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.

Capítulo

1

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*.

1.1.2 *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…

1.1.3 *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.

1.1.4 *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.

1.1.5 *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.

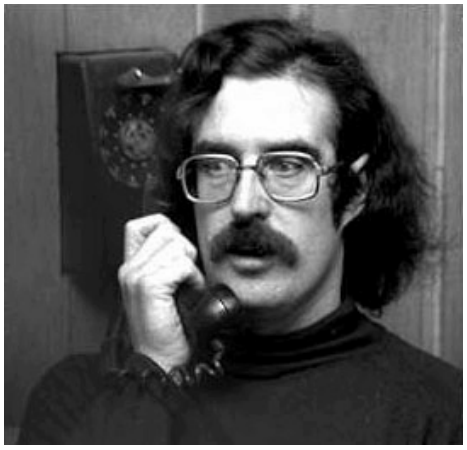

Figura 1.1. John Draper

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.

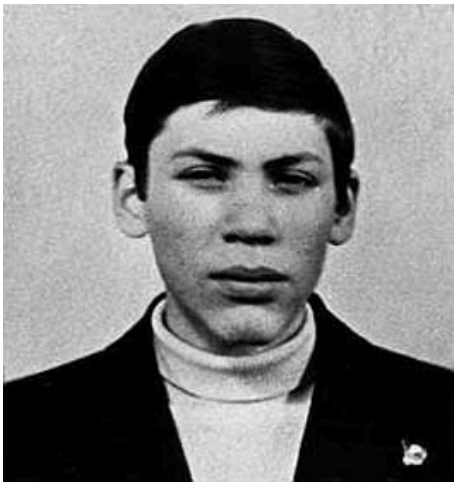

Figura 1.2. Vladimir Levin

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:

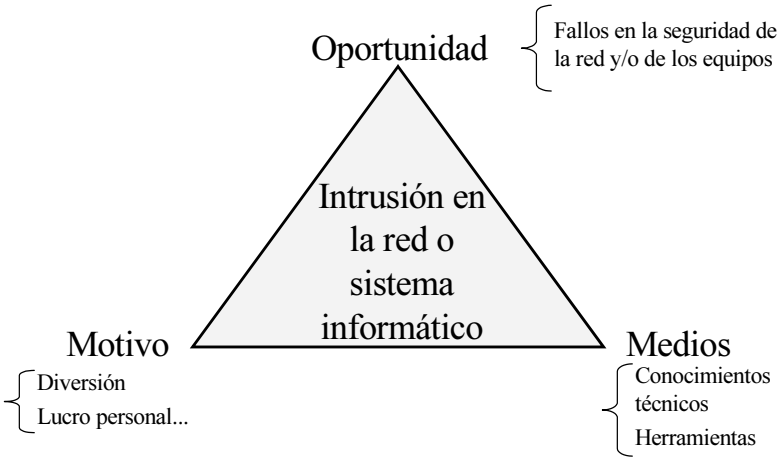

Figura 1.5. El "Triángulo de la Intrusión"

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.

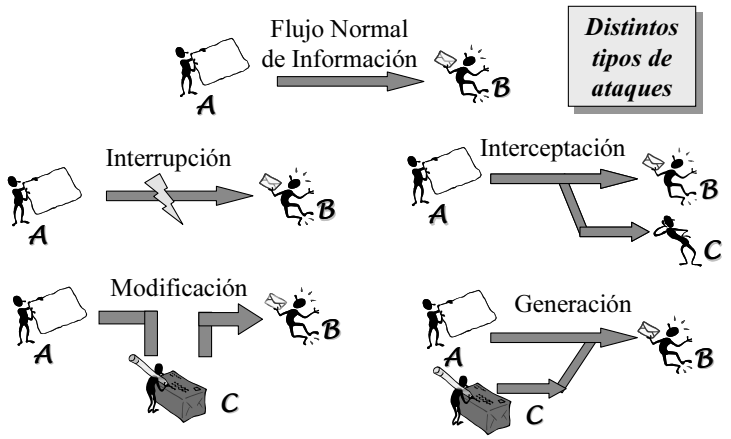

Figura 1.6. Distintos tipos de ataques en una red de ordenadores

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 Caribean Internet Addresses Registry): *http://lacnic.net*.

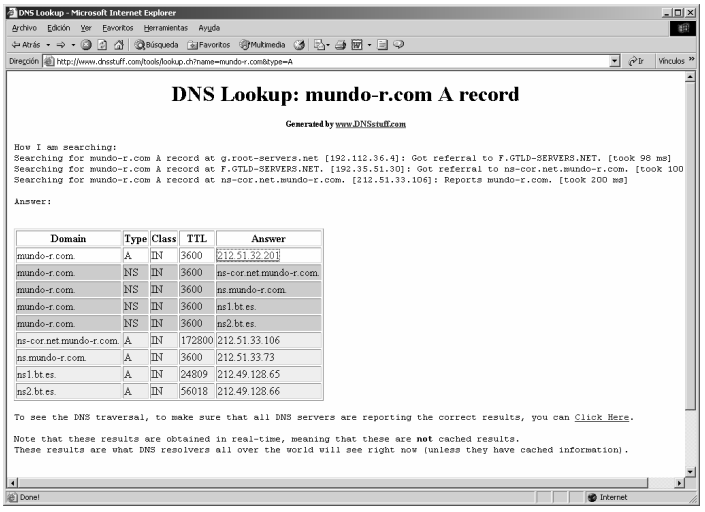

Figura 1.7. Consulta de la ficha de información sobre un determinado nombre de dominio, perteneciente en este caso a un operador de telecomunicaciones

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.

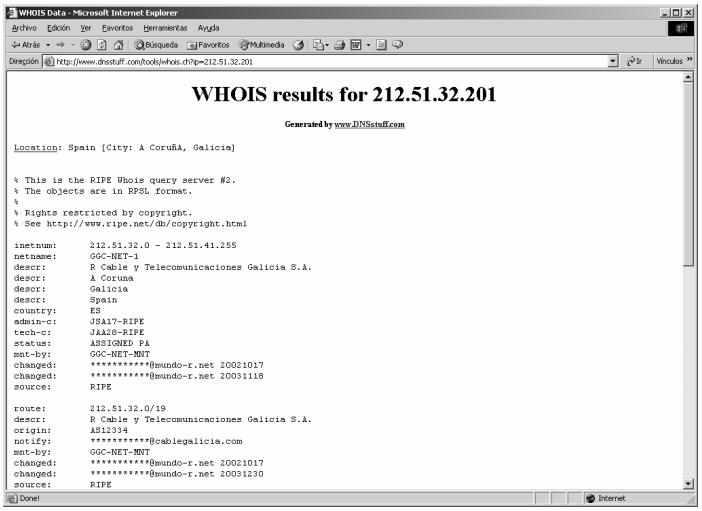

Figura 1.8. Acceso a la base de datos Whois

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*).

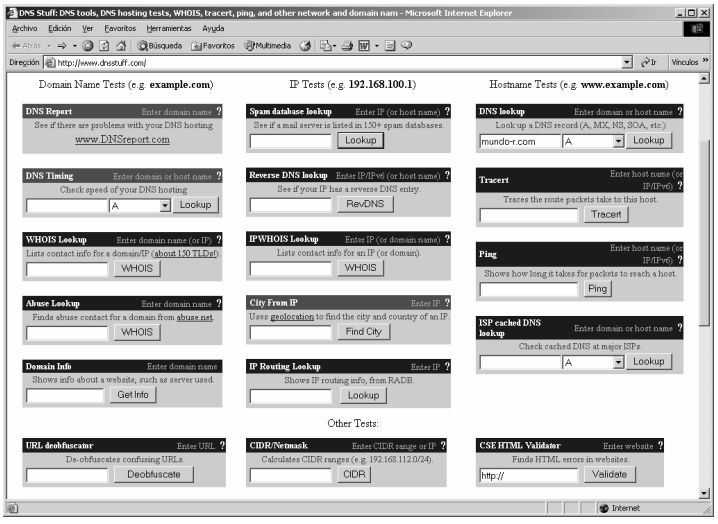

Figura 1.9. DNS Stuff

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 PING[2] (*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.

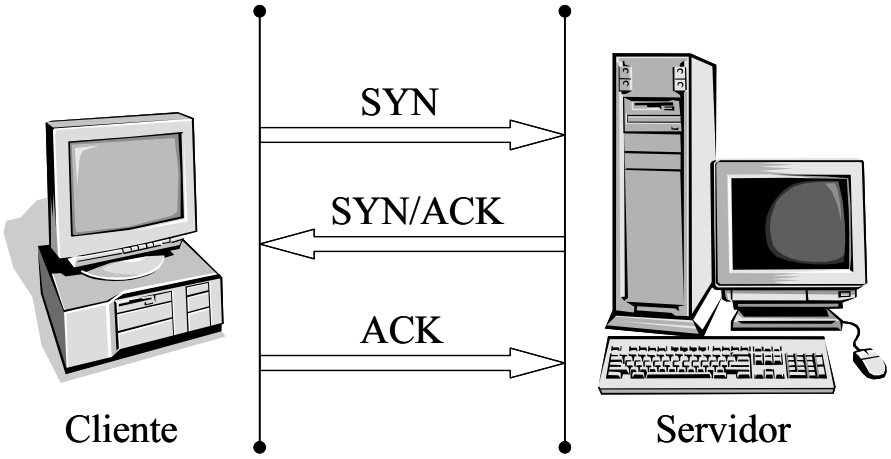

Figura 1.10. Técnica "TCP Connect Scanning"

- 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.

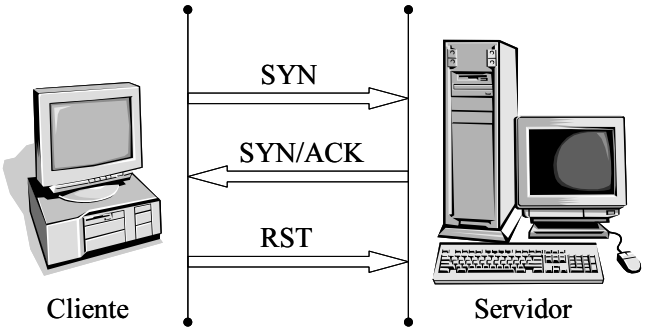

Figura 1.11. Técnica "TCP SYN Scanning"

- 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).

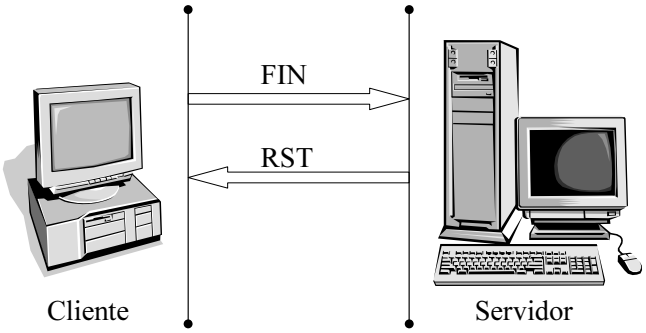

Figura 1.12. Técnica "TCP FIN Scanning"

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 Addresable 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 atraviese 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 física[3] 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 despiste, 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 ordenador[4] (*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 Redirect[5], 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 sistema[6].

- 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 <img src>, 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 malicios 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 construidos, 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.

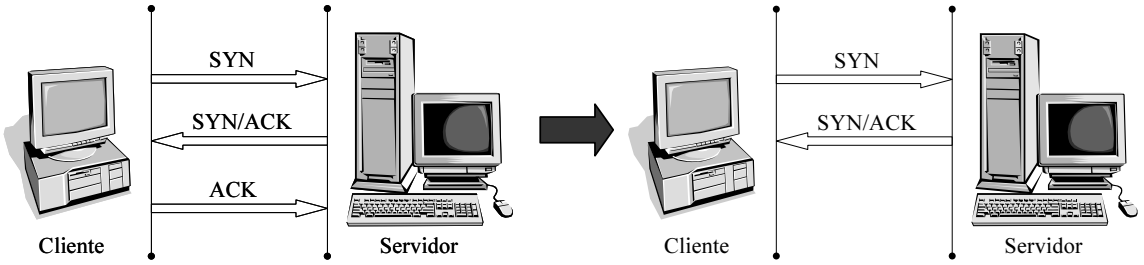

Figura 1.15. Ataque del tipo "SYN Flood"

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 Caribean 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/*.