivas que se consideren necesarias para mejorar la respuesta ante futuros incidentes de seguridad.
- Adquisición de herramientas y recursos para reforzar la seguridad del sistema y la respuesta ante futuros incidentes de seguridad.
- Revisión de las Políticas de Seguridad de la organización.
- Definición de nuevas directrices y revisión de las actualmente previstas por la organización para reforzar la seguridad de su sistema informático.

3.9 PRÁCTICAS RECOMENDADAS POR EL CERT/CC

El CERT/CC (*Computer Emergency Response Team/Coordination Center*) ha propuesto una serie de actividades para mejorar la respuesta de una organización ante los incidentes de seguridad informática. Seguidamente se presenta un extracto con algunas de las principales actividades propuestas por este organismo, agrupadas en tres fases o etapas:

3.9.1 Preparación de la respuesta ante incidentes de seguridad

- Definición del plan de actuación y los procedimientos para responder a los incidentes, especificando, entre otras cuestiones, a quién se debe informar en caso de incidente o qué tipo de información se debe facilitar y en qué momento (fase del incidente).
- Documentación del plan de actuación y de los procedimientos para responder a los incidentes.
- Comprobación de que el plan de actuación y los procedimientos previstos cumplen con los requisitos legales y las obligaciones contractuales con terceros (como, por ejemplo, exigencias de los clientes de la organización).

- Adquisición e instalación de herramientas informáticas y dispositivos que faciliten la respuesta ante incidentes. Conviene disponer de equipos redundantes, dispositivos de red y medios de almacenamiento para poder recuperar el funcionamiento normal del sistema.
- Verificación de los procedimientos y dispositivos de copias de seguridad.
- Creación de un archivo de discos de arranque y un conjunto de copias con todas las aplicaciones y servicios necesarios para el funcionamiento de los sistemas informáticos, así como de los parches y actualizaciones correspondientes.
- Formación y entrenamiento del personal afectado por este plan y procedimientos de actuación.
- Mantenimiento actualizado de una base de datos de contactos (personas y organizaciones).

3.9.2 Gestión del incidente de seguridad

- Aislamiento de los equipos afectados por el incidente, realizando además una copia de seguridad completa de sus discos duros.
- Captura y protección de toda la información asociada con el incidente: registros de actividad (*logs*) de los equipos y dispositivos de red, ficheros dentro de los servidores, tráfico intercambiado a través de la red, etcétera.
- Catalogación y almacenamiento seguro de toda esta información para poder preservar las evidencias. Convendría disponer de copias de seguridad con la información del estado previo y del estado posterior al incidente de los equipos y sistemas afectados.
- Revisión de toda la información disponible para poder caracterizar el tipo de incidente o intento de intrusión. Análisis detallado de los registros de actividad (*logs*) y del estado de los equipos para determinar cuál puede ser el tipo de ataque o incidente, qué sistemas se han visto afectados, qué modificaciones han realizado o qué programas han ejecutado los posibles intrusos dentro de estos sistemas.
- Comunicación con todas las personas y organismos que deberían ser informados del incidente, cumpliendo con lo establecido en las políticas y procedimientos de respuesta a incidentes. Mantenimiento de un registro detallado de todas las comunicaciones y contactos establecidos durante la respuesta ante el incidente.
- Participación en las medidas de investigación y de persecución legal de los responsables del incidente.

- Aplicación de soluciones de emergencia para tratar de contener el incidente: desconectar los equipos afectados de la red corporativa; desactivar otros dispositivos y servicios afectados; apagar temporalmente los equipos más críticos; cambiar contraseñas e inhabilitar cuentas de usuarios; monitorizar toda la actividad en estos equipos; verificar que se dispone de copias de seguridad de los datos de los equipos afectados por el incidente; etcétera.
- Eliminación de todos los medios posibles que faciliten una nueva intrusión en el sistema: cambiar todas las contraseñas de los equipos a los que hayan podido tener acceso atacantes o usuarios no autorizados; revisar la configuración de los equipos; detectar y anular los cambios realizados por los atacantes en los equipos afectados; restaurar programas ejecutables y ficheros binarios (como las librerías del sistema) desde copias seguras; mejorar, si es posible, los mecanismos de registro de la actividad en estos equipos.
- Recuperación de la actividad normal de los sistemas afectados: reinstalación de aplicaciones y servicios, incluyendo los parches y actualizaciones de seguridad; restauración de los datos de los usuarios y las aplicaciones desde copias de seguridad; recuperación de las conexiones y servicios de red; verificación de la correcta configuración de estos equipos.

3.9.3 Seguimiento del incidente de seguridad

- Identificación de las lecciones y principales conclusiones de cada incidente, recurriendo para ello al análisis post mórtem de los equipos afectados por el incidente y entrevistando a las personas implicadas en la gestión del incidente.
- Implementación de las mejoras de seguridad propuestas como consecuencia de las "lecciones aprendidas" en cada incidente: revisión de las políticas y procedimientos de seguridad, realización de un nuevo análisis detallado de las vulnerabilidades y riesgos del sistema, etcétera.

3.10 OBLIGACIÓN LEGAL DE NOTIFICACIÓN DE ATAQUES E INCIDENCIAS

La obligación legal de notificación de ataques e incidencias que puedan afectar a la seguridad informática es una medida que ya ha sido adoptada por el Estado de California en Estados Unidos. Así, en este Estado desde el 1 de julio de 2003 todos los *websites* de comercio electrónico están obligados por ley a informar a sus clientes cuando se haya producido una violación de la seguridad de su sistema informático.

De hecho la "Senate Bill 1386" fue aprobada en California en septiembre de 2002, después de que tuviese lugar una intrusión en los sistemas de nóminas de este Estado, a consecuencia de la cual los datos de más de doscientos mil empleados del Estado cayeron en manos de los atacantes, con un notable riesgo de fraudes y robos de identidad.

En virtud de lo dispuesto por esta ley, toda empresa afectada por un ataque o incidencia informática deberá informar de este hecho por correo electrónico a sus clientes, indicándoles que el número de su tarjeta de crédito o algún otro dato de carácter personal podría haber sido sustraído de los ordenadores de la empresa. Esta alerta informativa se tendrá que enviar tanto en caso de robo de información como cuando hayan sido descubiertas brechas de seguridad en el *website* de la empresa.

Esta ley del Estado de California no contempla la aplicación de multas a quienes no cumplan con este requisito, pero sí abre las puertas a todo tipo de procesos legales contra las empresas afectadas.

En la actualidad se estudia la posibilidad de aplicar esta misma medida a todas las empresas que cotizan en bolsa en Estados Unidos.

3.11 PLAN DE RECUPERACIÓN DEL NEGOCIO

Las empresas son cada vez más conscientes de la necesidad de estar preparadas para poder responder ante todo tipo de desastres y situaciones catastróficas, como podrían ser los incendios, inundaciones, terremotos, consecuencias de huracanes, etcétera. Sin embargo, estas situaciones también se podrían producir debido a los daños ocasionados por sabotajes, robos o, incluso, por atentados terroristas.

En este contexto, la definición e implantación de un **Plan de Recuperación del Negocio**, también conocido como **Plan de Continuidad del Negocio** o **Plan de Contingencias**, constituye un elemento fundamental para poder garantizar una respuesta adecuada frente a desastres y situaciones catastróficas, asegurando la integridad y la recuperación de los datos.

En este Plan de Recuperación se deben especificar los objetivos y prioridades a tener en cuenta por la organización en caso de un desastre que pueda afectar a la continuidad de su negocio. Para ello, es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento del sistema informático de la organización, así como recuperar los datos, aplicaciones y servicios básicos que se utilizan como soporte al negocio de la organización:

- Disponibilidad de un Centro Alternativo o Centro de Reserva para la ubicación de los principales recursos informáticos (servidores y bases de datos corporativas).

- Existencia de líneas de *back-up* para las comunicaciones.
- Sistemas de almacenamiento RAID en los servidores.
- Implantación de *clusters* de servidores con balanceo de carga.
- Herramientas para llevar a cabo una replicación de los documentos y las bases de datos, que puede ser síncrona, asíncrona o periódica.

Así mismo, se tiene que definir en el Plan de Recuperación del Negocio cuál va a ser la composición de un equipo de dirección que se encargará de coordinar todas las tareas de recuperación frente a un desastre, realizando esta labor desde un determinado centro de control, cuya ubicación también tiene que haber sido previamente especificada en el Plan de Recuperación.

Un elemento fundamental dentro del Plan de Recuperación del Negocio es la existencia de un **Centro Alternativo**, también conocido como **Centro de Respaldo** o **Centro de Back-up**, si bien en la práctica solo las grandes empresas podrán disponer de un local o edificio dedicado exclusivamente a esta misión. Este centro tendría que estar equipado con los equipos informáticos adecuados y contar con copias de seguridad de los datos más críticos para el negocio suficientemente actualizadas.

Este Centro Alternativo debería contar con las mismas medidas de seguridad informática que las instalaciones principales de la organización. Para su correcta implantación es necesario contemplar no solo el equipamiento de hardware y de software, sino también aspectos organizativos relacionados con su gestión. Así mismo, se debe tener presente este Centro Alternativo a la hora de instalar nuevos sistemas informáticos en la organización, para que pueda estar puesto al día y sea compatible con los nuevos sistemas implantados.

Las organizaciones pueden adoptar distintas estrategias a la hora de implantar un Centro Alternativo:

- No se dispone de un Centro Alternativo y no existen copias de seguridad externas. En esta situación el tiempo de recuperación puede ser impredecible e, incluso, dependiendo de la gravedad del desastre, es posible que nunca se puedan llegar a recuperar totalmente los datos, programas y la documentación del sistema afectado. Debemos señalar que un importante porcentaje de empresas y organizaciones de todo tipo (sobre todo las de menor tamaño) todavía se encuentra en esta situación.
- Transporte periódico de copias de seguridad a un almacén. En este caso podemos considerar que ya existe un Plan de Recuperación del Negocio, gracias a la existencia de copias de seguridad más o menos actualizadas en otra ubicación física. No obstante, el tiempo de recuperación puede ser alto, posiblemente superior a una semana, ya que no se dispone de un Centro Alternativo con

equipos adecuados para volver a poner en marcha las aplicaciones y servicios informáticos de la organización.

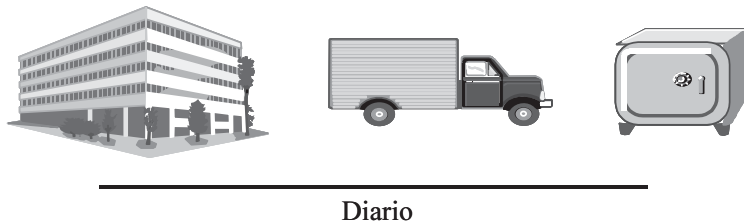


Figura 3.1. Transporte de copias de seguridad a un almacén

- Centro Alternativo "Frío": Se trata de un Centro Alternativo que cuenta con un equipamiento suficiente de hardware, software y de comunicaciones para mantener los servicios críticos de la organización. Así mismo, en este centro se guardan copias de seguridad de los datos y aplicaciones de la organización. El tiempo de recuperación puede ser de uno a varios días, ya que es necesario restaurar los datos y las aplicaciones desde las copias de seguridad, poniendo en funcionamiento los distintos equipos del Centro Alternativo.
- Centro Alternativo "Caliente": Se trata de un Centro Alternativo que cuenta con el equipamiento de hardware, software y de comunicaciones necesario para mantener los servicios críticos de la organización, y en el que además estos equipos se encuentran en funcionamiento y disponen de una réplica de todos los datos y aplicaciones del sistema informático, que se realizan de forma diaria o incluso cada hora. De este modo, el tiempo de recuperación es de unas pocas horas, inferior a un día.
- Centro Alternativo "Caliente" en una configuración en "espejo" (*mirror*): Se trata de un Centro Alternativo con el mismo equipamiento que el Centro Principal y que trabaja de un modo paralelo a éste, pudiendo entrar en acción inmediatamente a la caída del Centro Principal. Se trata, por tanto, de un sistema redundante, adecuado para situaciones que requieran de una alta disponibilidad.

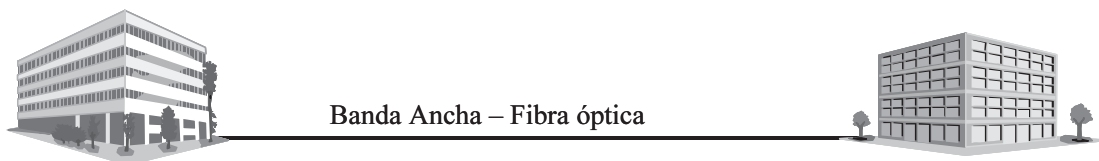


Figura 3.2. Centro Alternativo "Caliente"

Por otra parte, debemos destacar la importancia de documentar el sistema informático al mayor nivel de detalle posible, ya que en caso de desastre no siempre se podrá disponer de las personas clave para poder disponer de esta información.

En una empresa de pequeño o mediano tamaño se podría plantear la posibilidad de subcontratar este Centro Alternativo a una empresa especializada, por ejemplo, un *Data Center* de un operador de telecomunicaciones, formalizando la relación mediante un contrato en el que se contemple las condiciones y el nivel de servicio (*Service Level Agreement*).

Un procedimiento para la recuperación frente a desastres debería contemplar las siguientes actividades:

- Detección y respuesta al desastre en el Centro Principal:
 - Adopción de las medidas de contención previstas dependiendo del tipo de desastre: incendio, inundación, explosión...
 - Comunicación a las personas y organismos externos indicados según el tipo de desastre.
- Traslado de la actividad al Centro Alternativo:
 - Traslado del personal necesario al Centro Alternativo.
 - Puesta en marcha de los servidores y equipos informáticos.
 - Volcado de los datos disponibles en las copias de seguridad más recientes.
 - Recuperación de las aplicaciones y servicios necesarios para la continuidad de las operaciones, priorizando el orden de esta recuperación en función de su importancia o criticidad para el funcionamiento de la organización.
 - Verificación del nivel de servicio recuperado.
 - Registro de todos los incidentes ocurridos durante este proceso.
- Recuperación del Centro Principal siniestrado.

El resultado de este procedimiento de recuperación se puede determinar a partir de indicadores como el RTO (*Recovery Time Objective*), que informa de en cuánto tiempo se puede recuperar el sistema informático de la organización, así como el RPO (*Recovery Point Objective*), que indica hasta dónde se puede recuperar el sistema.

Debemos destacar la importancia de llevar a cabo auditorías y pruebas periódicas para garantizar la correcta ejecución de los procedimientos previstos para la continuidad del negocio: detección y respuesta al desastre en el Centro Principal, traslado de la actividad al Centro Alternativo y recuperación del Centro Principal siniestrado. Así mismo, en todo este proceso también resulta fundamental la adecuada formación y entrenamiento periódicos del personal que pueda estar implicado en las actividades de recuperación.

3.12 ORGANISMOS DE GESTIÓN DE INCIDENTES

Para combatir de forma más eficaz las distintas amenazas que afectan a la seguridad de los sistemas informáticos, en estos últimos años se han creado varios organismos especializados cuya misión es alertar a los gobiernos, empresas y ciudadanos en general para poder contener y minimizar los daños ocasionados por los ataques informáticos.

3.12.1 CERT/CC (*Computer Emergency Response Team/Coordination Center*)

El CERT, el “Equipo de Respuesta a Emergencias Informáticas”, es el primer y más conocido centro de respuesta, creado en diciembre de 1988 por la agencia DARPA de Estados Unidos para gestionar los incidentes de seguridad relacionados con Internet.

Se encuentra en el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon. La dirección en Internet es <http://www.cert.org>.



3.12.2 CERT INTECO

El Centro de Respuesta a Incidentes de Seguridad fue creado en 2006 en España dentro del Instituto Nacional de Tecnologías de la Información (INTECO).

Su dirección en Internet es <http://cert.inteco.es/>.



3.12.3 Agencia Europea de Seguridad de las Redes y de la Información

Agencia europea creada por decisión del Consejo y del Parlamento (EC 460/2004) con la finalidad de alcanzar un alto nivel de seguridad en las redes y en el tratamiento de la información dentro de la Unión Europea. Esta Agencia comenzó oficialmente sus actividades en septiembre de 2005, tras fijar su sede institucional en la isla de Creta.

Su dirección en Internet es <http://www.enisa.europa.eu/>.



3.12.4 CSRC (Computer Security Resource Center)

EL CSRC, "Centro de Recursos de Seguridad Informática", es un centro dependiente del NIST (*National Institute Standards of Technology* de Estados Unidos).

Su dirección en Internet es <http://csrc.nist.gov/>.

3.12.5 US-CERT

El US-CERT es un Centro de Respuesta a Incidentes de Seguridad Informática que depende del *National Cyber Security Division* (NCSD) en el Departamento de Seguridad Interior (*Department of Homeland Security* –DHS–) de Estados Unidos.

3.12.6 FIRST (Forum of Incident Response and Security Teams)

Foro constituido en 1990 con el objetivo de facilitar el intercambio de información sobre incidentes de seguridad entre los distintos miembros que lo integran (Centros de Respuesta a Incidentes de distintos países y organizaciones), así como para la detección, prevención y recuperación de estos incidentes de seguridad.

Su dirección en Internet es <http://www.first.org/>.

3.12.7 Otros centros de seguridad y respuesta a incidentes

Otros países también han puesto en marcha sus respectivos centros de respuesta a incidentes de seguridad, como el AusCERT (*Australian Computer Emergency Response Team*, <http://www.auscert.org.au>) de Australia o el DFN-CERT (*Computer Emergency Response Team for the German Research Network*, <http://www.cert.dfn.de>) de Alemania.

En España también podemos destacar los servicios del IRIS-CERT, Centro de Respuesta a Incidentes de Seguridad de la Red IRIS, que da soporte a los Centros de Investigación y Universidades del país, a través de la dirección de Internet <http://www.rediris.es/cert/>.

Así mismo, el Centro de Alerta Temprana sobre Virus y Seguridad Informática fue creado en julio de 2001 por el Ministerio de Ciencia y Tecnología español, para ofrecer información, alertas y distintos recursos sobre seguridad informática a ciudadanos y empresas, a través de la dirección <http://www.alerta-antivirus.es>. En la actualidad se encuentra integrado dentro del INTECO, en la dirección <http://www.inteco.es/Seguridad>.

3.12.8 Bases de datos de ataques e incidentes de seguridad

También existen distintos organismos que se encargan de capturar y agrupar los registros de incidencias (*logs*) y ataques sufridos por distintas organizaciones en una base de datos. DShield (*Distributed Intrusion Detection System*, Sistema de Detección de Intrusiones Distribuido) es una de las bases de datos sobre incidentes de seguridad informática más conocida (<http://www.dshield.org/>).

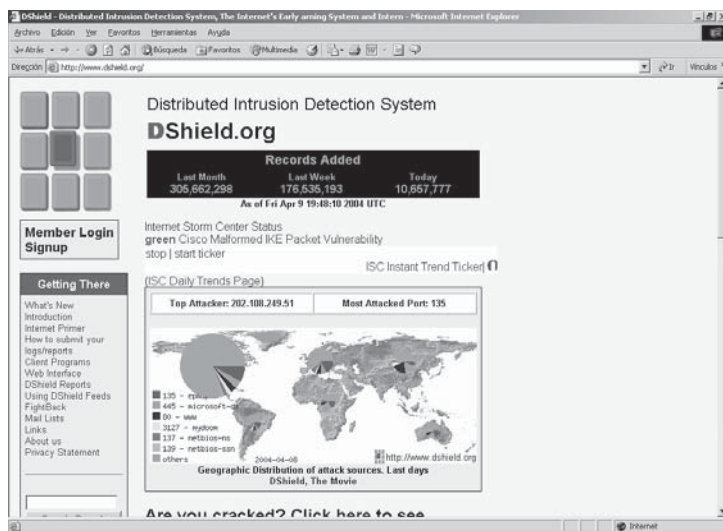


Figura 3.3. DShield.org

Otra completa base de datos con referencias sobre incidentes de seguridad se encuentra disponible en Security Focus (<http://www.securityfocus.com/>).

Así mismo, también podemos encontrar algunos servicios que se encargan de evaluar el estado del tráfico en Internet, como *Internet Health Monitoring* (www.internetpulse.net), que contribuye a la detección y control de los ataques de Denegación de Servicio (DoS).

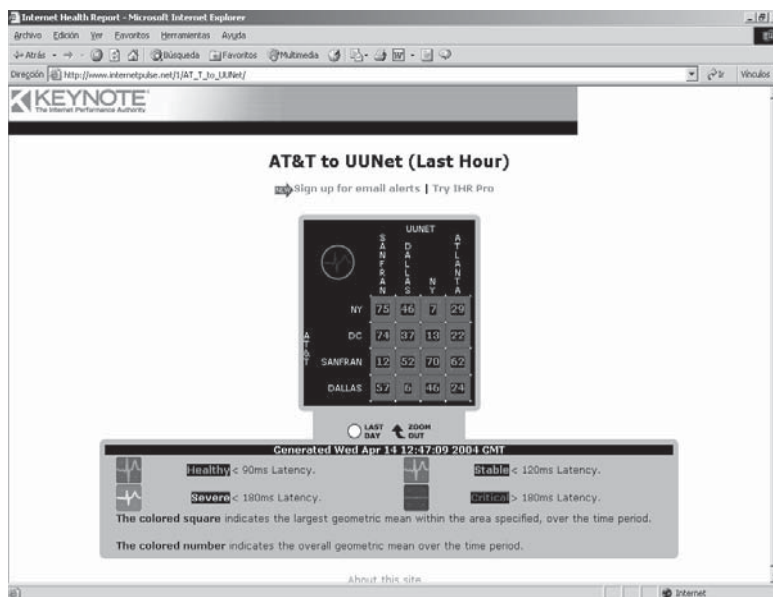


Figura 3.4. Internetpulse.net

3.13 DIRECCIONES DE INTERÉS



- Base de datos NSRL (National Software Reference Library) del NIST: <http://www.nsrl.nist.gov/>.
- RFC 2350 - Expectations for Computer Security Incident Response: <http://www.ietf.org/rfc/rfc2350.txt>.
- CERT: <http://www.cert.org/>.
- CERT - INTECO: <http://cert.inteco.es/>.
- ENISA: <http://www.enisa.europa.eu/>.
- US-CERT: <http://www.us-cert.gov/>.

- CSRC: *<http://csrc.nist.gov/>*.
- FIRST: *<http://www.first.org/>*.
- IRIS-CERT: *<http://www.rediris.es/cert/>*.
- AusCERT: *<http://www.auscert.org.au/>*.
- DFN-CERT: *<http://www.cert.dfn.de/>*.

ANÁLISIS FORENSE INFORMÁTICO

4.1 OBJETIVOS DE LA INFORMÁTICA FORENSE

La **Ciencia Forense** nos proporciona los principios y técnicas que facilitan la investigación de los delitos criminales, mediante la identificación, captura, reconstrucción y análisis de las evidencias.

La Ciencia Forense recurre a la aplicación de un método científico para analizar las evidencias disponibles y formular hipótesis sobre lo ocurrido.

El trabajo de la Ciencia Forense se basa en el "Principio de Transferencia de Locard"¹³, según el cual cualquier persona u objeto que entra en la escena del crimen deja un rastro en la escena o en la propia víctima, y viceversa, es decir, también se lleva consigo algún rastro de la escena del crimen.

Por su parte, la **Informática Forense** se encarga de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional (definición propuesta por el FBI).

Un equipo de análisis forense estará constituido por expertos con los conocimientos y experiencia necesarios en el desarrollo de estas actividades. Además, sus miembros deberían contar con el entrenamiento adecuado, prestando especial atención a la puesta al día de sus conocimientos y habilidades.

Para poder realizar este trabajo resultará fundamental contar con los medios y el material especializado para las distintas técnicas del análisis forense, así como disponer de un manual detallado de los procedimientos de actuación, definiendo de forma clara y precisa

¹³ Formulado por Edmond Locard, francés fundador del Instituto de Criminalística de la Universidad de Lyon, considerado como uno de los padres de la Ciencia Forense.

todas las actividades que se realizarán en cada una de las etapas del análisis forense en sistemas informáticos.

Podemos señalar que una interesante referencia para el análisis forense en los sistemas informáticos es la guía *Best Practices for Seizing Electronic Evidence*, publicada por el Servicio Secreto de Estados Unidos y accesible en la dirección de Internet <http://info.publicintelligence.net/ussbestpractices.pdf>.



Figura 4.1. Servicio Secreto de Estados Unidos

4.2 ETAPAS EN EL ANÁLISIS FORENSE DE UN INCIDENTE INFORMÁTICO

Podemos distinguir las siguientes etapas en el análisis forense de un incidente informático:

- Identificación y captura de las evidencias.
- Preservación de las evidencias.
- Análisis de la información obtenida.
- Elaboración de un informe con las conclusiones del análisis forense.

Seguidamente se estudiarán las actividades y aspectos a tener en cuenta en cada una de estas actividades¹⁴.

¹⁴ Se puede obtener más información en el documento RFC 3227: Guidelines for Evidence Collection and Archiving.

4.2.1 Captura de las evidencias volátiles y no volátiles



Una **evidencia** es toda aquella información que podrá ser capturada y analizada posteriormente para interpretar de la forma más exacta posible el incidente de seguridad: en qué ha consistido, qué daños ha provocado, cuáles son sus consecuencias y quién pudo ser el responsable. También se pueden considerar como evidencias los campos magnéticos y los pulsos electrónicos emitidos por los equipos informáticos.

A pesar de ser intangibles, las evidencias digitales o electrónicas pueden ser admitidas como prueba en un juicio, si se ofrecen unas determinadas garantías en las distintas etapas del análisis forense, mediante el aislamiento de la escena del crimen para evitar la corrupción de ésta y de las posibles evidencias que en ella puedan hallarse.

Así mismo, es posible generar distintas copias de las evidencias digitales para facilitar su conservación y posterior análisis. La tecnología informática permitirá averiguar si alguna de estas copias ha sido modificada o falsificada, comparándola con la original.

Debemos tener en cuenta, por lo tanto, que el proceso de captura de evidencias digitales no debe alterar el escenario objeto de análisis. En la práctica esto es muy difícil de conseguir, ya que las herramientas utilizadas van a modificar la memoria del sistema informático en el que se ejecutan. De hecho, la ejecución de determinados comandos en el sistema podría alterar la información registrada en el disco: así, por ejemplo, un simple listado del contenido de un directorio va a modificar la fecha de último acceso a cada fichero.

Además, conviene utilizar herramientas grabadas en un *pendrive*, en un CD-ROM o en otro soporte de almacenamiento, que se puedan ejecutar directamente sin requerir instalación ni utilizar un entorno gráfico, para que resulten lo menos intrusivas posible y no afecten a la imagen en los discos duros del sistema.

No es recomendable emplear las propias herramientas del sistema, ya que éstas podrían haber sido manipuladas por terceros, mediante *rootkits* o troyanos. Así mismo, es necesario emplear medios forensicamente estériles para guardar una copia de las evidencias digitales, es decir, medios que no hayan tenido datos previos en ellos.

También es conveniente obtener la imagen fotográfica de todas las pantallas que muestra el sistema informático durante el proceso de captura de las evidencias digitales.

La captura de las evidencias digitales se complica aún más con las **evidencias volátiles**, entendiendo como tales a toda aquella información que se perderá al apagar un equipo informático objeto de análisis. Podemos considerar la siguiente relación de evidencias digitales volátiles:

- Volcado de la memoria global del sistema y de cada proceso: ante la dificultad de realizar un análisis en profundidad, se podrá utilizar el volcado de memoria para buscar determinadas cadenas de caracteres que puedan dar pistas sobre el incidente que ha afectado al equipo.
- Procesos y servicios en ejecución dentro del sistema: de cada proceso o servicio sería conveniente identificar el fichero ejecutable y los parámetros de ejecución, así como la cuenta de usuario bajo la que se ejecuta, los ficheros que está usando y qué otro proceso o servicio lo ha llamado (árbol de ejecución), para posteriormente poder comparar esta información con la situación estable del sistema objeto de estudio.
- Controladores (*drivers*) instalados para gestionar distintos recursos hardware del sistema.
- Información de la situación y configuración de los servicios y las tarjetas de red: configuración del protocolo TCP/IP, puertos abiertos, caché del protocolo ARP, caché de DNS, enlaces entre los protocolos y las distintas interfaces de red...
- Usuarios y grupos de usuarios activos dentro del sistema: qué sesiones se encuentran abiertas en el momento de llevar a cabo el análisis del equipo.

Tras haber capturado todas las evidencias volátiles, se procederá a obtener la información de los discos duros del sistema. Para ello, conviene apagar de forma repentina el equipo, de modo que se pueda evitar que en el proceso de apagado desde el sistema operativo se puedan borrar algunas evidencias, ya que el atacante podría haber incluido alguna rutina para eliminar evidencias de sus actuaciones dentro del sistema cuando éste fuera apagado. Seguidamente se procederá a arrancar el sistema informático procurando no alterar la información existente en los discos duros: arranque desde CD-ROM o disquete, cargando un sistema operativo como MS-DOS o Linux.

Para la obtención de la imagen de los discos del sistema informático se tendrá que realizar una duplicación de la información de los discos duros del equipo a analizar, empleando herramientas especializadas como dd, Ghost, Safeback o EnCase, que son capaces de realizar una duplicación sector a sector de cada disco duro, copiando todos los bits en el proceso.

Así, estas herramientas especializadas en la duplicación de discos duros pueden copiar los bits pertenecientes a ficheros válidos, aunque hayan sido registrados como ocultos por el sistema operativo, bits que determinan el *used space* (espacio utilizado) del disco; los bits de los ficheros marcados como eliminados y que forman parte del *free space* (espacio libre o disponible); e incluso los bits que se encuentran en las zonas marcadas como no utilizadas

dentro de cada sector (*slack space*) y en los espacios de separación entre particiones y sectores¹⁵.

4.2.2 Preservación de las evidencias digitales: cadena de custodia

A la hora de preservar las evidencias digitales será necesario contemplar una serie de tareas de tipo técnico y de medidas de carácter organizativo, teniendo en cuenta las recomendaciones de la IOCE (*International Organization on Computer Evidence*, Organización Internacional sobre Evidencias Informáticas).

Así, en primer lugar, se deberá utilizar un adecuado método de identificación, precinto, etiquetado y almacenamiento de las evidencias, considerando la posible incorporación de una firma temporal (*digital timestamp*) en cada evidencia para que quede registrado el momento en que fue capturada.

Estas evidencias digitales deberán ser preservadas de factores ambientales adversos: campos magnéticos, fuentes de radiación, etcétera. Por este motivo, se recomienda conservar los soportes informáticos donde se han registrado las evidencias digitales en bolsas de plástico antiestáticas.

Así mismo, es necesario garantizar que los datos digitales adquiridos de copias no puedan ser alterados, por lo que para su obtención se deberían emplear herramientas de generación de imágenes bit a bit, que incorporen códigos de comprobación (*checksums* o algoritmos de huella digital como SHA-1 o MD5) para facilitar la comprobación de la integridad de estos datos.

Otro aspecto de gran importancia es la documentación de todo el proceso de adquisición de evidencias, llevado a cabo por profesionales con los conocimientos adecuados. En dicha documentación se debe reflejar de forma clara y precisa la identificación de las personas que intervienen en el proceso, así como el momento y lugar en que se captura cada una de las evidencias. También se puede prever la posibilidad de realizar una grabación en vídeo por parte del equipo encargado de la captura de evidencias digitales.

Por último, resultará fundamental, sobre todo desde un punto de vista legal, el mantenimiento de la cadena de custodia de las evidencias. Con tal motivo, deben estar perfectamente definidas las obligaciones y funciones de cada uno de los miembros del equipo de análisis forense.

¹⁵ Estos espacios son empleados en ocasiones por usuarios expertos para guardar información que no resulta accesible desde el propio sistema operativo del equipo.

4.2.3 Análisis de las evidencias obtenidas

El análisis de las evidencias digitales capturadas en las etapas anteriores podría ser realizado mediante herramientas especializadas (como EnCase) que permiten analizar la imagen obtenida de los discos duros sin tener que volcarla a otro disco o unidad de almacenamiento.

La labor de análisis puede comenzar con la búsqueda de información (cadenas de caracteres alfanuméricos) en el volcado de la memoria del sistema o en las imágenes de los discos duros para localizar ficheros sospechosos, como podrían ser programas ejecutables, *scripts* o posibles troyanos.

A continuación se podrán ejecutar estos ficheros sospechosos en un entorno de pruebas totalmente controlado (por ejemplo, en una máquina virtual creada mediante la herramienta VMware con la misma configuración que el sistema que ha sufrido el incidente), para estudiar su comportamiento: interacción con el sistema, llamadas a otras aplicaciones o ficheros que intenta modificar (para esto último se pueden emplear herramientas como Filemon o Regmon en los sistemas Windows).

Así mismo, se tendrá que realizar una comprobación de la integridad en los ficheros y librerías del sistema, para detectar posibles manipulaciones (presencia de *rootkits* en el sistema). Para ello, será necesario disponer de la información sobre el estado del sistema previo al incidente (firmas digitales de los ficheros y librerías, mediante algoritmos como SHA-1 o MD5). También es posible consultar una base de datos de firmas para instalaciones típicas de distintos sistemas operativos, como la base de datos NSRL (*National Software Reference Library*) del Instituto de Estándares NIST de Estados Unidos (www.nsl.nist.gov).

El análisis de las evidencias también debe contemplar la revisión de los ficheros de configuración del sistema, donde se establecen los parámetros básicos de arranque, los servicios que se van a ejecutar y las directivas de seguridad. Por este motivo, será necesario comprobar la ejecución programada de aplicaciones, así como revisar la configuración de las aplicaciones servidoras que se ejecutaban en el sistema informático objeto de estudio (servidor WWW, servidor FTP...) y los registros de actividad de estas aplicaciones (*logs*). Se debería tener en cuenta, además, la posibilidad de obtener datos adicionales de los *logs* de otros equipos y dispositivos de la red (como, por ejemplo, los cortafuegos o los IDS) para llevar a cabo un análisis más completo de estos registros de actividad.

En relación con los ficheros incluidos en la copia del disco o discos del sistema, conviene realizar las siguientes tareas:

- Identificación de los tipos de archivos, a partir de sus extensiones o del estudio de los "números mágicos" (*Magic Numbers*), es decir, de la información contenida en la cabecera de cada fichero.

- Visualización del contenido de los ficheros gráficos.
- Estudio de las fechas de creación, cambio y último acceso a los ficheros, para detectar qué ficheros han experimentado cambios o han sido creados en las fechas próximas al incidente. Hay que tener en cuenta la fecha y hora del sistema en el momento de obtener las evidencias.
- Revisión de los permisos de acceso y ejecución de los ficheros, así como de la información sobre quiénes son sus propietarios.
- Revisión de los distintos ficheros temporales obtenidos en la imagen del sistema: memoria temporal (caché) del navegador, direcciones URL que se han tecleado en la caja de direcciones, contenido del historial del navegador, caché del protocolo ARP, archivo de paginación del sistema (*swap*), *spooler* de impresión, etcétera.

La tarea de análisis de los ficheros se puede ver dificultada por el hecho de que algunos de estos ficheros se encuentren comprimidos y/o cifrados (en este último caso resultará mucho más difícil el análisis si se ha utilizado un algoritmo de cifrado robusto).

Del mismo modo, será difícil localizar y analizar los ficheros ocultos mediante distintas técnicas dentro del sistema:

- Activación del atributo "oculto" en las propiedades de algún fichero para que no sea mostrado por el sistema operativo.
- Información y ficheros ocultos en otros ficheros mediante técnicas esteganográficas.
- Mecanismo ADS (*Alternate Data Streams*) del sistema de ficheros NTFS de Windows, utilizado para mantener información sin estructura asociada a un fichero (un icono, por ejemplo). No obstante, este mecanismo puede ser empleado por un intruso para ocultar archivos asociados a otros sin que sean detectados por el administrador del sistema.

El equipo de análisis forense deberá tener especial cuidado a la hora de localizar aquellos ficheros marcados como borrados en el disco pero que todavía no habían desaparecido de éste, es decir, los sectores que todavía no habían sido asignados a otros ficheros, por lo que formaban parte del *free space* (espacio libre del disco).

Con las herramientas adecuadas también es posible recuperar fragmentos de antiguos ficheros, además de facilitar el análisis de los datos que pudieran encontrarse en los espacios de separación entre particiones y sectores, así como en el espacio no utilizado dentro de cada sector (*slack space*).

4.3 HERRAMIENTAS DE ANÁLISIS FORENSE

Las herramientas de análisis forense permiten asistir al especialista durante el análisis de un delito informático, automatizando buena parte de las tareas descritas en los apartados anteriores para facilitar la captura, preservación y posterior análisis de las evidencias digitales.

Además, se distinguen por su capacidad para trabajar con distintos sistemas de ficheros: FAT y FAT32, NTFS de Windows, Ext2/3 de Linux, HFS de Macintosh, etcétera.

De las herramientas de análisis forense disponibles en el mercado podríamos considerar que las más populares serían EnCase, Autopsy, The Forensic Toolkit, The Sleuth Kit o The Coroner's Toolkit, entre otras.

4.4 ORGANISMOS Y MEDIOS ESPECIALIZADOS EN INFORMÁTICA FORENSE

Entre los principales organismos internacionales especializados en la Informática Forense destacan la IACIS (*International Association of Computer Investigative Specialists*) y la IOCE (*International Organization on Computer Evidence*).

La IACIS (Asociación Internacional de Especialistas en Investigación Informática) es una organización sin ánimo de lucro dedicada a la formación de los profesionales de la ley en el área del análisis informático forense (www.iacis.com).



Figura 4.2. IACIS

Por su parte, la IOCE (Organización Internacional sobre las Evidencias Informáticas) es un organismo creado en 1995 para constituir un foro en el que las agencias de ley de todo el mundo pudieran intercambiar información sobre el análisis forense informático (www.ioce.org).



Figura 4.3. IOCE

Así mismo, también podríamos citar revistas especializadas en Informática Forense, como The International Journal of Digital Evidence (www.ijde.org).

4.5 DIRECCIONES DE INTERÉS



- IACIS: <http://www.iacis.com/>.
- IOCE: <http://www.ioce.org/>.
- RFC 2350 - Expectations for Computer Security Incident Response: <http://www.ietf.org/rfc/rfc2350.txt>.
- RFC 3227 - Guidelines for Evidence Collection and Archiving: <http://www.ietf.org/rfc/rfc3227.txt>.
- Computer Forensic: <http://www.computer-forensic.com/>.
- The International Journal of Digital Evidence: <http://www.ijde.org/>.
- The Electronic Evidence Information Center, con recursos sobre análisis forense digital: <http://www.e-evidence.info/>.

CIBERTERRORISMO Y ESPIONAJE EN LAS REDES DE ORDENADORES

5.1 LA AMENAZA DEL CIBERTERRORISMO Y DE LAS GUERRAS INFORMÁTICAS

Las sociedades avanzadas tienen una dependencia cada vez mayor de los sistemas informáticos para el control de muchos procesos y actividades cotidianas: control del fluido eléctrico, de la red de abastecimientos de aguas, de las centrales de conmutación telefónicas, del tráfico aéreo, de las redes de señalización de semáforos, de los sistemas financieros, etcétera.

Por este motivo, se podría colapsar por completo el funcionamiento de un país desarrollado si se dañasen algunos de sus principales redes y sistemas informáticos. De hecho, expertos militares llevan años estudiando la posible aplicación de los ataques informáticos en los conflictos bélicos del futuro, y distintos gobiernos han decidido crear unidades especiales en sus ejércitos para responder ante posibles ataques informáticos.

Entre las posibles consecuencias de una guerra informática, podríamos citar las siguientes:

- Corte del suministro eléctrico y posible descontrol de centrales nucleares, centrales hidroeléctricas y térmicas.
- Colapso total de las redes telefónicas y los sistemas de comunicaciones.
- Desarrollo de ataques específicos contra los sistemas de comunicaciones militares.
- Caos financiero: ataques a las entidades financieras y a las bolsas, paralizando cualquier gestión y borrando o alterando los datos de todas las cuentas corrientes y otros registros de información.

- Intervención del control del tráfico aéreo y ferroviario, provocando colisiones de aviones y trenes, y dejando inoperantes estas redes de transporte.
- Ataques informáticos de todo tipo protagonizados por virus, programados y controlados de forma remota para activarse en el momento adecuado.
- Destrucción de grandes bases de datos estatales, vitales para el funcionamiento del país, como las de los cuerpos de policía, el Tesoro Público, la Sanidad, la Seguridad Social y el resto de Administraciones Públicas en general.
- Sabotajes locales en la capital y otras ciudades importantes por su población o su actividad económica, alterando el funcionamiento de los semáforos para causar choques en cadena que colapsen durante horas las principales carreteras.
- Otros sabotajes, como por ejemplo los dirigidos a las empresas más importantes y a organismos oficiales locales.
- Lanzamiento de bombas electromagnéticas para neutralizar todos los equipos electrónicos militares no protegidos y silenciar a las principales emisoras de radio y televisión.

En un estudio divulgado en agosto de 2005 por la asociación norteamericana de ingenieros IEEE-USA, titulado *United States Facing Cyber Security Crisis* y distribuido a través de su publicación *Today's Engineer*, se ponía de manifiesto la gran vulnerabilidad de muchas redes y sistemas informáticos de Estados Unidos frente a ataques terroristas y criminales. Las instalaciones afectadas y comprendidas en el estudio van desde los sistemas de control de tráfico aéreo, redes de suministro energético, sistemas financieros, así como redes de inteligencia y militares. En sus conclusiones los autores del estudio definían la actual situación como "al borde de la pérdida de control" en varias de estas instalaciones y sistemas vulnerables.

De hecho, el Departamento de Defensa de Estados Unidos, con sus cerca de 12.000 sitios informáticos y 3,5 millones de ordenadores personales repartidos por todo el mundo, constituye uno de los objetivos favoritos para miles de *hackers* y *crackers* de todo el planeta.

Precisamente uno de los casos más conocidos de un "ciberataque" contra el Pentágono fue protagonizado por el británico Gary McKinnon, quien justo después de los atentados del 11-S de 2001 logró acceder a una red de 300 ordenadores en la base de armamento naval de Earle, en Colt Neck (Nueva Jersey) y robó 950 contraseñas. El sistema informático de ese centro militar tuvo que ser apagado durante una semana. McKinnon fue perdiendo todas las apelaciones contra su extradición a Estados Unidos, y en julio de 2008 la Cámara de los Lores decidió no evitar dicha extradición, por lo que McKinnon será entregado a las autoridades de ese país, donde se enfrenta a una posible condena de 70 años de cárcel y multas de hasta 1,75 millones de dólares.

Más recientemente, la publicación de decenas de miles de documentos secretos e información confidencial por parte de la organización Wikileaks a finales del año 2010 ha venido a poner de manifiesto las deficientes medidas de seguridad informática en distintos Departamentos del Gobierno de Estados Unidos.

Por otra parte, y según se ha divulgado en algunos medios, ya se han producido cierto tipo de ataques informáticos a gran escala contra las redes y sistemas de un país. Así, por ejemplo, en octubre de 2004 Corea del Norte daba a conocer que había formado a más de medio millar de expertos informáticos capaces de lanzar una guerra virtual contra países como Estados Unidos. Estos expertos norcoreanos siguieron una formación universitaria específica durante cinco años para ser capaces de penetrar los sistemas informáticos de Corea del Sur, Estados Unidos y Japón. Parece ser que podrían estar detrás de algunos ataques realizados en el verano de 2004 contra determinadas redes y sistemas informáticos surcoreanos, pertenecientes a agencias gubernamentales, la Asamblea Nacional, empresas privadas, universidades y distintos medios informativos.

A lo largo de estos últimos años también se ha creado lo que algunos expertos en seguridad informática han dado en llamar la "*yihad* electrónica", constituida por varios miles de islamistas que se han especializado en la organización y la coordinación de cibercampañas contra los sitios Web israelíes, estadounidenses, católicos o daneses (en este último caso a raíz de la publicación de las caricaturas de Mahoma en ese país).

En abril de 2007 se daba a conocer que un grupo de piratas informáticos chinos habían logrado acceder a los ordenadores personales de varios oficiales de Taiwán y copiar información secreta sobre las maniobras anuales Han Kuang, que simulan la defensa de la isla frente a un ataque chino. Por este motivo, para poder afrontar las nuevas amenazas del ciberterrorismo y las guerras cibernéticas, Taiwán decidió crear un batallón de mujeres especializado en la guerra electrónica e informática, integrado por 100 oficiales y soldados, según informó el Ministerio de Defensa de la isla.

También Estonia anunciaba en mayo de 2007 su intención de crear un centro para proteger las instituciones oficiales de los ataques informáticos, después de que a finales de abril de ese año varios ataques informáticos externos consiguieran paralizar la labor de varios servicios públicos de ese país báltico, así como de algunas entidades financieras y medios de comunicación.

En junio de 2007 un grupo de piratas informáticos checos lograba interrumpir un programa de la cadena de televisión Ceska Televize sobre las montañas de Krkonose, y mostraron los efectos devastadores de la explosión de una bomba atómica en la zona, lo que atemorizó a muchos telespectadores.

En noviembre de 2007 el "ciberespionaje" chino era descrito como "la mayor amenaza" para la tecnología estadounidense por una comisión del Congreso de Estados Unidos, que hacía un llamamiento para incrementar la protección de los secretos industriales y de las redes informáticas. El Reino Unido también daba la voz de alarma ese mismo mes al informar en un estudio titulado "Virtual Criminology" que las redes informáticas del Gobierno

y de la Defensa del Reino Unido estaban siendo sometidas a ataques sistemáticos por parte de China y otros países.

En agosto de 2008 un fallo informático en la Agencia Federal de Aviación (FAA) de Estados Unidos provocaba el colapso del tráfico aéreo en todo el país, tal y como reflejaban en directo las noticias de la CNN.



Figura 5.1. Colapso del tráfico aéreo en Estados Unidos por un fallo informático

En marzo de 2009 una investigación llevada a cabo por la Universidad de Toronto revelaba que una red de espionaje informático había logrado penetrar en ordenadores de Gobiernos, embajadas, organizaciones de defensa de los derechos humanos y medios de comunicación, entre otras instituciones, en 103 países.

También en marzo de 2009 la Comisión Europea presentaba un comunicado en el que alertaba a los Estados miembros de la Unión Europea sobre la necesidad de proteger las infraestructuras de información y comunicación. Según dicho informe, la perturbación de estos sistemas podría tener graves incidencias en funciones vitales de la sociedad, y citaba como ejemplos dos casos recientes: el ataque cibernético de gran envergadura que sufrió Estonia en 2007 y la ruptura de cables transcontinentales en 2008.

Posteriormente, un estudio publicado en noviembre de 2009 y titulado "*Virtually Here: The Age of Cyber Warfare*", realizado por la empresa McAfee, señalaba que algunos expertos en seguridad informática han venido detectando movimientos encaminados a la recogida de más información en Internet y a la creación de mejores capacidades para realizar posibles ataques cibernéticos.

De hecho, en julio de 2010 el Ejército de China anunciaba la puesta en marcha de su primera base militar cibernética para combatir los ataques y amenazas informáticas, según revelaba el periódico oficial en inglés *Global Times*.

En agosto de 2010 el subsecretario de Defensa de Estados Unidos, William Lynn, reconocía en una entrevista en la revista *Foreign Affairs* que la infiltración más grave en ordenadores militares de ese país había sido causada por una tarjeta de memoria insertada en un ordenador portátil en Oriente Medio en 2008. Este alto cargo del Pentágono señalaba en dicha entrevista que un "código malicioso, colocado en el ordenador por una agencia de inteligencia extranjera, descargó su programa en una red administrada por el Mando Central militar de Estados Unidos". Este Mando Central, que tiene su sede en Tampa (Florida), supervisa las operaciones militares desde el Mar Rojo al Golfo y el sur de Asia hasta Pakistán.

Posteriormente, el Ejército de Estados Unidos anunciaba en diciembre de 2010 la creación de un nuevo Comando Cibernético, que estaría constituido por unos 30.000 soldados y expertos en seguridad informática que puedan afrontar ataques por Internet.

Pero los Gobiernos no solo deben afrontar las amenazas del ciberterrorismo y las guerras cibernéticas, sino que también deben mejorar la seguridad física y lógica de sus sistemas y bases de datos, para evitar que por un descuido puedan extraviarse decenas de miles de registros con datos de los ciudadanos.

Así, por ejemplo, en noviembre de 2007 se daba a conocer el caso de que una de las agencias del Ministerio de Hacienda del Reino Unido había extraviado dos discos duros con datos de 25 millones de ciudadanos, que contenían nombres y apellidos, direcciones, fechas de nacimiento, de padres e hijos menores de 16 años, los números de la tarjeta de la Seguridad Social y también, en el caso de diez millones de personas, de sus cuentas bancarias. Unas semanas más tarde, en diciembre de 2007, la Ministra de Transportes de este mismo país informaba del extravío de un disco duro que contenía los datos de más de tres millones de solicitudes para permisos de conducir, incluyendo los nombres, los domicilios, las direcciones de correo electrónico y los números de teléfono personales de solicitantes para obtener el permiso de conducir en el Reino Unido entre septiembre de 2004 y abril de 2007.

Al poco de conocerse estas dos pérdidas masivas de datos de ciudadanos británicos, el diario *The Times* demostró que existía un mercado de compraventa de datos personales a través de Internet, lo que puso aún más en entredicho la seguridad en el tratamiento de este tipo de información sensible en el Reino Unido.

5.2 CONSECUENCIAS DE LOS FALLOS Y ATAQUES EN LAS EMPRESAS

La mayoría de las empresas y organizaciones de nuestro entorno también podrían ser vulnerables a ataques informáticos llevados a cabo contra sus propios recursos e intereses, en una especie de "guerra informática" a pequeña escala. De hecho, algunas empresas ya han sufrido varios casos de difusión de virus y ataques de denegación de servicio realizados por expertos informáticos que habían sido contratados por algún competidor.

Los avances de las redes y servicios de telecomunicación han facilitado el desarrollo del teletrabajo en algunos sectores y tipos de organizaciones. Además, los empleados que se tienen que desplazar con frecuencia (por ejemplo, los comerciales que constituyen la fuerza de ventas de una empresa) también dependen hoy en día de las conexiones a los recursos informáticos centrales de su organización para poder realizar su trabajo. Todos estos empleados se verían imposibilitados para trabajar con normalidad si se viera interrumpido el funcionamiento de la red y los servicios informáticos de su empresa.

Además, los fallos en los sistemas informáticos pueden tener importantes consecuencias económicas para las empresas. Así, por ejemplo, un fallo informático provocó en septiembre de 2004 varias decenas de cancelaciones e innumerables retrasos en vuelos de Lufthansa en todo el mundo, afectando a miles de pasajeros. El sistema mundial informático de Lufthansa, que facilita la facturación de los pasajeros, se colapsó a las 6:22 horas del jueves 23 de septiembre de 2004, lo que obligó a rellenar a mano las tarjetas de embarque. Los técnicos pudieron solucionar parcialmente el problema seis horas después, aunque no lograron volver a ponerlo en funcionamiento completamente, porque la operación hubiera llevado unas cuatro o cinco horas y habría provocado nuevas demoras en los servicios.

Otro ejemplo similar, de entre los muchos que podríamos seguir citando, tuvo lugar el 24 de agosto de 2005, cuando un fallo informático en un centro de control de tráfico aéreo de Londres provocó grandes retrasos en los vuelos de entrada y salida del Reino Unido, afectando a miles de pasajeros y obligando a cancelar decenas de servicios. La avería, que se produjo a primera hora de la mañana, afectó al sistema de procesamiento de vuelos del Centro Nacional de Servicios de Tráfico Aéreo (NATS), con sede en West Drayton, en el oeste de Londres. Los técnicos tardaron unos veinte minutos en subsanar el fallo, pero cuando lo lograron, la avería ya había trastocado los planes de cientos de aviones en todo el país.

Con estos dos ejemplos se pone de manifiesto cómo una pequeña interrupción o determinadas anomalías en el servicio informático de una empresa puede provocar daños muy importantes a la organización, por lo que nos podríamos imaginar cuáles serían las consecuencias si el servicio informático se viera interrumpido durante varios días debido a un ataque o sabotaje a gran escala.

Por otra parte, numerosos estudios publicados sobre esta cuestión reflejan el elevado porcentaje de empresas que han sufrido ataques y fallos informáticos en estos últimos años. Así, por ejemplo, un estudio realizado en Estados Unidos por el *Computer Security Institute* (Instituto de Seguridad Informática) en colaboración con el FBI en el año 2000 reflejó que el 90% de las organizaciones encuestadas, entre las que se incluían grandes empresas, entidades financieras, universidades, hospitales y agencias gubernamentales, habían detectado agujeros de seguridad en sus sistemas informáticos durante el año 1999, situación que había provocado incidentes de seguridad de una cierta importancia en muchas de ellas.

Un estudio de la empresa especializada en seguridad informática McAfee publicado en febrero de 2009 señalaba que el robo de datos y las infracciones cometidas en los delitos informáticos podían tener para las empresas un coste de un billón de dólares a nivel mundial, debido a la pérdida de propiedad intelectual y a los gastos ocasionados por la reparación de los daños sufridos.

5.3 EL ESPIONAJE EN LAS REDES DE ORDENADORES

5.3.1 El polémico chip “Clipper” y el papel de la NSA

A principios de los años noventa surgía la polémica en Estados Unidos por la intención del gobierno de ese país de intervenir en todo tipo de comunicaciones a través de redes telefónicas y de ordenadores. Así, en 1994 la Administración Clinton aprobó el *Escrowed Encryption Standard*, que contemplaba el desarrollo de productos con la característica de *key-escrow*, para facilitar el descifrado de las comunicaciones por parte de organismos del gobierno (como la CIA o el FBI).

A su vez, la NSA (Agencia de Seguridad Nacional) diseñó el polémico chip “Clipper” para el cifrado de comunicaciones de voz, que cumplía con estas especificaciones (al facilitar el descifrado mediante una clave que estaría en poder del gobierno de Estados Unidos). De este modo, el gobierno podría interceptar todas las comunicaciones de sus ciudadanos, al estilo de un “Gran Hermano” Orwelliano.

La NSA (*National Security Agency*, Agencia Nacional de Seguridad de Estados Unidos) es un organismo envuelto en un halo de misterio y de polémica. Fue creada en 1952 por el presidente Harry Truman, como una agencia integrada en el Departamento de Defensa y durante muchos años su existencia se mantuvo en secreto (de ahí los apodos de *No Such Agency* o *Never Say Anything*). De hecho, la mayor parte de la información sobre esta agencia se encuentra clasificada.



Figura 5.2. NSA

La NSA se dedica fundamentalmente al espionaje de todas las comunicaciones que pudieran resultar de interés para los Estados Unidos. Así mismo, la NSA es uno de los principales centros de investigación en criptografía y criptoanálisis del mundo. De hecho, se considera que esta organización es el mayor empleador de matemáticos del mundo, así como uno de los mayores inversores en hardware.

La NSA utiliza su poder e influencias para restringir la disponibilidad pública de los últimos avances y técnicas criptográficas.

5.3.2 ECHELON

ECHELON es una red de espionaje electrónico creada en los años cincuenta por la Agencia Nacional de Seguridad norteamericana (NSA), contando con la colaboración de Gran Bretaña, Australia y Nueva Zelanda. ECHELON es un sistema militar de espionaje de todo tipo de comunicaciones electromagnéticas, con capacidad para interceptar llamadas de teléfono (incluso a teléfonos móviles con el sistema GSM, que emplea algoritmos de cifrado), transmisiones por Internet, envíos de fax y télex, transmisión de datos y de llamadas vía satélite, etcétera.

Los principales centros de interceptación de comunicaciones de esta red se encuentran situados en Menwith Hill (Gran Bretaña), Bad Aibling (base militar en Alemania), Sugar Grove (Virginia, Estados Unidos), Sabana Seca (Puerto Rico), Leitrim (Canadá), Shoal Bay (Australia) y Waihopai (Nueva Zelanda).

La capacidad de captación de estas estaciones de radiocomunicaciones se ha venido incrementando en estos últimos años. Así, por ejemplo, la base de Sugar Grove, situada en una remota área de las montañas Shenandoah (en Virginia, Estados Unidos), disponía en 1990 de solo cuatro antenas de satélite, mientras que en noviembre de 1998 este número ya había aumentado hasta un total de nueve, de las cuales seis se encontraban orientadas a las comunicaciones europeas y atlánticas.

Esta red de espionaje es capaz de capturar grandes cantidades de información y de filtrarla para detectar las transmisiones de otros gobiernos, militares, disidentes, activistas o grupos terroristas. Para ello, cuenta con varios superordenadores capaces de almacenar todos los datos posibles sobre determinados objetivos, que se pueden definir a partir de un nombre, una dirección, un número telefónico, unas determinadas palabras clave u otros criterios seleccionados. Cuando un satélite de la red detecta una comunicación que pueda ser interesante, se captura el mensaje y se envía a los centros especializados de la NSA para su posterior análisis.

La existencia de esta red fue divulgada en los años setenta por un grupo de investigadores británicos. En estos últimos años saltó la polémica al hacerse público que los servicios secretos también estaban interceptando de forma indiscriminada las comunicaciones de las empresas y de toda la ciudadanía en general. De hecho, se ha utilizado para el

espionaje industrial y comercial por parte de Estados Unidos, con la colaboración del Reino Unido.

El Parlamento Europeo creó en julio de 2000 la Comisión Echelon tras la publicación de un libro sobre esta red de espionaje escrito por el físico escocés Duncan Campbell. El informe de esta Comisión fue presentado en julio de 2001 y en él se confirma la existencia de la red Echelon y su implicación en el espionaje a distintos gobiernos, organizaciones y empresas europeas. Este informe causó un profundo malestar entre los eurodiputados de varios Estados miembros, ya que en él se exponían algunos casos en los que empresas europeas habían perdido contratos en otros países, al filtrarse el contenido de sus propuestas a compañías norteamericanas que competían por los mismos contratos.

Algunos medios de comunicación revelaron entonces que en mayo de 1977, la NSA, la CIA y el Departamento de Comercio norteamericano habían creado una estructura secreta, la *Office of Intelligence Liaison*, que enviaba automáticamente al Departamento de Comercio de Estados Unidos toda información que pudiera resultar de interés para las empresas norteamericanas activas en el extranjero, como ayuda a sus operaciones y contratos internacionales.

Así, podemos citar varios casos concretos de espionaje que han salido posteriormente a la luz a través de distintos medios de comunicación:

- La compañía francesa Thompson CSF perdió en 1994 un contrato de 220.000 millones de pesetas en Brasil para el desarrollo de un sistema de supervisión por satélite de la selva amazónica. Este proyecto fue finalmente concedido a la empresa norteamericana Raytheon.
- En 1995 el consorcio europeo Airbus perdió en el último momento un contrato de más de 800.000 millones de pesetas que iba a firmar con el gobierno de Arabia Saudí y que finalmente fue concedido a Boeing, gracias a la interceptación de las llamadas telefónicas y los faxes enviados por los directivos de Airbus.
- La interceptación y escucha de transmisiones de Greenpeace por parte de Estados Unidos durante su campaña de protesta contra las pruebas nucleares francesas en el Atolón de Mururoa en 1995.
- El espionaje de las comunicaciones de la delegación francesa durante las reuniones para alcanzar los acuerdos de liberalización comercial de la Ronda de Uruguay, las negociaciones del consorcio europeo Panavia para vender el avión de combate Tornado a los países de Oriente Medio, o la Conferencia Económica Asia-Pacífico de 1997.
- También se han dado otros casos de espionaje a la industria automovilista japonesa.

También se ha comentado que la red ECHELON pudo ser utilizada para facilitar la localización de Dzokhan Dudayev, terrorista checheno que fue asesinado mediante un misil teledirigido por los rusos mientras hablaba desde su teléfono móvil.

Se puede obtener más información sobre la red ECHELON consultando la página web del físico británico Duncan Campbell (<http://duncan.gn.apc.org/>).

5.3.3 ENFOPOL (Enforcement Police)

El proyecto Enfopol nació en Bruselas en 1995, como una serie de requisitos técnicos para que los operadores de telecomunicaciones adecuasen sus sistemas para facilitar la interceptación de las comunicaciones de sus usuarios, incluyendo los nuevos servicios de Internet, en el ámbito de Europa y otros países, ante eventuales demandas de pinchazos policiales autorizados judicialmente. Posteriormente, en el año 1999 el Parlamento Europeo aprobaba la Resolución Enfopol.

De este modo, los Servicios de Seguridad Estatales podrían tener acceso al contenido de las comunicaciones de los usuarios y a la información sobre el tráfico cursado tanto en Internet, como en los servicios de llamadas móviles terrestres, los servicios de llamadas de larga distancia e internacionales, la transmisión de datos o los mensajes de correo de voz.

Entre otros datos, los operadores deberían facilitar los números de teléfono, tanto de los que realizan la llamada como de los que la reciben; direcciones IP; direcciones de correo electrónico; identificadores y contraseñas de acceso; número de cuenta desde la que se paga el servicio; etcétera.

En España, la Ley de Servicios de la Sociedad de la Información contempla la obligación de retención de datos de tráfico. En virtud de lo dispuesto en esta Ley, los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes y los prestadores de servicios de alojamiento de datos tienen la obligación de retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información (conexión a Internet, hospedaje de páginas web...), por un período de tiempo de hasta 12 meses.

Los operadores de redes y servicios y los proveedores de acceso deberán conservar únicamente los datos necesarios para facilitar la localización de los equipos terminales (es decir, se tiene que registrar la dirección IP asignada a cada usuario en una conexión a Internet, pero no qué páginas web o servicios de Internet ha utilizado).

A raíz de los atentados de Madrid (11 de marzo de 2004) y, especialmente, de Londres (7 de julio de 2005) distintos gobiernos europeos liderados por el británico se han mostrado partidarios de facilitar el acceso de la Policía a las llamadas telefónicas y los correos

electrónicos de los ciudadanos, por lo que en la actualidad se están estudiando varios paquetes de medidas sobre esta cuestión.

Así, por ejemplo, el Reino Unido anunciaba en agosto de 2008 una propuesta para controlar los mensajes de correo electrónico, el uso de Internet, los mensajes de móvil SMS y las llamadas telefónicas de los ciudadanos británicos. De hecho, en ese momento ya era obligatorio en el Reino Unido que las grandes empresas de telecomunicaciones, como BT, Orange u O2 mantuvieran un registro del tráfico de las llamadas de cada ciudadano desde teléfonos fijos y móviles.

Por su parte, Francia también anunciaba en septiembre de 2008 la creación de la base de datos denominada "Edvige" (Explotación Documental y Valorización de la Información General), registrando detalles como los rasgos físicos, el origen étnico, los datos fiscales y financieros, así como el número de teléfono de cientos de miles de ciudadanos.

En Alemania la Cámara Alta del Parlamento aprobaba en diciembre de 2008 una controvertida ley que permite a la policía criminal (la Oficina Federal de Investigaciones Criminales, conocida por sus siglas BKA) actuar en materia antiterrorista fuera de las fronteras alemanas e instalar programas espía en los ordenadores privados de ciudadanos sospechosos de terrorismo.

5.3.4 CARNIVORE

CARNIVORE es un polémico programa desarrollado en el año 2000 por el FBI en Estados Unidos para interceptar y leer mensajes de correo electrónico y otras comunicaciones entre presuntos criminales, espías y terroristas, contando para ello con la colaboración de los operadores de redes de telecomunicaciones.

Desde entonces este costoso programa (el proyecto tuvo un coste superior a los 170 millones de dólares) fue utilizado de forma importante a partir de los atentados del 11-S en Estados Unidos.

Sin embargo, en enero de 2005 el FBI anunciaba su intención de desechar este programa y reemplazarlo por otras soluciones comerciales convencionales que resultaban mucho más económicas.

Por otra parte, en noviembre de 2004 se daba a conocer la noticia de que la Agencia de Inteligencia de Estados Unidos (CIA) había aportado fondos para el desarrollo de nuevos métodos de escucha automática y no detectable de servicios de *chat* en Internet. En la actualidad la investigación también se centra en la interceptación de las conversaciones mediante telefonía IP (transmisión de voz a través de la propia Internet).

5.4 DIRECCIONES DE INTERÉS



- NSA: <http://www.nsa.gov/>.
- Página personal del físico Duncan Campbell, autor de un libro sobre la red Echelon: <http://duncan.gn.apc.org/>.
- Información adicional sobre la red Echelon:
<http://www.fas.org/irp/program/process/echelon.htm>.
- Información sobre el programa Carnivore del FBI ofrecida por el EPIC (Electronic Privacy Information Center):
<http://www.epic.org/privacy/carnivore/>.

BIBLIOGRAFÍA

- Alberts, C. (2002): *Managing Information Security Risks: The OCTAVE Approach*, Addison Wesley.
- Barman, S. (2001): *Writing Information Security Policies*, New Riders Publishing.
- Casey, E. (2004): *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Academic Press.
- Chirillo, J. (2001): *Hack Attacks Revealed: A Complete Reference*, John Wiley & Sons.
- Cole, E. (2001): *Hackers Beware*, New Riders.
- Cresson, C. (2002): *Information Security Policies Made Easy*, PentaSafe Security Technologies.
- Erickson, J. (2003): *Hacking: The Art of Exploitation*, No Starch Press.
- Hare, C.; Siyan, K. (1996): *Internet Firewalls and Network Security - 2nd Edition*, New Riders.
- Hoglund, G.; Butler, J. (2005): *Rootkits: Subverting the Windows Kernel*, Addison Wesley.
- Kaspersky, K. (2003): *Hacker Disassembling Uncovered*, A-LIST Publishing.

- Kahn, D. (1996): *The Code Breakers*, Scribner.
- Klevinsky, T. J.; Laliberte, S.; Gupta, A. (2002): *Hack I.T.: Security Through Penetration Testing*, Addison Wesley.
- Long, J. (2005): *Google Hacking for Penetration Testers*, Syngress.
- McClure, S.; Shah, S.(2002): *Web Hacking: Attacks and Defense*, Addison Wesley.
- Mirkovic, J.; Dietrich, S.; Dittrich, D.; Reiher, P. (2004): *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall.
- Mitnick, K.; Simon, W. (2005): *The Art of Intrusion*, John Wiley & Sons.
- Pipkin, D. (2002): *Halting the Hacker: A Practical Guide To Computer Security*, Prentice Hall.
- Prasad, A.; Prasad, N. (2005): *802.11 WLANs and IP Networking Security*, Artech House.
- Russell, R. (2000): *Hack Proofing Your Network*, Syngress.
- Russell, R. (2003): *Stealing the Network: How to Own the Box*, Syngress.
- Scambray, J.; McClure, S.; Kurtz, G. (2001): *Hacking Exposed: Network Security Secrets & Solutions - 2nd Edition*, Osborne/McGraw-Hill.
- Scambray, J.; Shema, M. (2002): *Hacking Exposed Web Applications*, Osborne/McGraw-Hill.
- Schneier, B. (2000): *Secrets & Lies. Digital Security in a Networked World*, John Wiley & Sons.
- Shema, M. (2002): *Anti-Hacker Tool Kit*, Osborne/McGraw-Hill.
- Sinchak, S. (2004): *Hacking Windows XP*, John Wiley & Sons.
- Skoudis, E.; Zeltser, L. (2003): *Malware: Fighting Malicious Code*, Prentice Hall.

- Szor, P. (2005): *The Art Of Computer Virus Research And Defense*, Addison Wesley.
- Sutton, R. (2002): *Secure Communications: Applications and Management*, John Wiley & Sons.
- Warren, H. (2002): *Hacker's Delight*, Addison Wesley.
- Young, M. (2003): *Internet Security: Cryptographic Principles, Algorithms and Protocols*, John Wiley & Sons.

ÍNDICE ALFABÉTICO

A

Acciones legales	77
Actividades de reconocimiento de sistemas	24
Address Resolution Protocol	32
Agencia Nacional de Seguridad	111
Agujeros de seguridad	38
Alternate Data Streams	101
Análisis "post-mortem"	84
Análisis de las evidencias digitales	100
Análisis de un incidente de seguridad	75
Análisis forense	95
Analizadores de protocolos	68
Anti-sniffers	68
ARP	67
ARP spoofing	61
Arquitecturas de IDS	62
Ataque smurf	47
Ataques activos	24
Ataques de denegación de servicio	109
Ataques de denegación de servicio distribuidos	48
Ataques de diccionario	43
Ataques de fuerza bruta	43
Ataques de modificación del tráfico	37
Ataques de repetición	31
Ataques de suplantación de la identidad	32
Ataques del tipo "salami"	43
Ataques informáticos	24, 105
Ataques pasivos	24

Auto-rooters	23
--------------------	----

B

Backdoors	38
Backdoors kits	23
Balanceo de carga	86
Bomba UDP	47
Bombas electromagnéticas	106
Bombas lógicas	18, 39
Botnets	49

C

Captura de evidencias	96
Carnivore	115
Casos de espionaje	113
Centro alternativo	85
Centro alternativo "caliente"	87
Centro alternativo "frío"	87
Centro de alerta temprana	91
Centro de back-up	86
Centro de reserva	85
CERT	82, 89
Chantaje y extorsión on-line	44
Checksums	99
CIDF	62
Ciencia forense	95
CIF	54
Click kiddies	17

Clickjacking	44
Clipper.....	111
Clusters de servidores.....	86
Código malicioso	39
Códigos de comprobación	99
Common Intrusion Detection Framework ...	62
Common Log Format	54
Comprobación de la integridad	100
Comunicación con terceros	79
Conexión no autorizada.....	38
Connection flood	47
Consecuencias de ataques e incidentes.....	38
Consecuencias de un incidente	81
Consecuencias económicas	110
Contención de un incidente	76
Contenidos ilegales	39
Content Addressable Memory	31
Continuidad del negocio	85
Control del tráfico.....	37
Cookies.....	40
Crackers	16
Creadores de virus	17
Criptoanálisis.....	43
Cross-site scripting	40
CSIRT	72
CSRC.....	90

D

Data center	88
DDOS	48
Denegación de servicio.....	33, 45
Dependencia de los sistemas informáticos	105
Detección de un mal uso	58
Detección de un uso anómalo.....	58
Dialers.....	49
DIDS	60
Difusión de virus	109
Digital timestamp	99
Disponibilidad de los recursos	85
Distributed intrusion detection system.....	91
DNS	33
DNS seguro	35
DNS spoofing.....	33, 60
DSEC.....	35
Documentación de un incidente	80
DOS	33, 45
Dynamic Trunk Protocol	31

E

Eavesdropping.....	31
Echelon	112
ELF	54
Encaminamiento fuente	37
Enfopol.....	114
Enmascaramiento	32
Envenenamiento de la caché	33
Envenenamiento de las tablas ARP	61
Equipo de respuesta a emergencias informáticas.....	89
Equipo de respuesta a incidentes de seguridad informática.....	72
Erradicación	77
Escaneo de puertos	25
Escaneo de vulnerabilidades	73
Escáneres de puertos	23
Escrowed Encryption Standard	111
Espionaje.....	111
Estafas financieras	43
Etapas en el análisis forense.....	96
Evaluación del coste	81
Evidencias digitales	97
Evidencias volátiles	97
Exempleados.....	18
Exploits	22, 23, 30, 38
Extended Log Format	54
Extorsiones	44

F

Fallos en los sistemas informáticos	110
Falsificación de DNS	33
Falsos negativos	58
Falsos positivos	58, 74
Fases de un ataque informático.....	22
Ficheros ocultos.....	101
Finger	67
First.....	90
Fisgonas	18
Fraggle.....	61
Free space	98, 101

G

Generadores de virus	24
----------------------------	----

Guerra informática	105
Guía de actuación.....	72
Guía de procedimientos.....	73
Gusanos.....	39

H

Hackers	15
Hacking tools.....	23
Herramientas de análisis forense	102
Hijacking.....	32
Honeynet	63
Honeynet virtual	66
Honeypot	63
Honeywall	64
Host IDS	59

I

IACIS	102
Identificación del atacante	77
IDS	57, 73
IDS distribuidos	60
IDWG	62
Incident object description and exchange format requirements	80
Incidente de seguridad.....	53
Indicadores de un incidente	73
Informática forense	95, 102
Ingeniería social.....	37
Insiders	18
Integridad de los ficheros	59
Integrity check.....	60
Interceptación de comunicaciones.....	112
Interceptación de mensajes	30
Interceptación de mensajes de correo	115
Interceptación de tráfico.....	31
Internet Health Monitoring.....	92
Intrusion Alert Protocol	63
Intrusion Detection Exchange Format.....	62
Intrusion Detection Message Exchange Format	63
Intrusion Detection Systems	57
Intrusion Detection Working Group	62
Intrusion Prevention System	63
Intrusos	15
Intrusos remunerados.....	18

Investigación sobre las causas de un incidente	81
Inyección de código SQL	41
IOCE	99, 102
IP spoofing	32, 60, 78
IPconfig.....	67
IPS	63

K

Kevin mitnick	20
Key-escrow	111
Keyloggers.....	36
Know your enemy	64

L

Lamers.....	17
Land attack.....	46
Logs.....	22, 53, 73, 83

M

Mac flooding.....	31
Magic numbers	100
Mail bombing	45
Mail relaying	39
Malware	39
Man-in-the-middle	32
Marcadores telefónicos	49
Masquerading.....	36
Matriz de diagnóstico.....	75
Mice.....	21
Mirror.....	87
Mirrored ports	59
Modem	38
Modo promiscuo	68
Módulo de respuesta	57
Motivaciones de los atacantes.....	21
Motor de análisis.....	57

N

NbtStat	67
Net Flood.....	47
NetStat	67

Network IDS	60
Network taps	68
Network time protocol	54
NSA	111
NSLookup	67
Números mágicos	100

O

Obligación legal de notificación	84
Office of Intelligence Liaison	113
Operaciones fraudulentas	43
Organismos especializados	89
Outsiders	18

P

Paquetes "out-of-band"	46
Password crackers	23
Personal interno	18
Pharming	43
Phishing	33, 43
Phreakers	16
Ping	67
Ping de la muerte	46
Piratas informáticos	17
Plan de actuación	82
Plan de comunicación con los medios	80
Plan de contingencias	85
Plan de recuperación	85
Plan de respuesta a incidentes	71
Precursores de un ataque	73
Preservación de las evidencias digitales	99
Priorización de las actividades	76
Privacidad	54
Programas dañinos	17
Programas privilegiados	60
Propagación de códigos dañinos	40
Propiedad intelectual	17
Pruebas de intrusión	69
Puertas traseras	23, 38, 77

R

Ransom-ware	44
Reconocimiento de versiones	25
Recovery Point Objective	88

Recovery time objective	88
Recuperación	77
Recuperación de la actividad	84
Recuperación de los datos	72
Red de espionaje	112
Red señuelo	63
Reflector attack	45
Registro de eventos	54
Registro de nombres de dominio	35
Registros de actividad	53, 59, 100
Replay attacks	31
Respuestas activas	58
Respuestas pasivas	58
Retención de datos de tráfico	114
Revisión de las políticas de seguridad	82
Rootkits	23, 38, 77

S

Script	40
Script kiddies	17
Secuestro de archivos	44
Secuestro de sesiones	32
Seguridad de los sistemas criptográficos ...	43
Sentencia SQL	42
Service Level Agreement	88
Servidor centralizado de "logs"	54
SetuID	60
Sistemas de detección de intrusiones ...	57, 73
Slack space	99, 101
Smtip spoofing	36
Sniffers	16, 23, 31, 68
SNMP	55
Snoopers	37
Snooping	37
Snork udp	47
Snort	59, 61
Source routing	37
Spammers	16
Spanning ports	59
Spoofing	24
SQL	41
Supernuke	46
Suplantación de direcciones ip	24
Switch	59
Switches	31
Syn flood	46
Syn flooding	61
Syslog	54

T

Tablas de enrutamiento.....	37
Teardrop	46
Telnet.....	67
Tempest	31
Terena.....	80
Test de penetración	69
Three-way handshake	46
Tracert	67
Triángulo de la intrusión.....	22
Tribe flood net	49
Troyanos.....	39

U

Us-cert	90
Used space.....	98

V

Valoración de los daños	76
Virus.....	39
Visor de sucesos	55
VLan	31
VMWare	66
Vulnerabilidades	30, 60

W

Wardialers	38
Wardialing	38
Website vandalism	39
Whois.....	67
Wikileaks	107
Winnuke	46
Wrappers.....	68

MÓDULO FORMATIVO 0488_3

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

La presente obra está dirigida a los estudiantes de los nuevos Certificados de Profesionalidad de la familia profesional **Informática y Comunicaciones**, en concreto al Módulo Formativo **Gestión de Incidentes de Seguridad Informática**.

Este libro pretende aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Planificar e implantar los sistemas de detección de intrusos.
- Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.
- Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

Para ello, el libro comienza analizando las principales amenazas y tipos de ataques a los sistemas informáticos. A continuación, se aborda el estudio de la gestión de incidentes de seguridad y cuáles son los principales aspectos a tener en cuenta en la respuesta ante incidentes de seguridad y en la definición de planes de continuidad del negocio.

Las principales características y procedimientos incluidos en el análisis forense informático ocupan otro de los capítulos de la obra y, por último, se revisan cuestiones relacionadas con el ciberterrorismo y el espionaje en las redes y sistemas informáticos.

FAMILIA PROFESIONAL: Informática y Comunicaciones

CERTIFICADO DE PROFESIONALIDAD EN EL QUE SE INCLUYE:

- Seguridad Informática

