

CAPÍTULO 7

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar



“La seguridad de un sistema es tan fuerte como su punto más débil... La seguridad total no existe pero si la mínima inseguridad”

infohack.org

AMENAZAS LÓGICAS

La Entropía es una magnitud termodinámica que cuantifica el grado de desorden de un sistema; y según las leyes físicas todo sistema tiende a su máxima entropía. Si extrapolamos este concepto a la Seguridad resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir:

- Los protocolos de comunicación utilizados carecen, en su mayoría, de seguridad o esta ha sido implementada, tiempo después de su creación, en forma de “parche”.
- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.

- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.
- Todo sistema es inseguro.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

7.1 ACCESO – USO – AUTORIZACIÓN

La identificación de estas palabras es muy importante ya que el uso de algunas implica un uso desapropiado de las otras.

Específicamente “Acceso” y “Hacer Uso” no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

- Cuando un **usuario** tiene **acceso autorizado**, implica que tiene **autorizado el uso** de un recurso.
- Cuando un **atacante** tiene **acceso desautorizado** está haciendo **uso desautorizado** del sistema.
- Pero, cuando un **atacante** hace **uso desautorizado** de un sistema, esto implica que el **acceso fue autorizado** (simulación de usuario).

Luego un **Ataque** será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un **Incidente** envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

John D. Howard¹ en su tesis estudia la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los laboratorios del CERT² afirma que esta cantidad varía entre 10 y 1.000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

Tesis "Seguridad Informática: Sus Implicancias e Implementación". □ Copyright Cristian F. Borghello 2001 □ webmaster@cfbsoft.com.ar □ www.cfbsoft.com.ar □
--

7.2 DETECCIÓN DE INTRUSOS

A finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow). Los

¹ HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 12–Página 165

² CERT: Computer Emergency Response Team. Grupo de Seguridad Internacional especializado en dar respuesta a las empresas y organizaciones que denuncian ataques informáticos a sus sistemas de información. <http://www.cert.org>

problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados. Así por ejemplo, un problema de seguridad del grupo rojo es un equipo que tiene el servicio de FTP anónimo mal configurado.

Los problemas de seguridad del grupo amarillo son menos serios pero también reseñables. Implican que el problema detectado no compromete inmediatamente al sistema pero puede causarle serios daños o bien, que es necesario realizar tests más intrusivos para determinar si existe o no un problema del grupo rojo.

La tabla 7.1 resume los sistemas evaluados, el número de equipos en cada categoría y los porcentajes de vulnerabilidad para cada uno. Aunque los resultados son límites superiores, no dejan de ser... escandalosos.

Tipo de sitio	# Total sitios testeados	% Total Vulnerables	% Yellow	% Red
Bancos	660	68,34	32,73	35,61
Créditos	274	51,1	30,66	20,44
Sitios Federales US	47	61,7	23,4	38,3
News	312	69,55	30,77	38,78
Sexo	451	66,08	40,58	25,5
Totales	1.734	64,93	33,85	31,08
Grupo aleatorio	469	33,05	15,78	17,27

Tabla 7.1 – Porcentaje de Vulnerabilidades por tipo de sitio. Fuente: <http://www.trouble.org/survey>

Como puede observarse, cerca de los dos tercios de los sistemas analizados tenían serios problemas de seguridad y Farmer destaca que casi un tercio de ellos podían ser atacados con un mínimo esfuerzo.

7.3 IDENTIFICACIÓN DE LAS AMENAZAS

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- **Data Corruption:** la información que no contenía defectos pasa a tenerlos.
- **Denial of Service (DoS):** servicios que deberían estar disponibles no lo están.
- **Leakage:** los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

La Tabla 7.2 detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos³.

³ HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6–Página 71

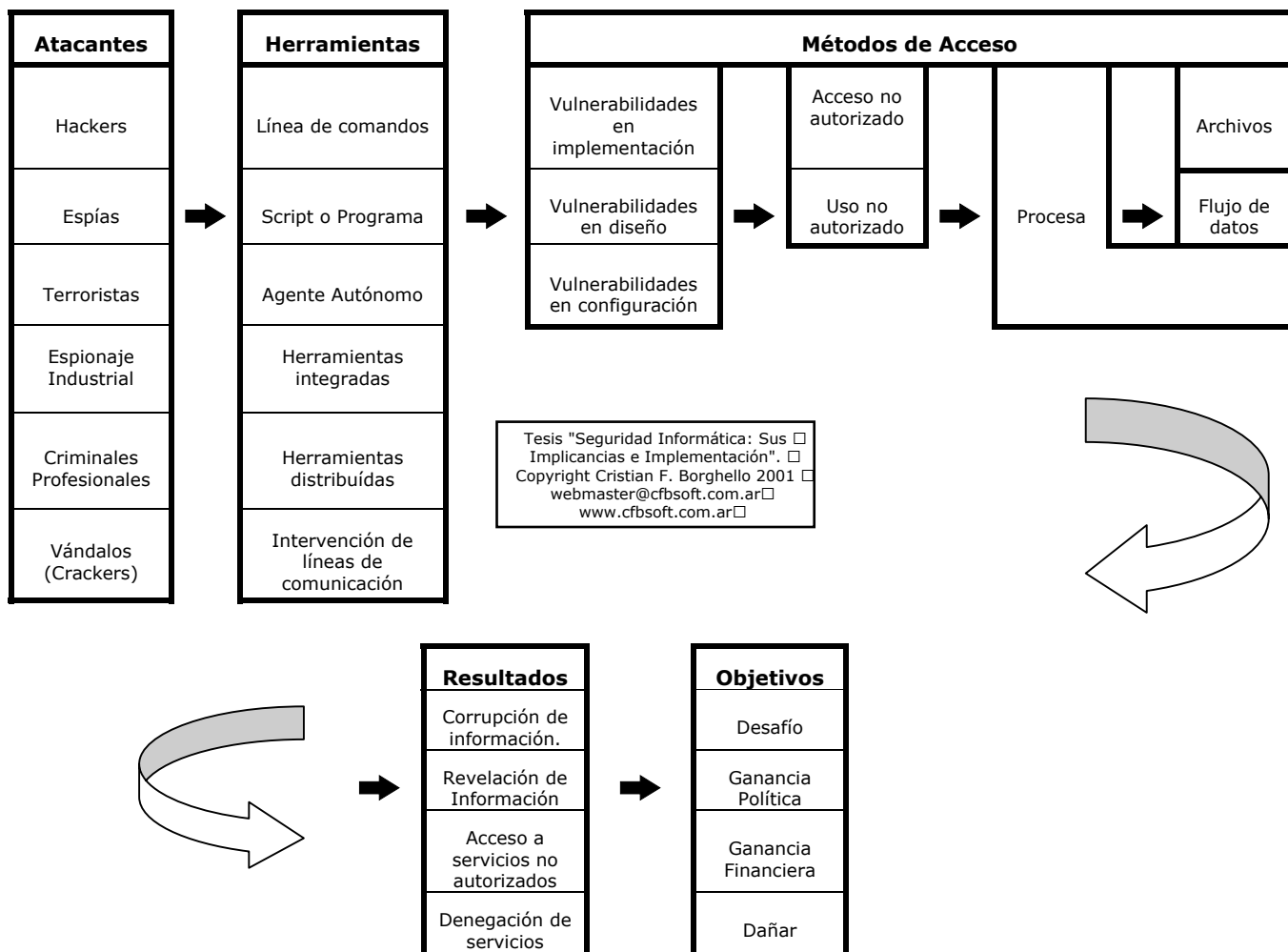


Tabla 7.2. Detalle de Ataques. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6–Página 71

Cualquier adolescente de 15 años (Script Kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Los número que siguen no pretenden alarmar a nadie ni sembrar la semilla del futuro Hacker. Evidentemente la información puede ser aprovechada para fines menos lícitos que para los cuales fue pensada, pero esto es algo ciertamente difícil de evitar.

Año	Incidentes Reportados	Vulnerabilidades Reportadas	Mensajes Recibidos
1988	6		539
1989	132		2.868
1990	252		4.448
1991	406		9.629
1992	773		14.463
1993	1.334		21.267
1994	2.340		29.580

1995	2.412	171	32.084
1996	2.573	345	31.268
1997	2.134	311	39.626
1998	3.734	262	41.871
1999	9.859	417	34.612
2000	21.756	1.090	56.365
2001 (4 meses)	15.476	1.151	39.181
Total	63.187	3.747	357.802

Tabla 7.3 – Vulnerabilidades Reportadas al CERT 1988–2001. Fuente: CERT Internacional.
<http://www.cert.org/statistics>

Nota I: Estos incidentes sólo representan el 30% correspondientes a los Hackers.

Nota II: En 1992 el DISA⁴ realizó un estudio durante el cual se llevaron a cabo 38.000 ataques a distintos sitios de organizaciones gubernamentales (muchas de ellas militares). El resultado de los ataques desde 1992 a 1995 se resumen en el siguiente cuadro⁵:

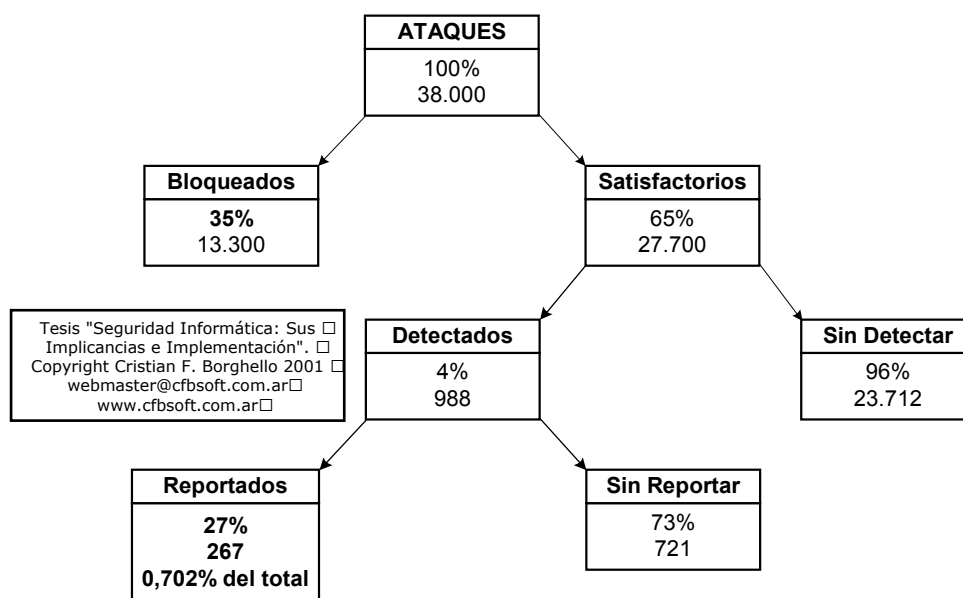


Gráfico 7.1 – Porcentaje de Ataques. Fuente: <http://www.disa.mil>

Puede observarse que solo el 0,70% (267) de los incidentes fueron reportados. Luego, si en el año 2000 se denunciaron 21.756 casos eso arroja 3.064.225 incidentes en ese año.

Nota III: Puede observarse que los incidente reportados en 1997 con respecto al año anterior es menor. Esto puede deberse a diversas causas:

- Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.

⁴ DISA (Defense Information System Agency). <http://www.disa.mil>

⁵ HOWARD, John D. Thesis. An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 12–Página 168.

- Los administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.
- Los “Advisories” (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.

7.4 TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar “agujeros” en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de las mismas. Ante la diversificación de clasificaciones de amenazas y la inminente aparición de nuevas técnicas, para la realización del presente los ataques serán clasificados y categorizados según mi experiencia y conocimiento de cada caso.

Otra lista de términos asociada con los ataques puede ser la siguiente⁶:

<i>Trojan horses</i>	<i>Fraud networks</i>	<i>Fictitious people</i>	<i>Infrastructure observation</i>	<i>e-mail overflow</i>
<i>Time bombs</i>	<i>Get a job</i>	<i>Protection limit poke</i>	<i>Infrastructure interference</i>	<i>Human engineering</i>
<i>Bribes</i>	<i>Dumpster diving</i>	<i>Sympathetic vibration</i>	<i>Password guessing</i>	<i>Packet insertion</i>
<i>Data diddling</i>	<i>Computer viruses</i>	<i>Invalid values on calls</i>	<i>Van Eck bugging</i>	<i>Packet watching</i>
<i>Login spoofing</i>	<i>Data diddling</i>	<i>Wiretapping</i>	<i>Combined attacks</i>	<i>e-mail spoofing</i>
<i>Scanning</i>	<i>Dumpster diving</i>	<i>Eavesdropping</i>	<i>Denial-of-service</i>	<i>Harassment</i>
<i>Masquerading</i>	<i>Software piracy</i>	<i>Data copying</i>	<i>Degradation of service</i>	<i>Traffic analysis</i>
<i>Trap doors</i>	<i>Covert channels</i>	<i>Viruses and worms</i>	<i>Session hijacking</i>	<i>Timing attacks</i>
<i>Tunneling</i>	<i>Trojan horses</i>	<i>IP spoofing</i>	<i>Logic bombs</i>	<i>Salamis</i>
<i>Password sniffing</i>	<i>Excess privileges</i>			

Al describirlos no se pretende dar una guía exacta ni las especificaciones técnicas necesarias para su uso. Sólo se pretende dar una idea de la cantidad y variabilidad de los mismos, así como que su adaptación (y aparición de nuevos) continúa paralela a la creación de nuevas tecnologías.

Cabe destacar que para la utilización de estas técnicas no será necesario contar con grandes centros de cómputos, lo que queda fehacientemente demostrado al saber que algunos

⁶ HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6-Página 52. Se conserva el idioma original (inglés) para no falsear información con respecto a los términos empleados.

Hackers más famosos de la historia hackeaban con computadoras (incluso armadas con partes encontradas en basureros) desde la habitación de su hogar (ver Anexo II).

Cada uno de los ataques abajo descriptos serán dirigidos remotamente. Se define **Ataque Remoto** como “un ataque iniciado contra una maquina sobre la cual el atacante no tiene control físico”⁷. Esta máquina es distinta a la usada por el atacante y será llamada **Víctima**.

7.4.1 INGENIERA SOCIAL

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente (generalmente es así), puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. O bien, podría enviarse un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

Para evitar situaciones de IS es conveniente tener en cuenta estas recomendaciones:

- Tener servicio técnico propio o de confianza.
- Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y deriven la inquietud a los responsables que tenga competencia para dar esa información.
- Asegurarse que las personas que llaman por teléfono son quien dicen ser. Por ejemplo si la persona que llama se identifica como proveedor de Internet lo mejor es cortar y devolver la llamada a forma de confirmación.

7.4.2 INGENIERÍA SOCIAL INVERSA

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

La ISI es más difícil de llevara cabo y por lo general se aplica cuando los usuarios están alertados de acerca de las técnicas de IS. Puede usarse en algunas situaciones específicas y después de mucha preparación e investigación por parte del intruso:

⁷ Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing®. 1999. EE.UU. Capítulo 25.
<http://sams.net>. <http://www.itlibrary.com/reference/library/1575212684/ewtoc.html>

1. Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruso tenga un mínimo contacto con el sistema.
2. Comunicación a los usuarios de que la solución es brindada por el intruso (publicidad).
3. Provisión de ayuda por parte del intruso encubierto como servicio técnico.

7.4.3 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema...”nada se destruye, todo se transforma”.

El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

7.4.4 ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

7.4.4.1 SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post-it adheridos al monitos o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

7.4.4.2 DECOY (SEÑUELOS)

Los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras “visitas”.

Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

7.4.4.3 SCANNING (BÚSQUEDA)

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma.

El Scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número.

Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están “escuchando” por las respuestas recibidas o no recibidas.

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

7.4.4.3.1 TCP Connect Scanning

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina, que lanza el scanner, y también se verá su inmediata desconexión.

7.4.4.3.2 TCP SYN Scanning

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecerla. La aplicación del Servidor “escucha” todo lo que ingresa por los puertos.

La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control de llamada HandShake (saludo) se intercambia entre el Cliente y el Servidor para establecer un dialogo antes de transmitir datos. Los “paquetes” o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos máquinas.

El establecimiento de dicha conexión se realiza mediante lo que se llama Three-Way Handshake (“conexión en tres pasos”) ya que intercambian tres segmentos.

En forma esquemática se tiene:

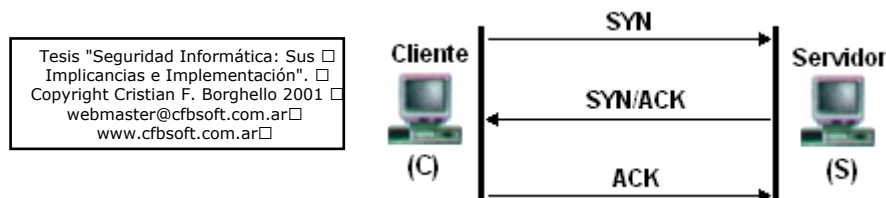


Gráfico 7.2 – Conexión en Tres Pasos.

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN. Este segmento le dice a S que C desea establecer una conexión.
2. S (si está abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autenticación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia, realizan otra negociación a tres bandas con segmentos FIN en vez SYN.

La técnica TCP SYN Scanning, implementa un scaneo de “media-apertura”, dado que nunca se abre una sesión TCP completa.

Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

7.4.4.3.3 TCP FIN Scanning– Stealth Port Scanning

Hay veces en que incluso el scaneo SYN no es lo suficientemente “clandestino” o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos.

Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas, entre los que se hallan los de Microsoft®, no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas Unix.

Este último es un ejemplo en el que se puede apreciar que algunas vulnerabilidades se presentan en la aplicación de tecnologías (en este caso el protocolo TCP nacido en los años '70) y no sobre sus implementaciones. Es más, se observa que una implementación incorrecta (la de Microsoft®) soluciona el problema.

“Muchos de los problemas globales de vulnerabilidades son inherentes al diseño original de algunos protocolos”⁸.

7.4.4.3.4 Fragmentation Scanning

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

7.4.4.4 EAVESDROPPING–PACKET SNIFFING

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Cada maquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino de los paquetes TCP. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen.

Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).

Inicialmente este tipo de software, era únicamente utilizado por los administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y

⁸ GONCALVES, Marcus. Firewalls Complete. Beta Book. McGraw Hill. 1997. EE.UU. Página 25

salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan.

Normalmente, los buenos Sniffers, no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

7.4.4.5 SNOOPING–DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron: el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

7.4.5 ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

7.4.5.1 SPOOFING–LOOPING

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

Spoofing puede traducirse como “hacerse pasar por otro” y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño).

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de “evaporar” la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del Looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un

Insider, o por un estudiante a miles de Kilómetros de distancia, pero que ha tomado la identidad de otros.

La investigación de procedencia de un Looping es casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta.

El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía e-mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaria había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.

Muchos ataques de este tipo comienzan con Ingeniería Social, y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

7.4.5.2 SPOOFING

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing

7.4.5.2.1 IP Spoofing

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima “ve” un ataque proveniente de esa tercera red, y no la dirección real del intruso.

El esquema con dos puentes es el siguiente:

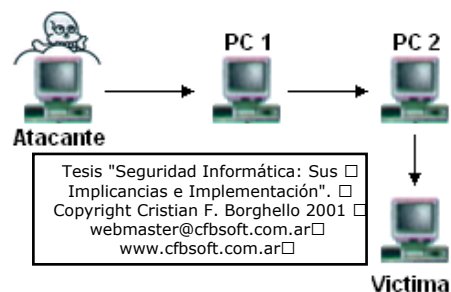


Gráfico 7.3 – Ataque Spoofing

Nótese que si la Victima descubre el ataque verá a la PC_2 como su atacante y no el verdadero origen.

Este ataque se hizo famoso al usarlo Kevin Mitnick (ver Anexo II).

7.4.5.2.2 DNS Spoofing

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server–DNS) de Windows

NT[©]. Si se permite el método de recursión en la resolución de “Nombre↔Dirección IP” en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método de funcionamiento por defecto.

7.4.5.3 WEB SPOOFING

En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc.

El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

7.4.5.4 IP SPLICING–HIJACKING

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

Para entender el procedimiento supongamos la siguiente situación:

IP Cliente : IP 195.1.1.1
IP Servidor: IP 195.1.1.2
IP Atacante: IP 195.1.1.3

1. El cliente establece una conexión con su servidor enviando un paquete que contendrá la dirección origen, destino, número de secuencia (para luego armar el paquete) y un número de autenticación utilizado por el servidor para “reconocer” el paquete siguiente en la secuencia. Supongamos que este paquete contiene:

IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF45ADA (el primero es al azar)
ACK = F454FDF5
Datos: Solicitud

Tesis "Seguridad Informática: Sus Implicancias e Implementación". □ Copyright Cristian F. Borghello 2001 □ webmaster@cfbsoft.com.ar□ www.cfbsoft.com.ar□
--

2. El servidor, luego de recibir el primer paquete contesta al cliente con paquete Echo (recibido).

IP Origen : 195.1.1.2 Puerto 1025
IP Destino: 195.1.1.1 Puerto 23
SEQ = F454FDF5 (ACK enviado por el cliente)
ACK = 3DF454E4
Datos: Recepción OK (Echo)

3. El cliente envía un paquete ACK al servidor, sin datos, en donde le comunica lo “perfecto” de la comunicación.

IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23

SEQ = 3DF454E4 (ACK enviado por el servidor)

ACK = F454FDFF

Datos: Confirmación de Recepción (ACK)

4. El atacante que ha visto, mediante un Sniffer, los paquete que circularon por la red calcula el número de secuencia siguiente: el actual + tamaño del campo de datos. Para calcular el tamaño de este campo:

1° Paquete ACK Cliente = F454FDF5

2° Paquete ACK Cliente = F454FDFF

Tamaño del campo datos = F454FDFF - F454FDF5 = **0A**

5. Hecho esto el atacante envía un paquete con la siguiente aspecto:

IP Origen : IP 195.1.1.1 (IP del Cliente por el atacante)

IP Destino: IP 195.1.1.2 (IP del Servidor)

SEQ = 3DF454E4 (Ultimo ACK enviado por el Cliente)

ACK = F454FE09 (F454FDFF + 0A)

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son los que esperaba recibir. El cliente, a su vez, quedará esperando datos como si su conexión estuviera colgada y el atacante podrá seguir enviando datos mediante el procedimiento descrito.

7.4.5.5 UTILIZACIÓN DE BACKDOORS

“Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autenticación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo”⁹.

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

7.4.5.6 UTILIZACIÓN DE EXPLOITS

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos “agujeros” reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

⁹ HUERTA, Antonio Villalón. “Seguridad en Unix y redes”. Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000. Capítulo 5–Página 81. <http://www.kriptopolis.com>

7.4.5.7 OBTENCIÓN DE PASSWORDS

Este método comprende la obtención por “Fuerza Bruta” de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados.

Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y “diccionarios” que prueban millones de posibles claves hasta encontrar la password correcta.

La política de administración de password será discutida en capítulos posteriores.

7.4.5.7.1 Uso de Diccionarios

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada.

Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se este atacando.

En la tabla 7.4 podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

Cantidad de Caracteres	26–Letras minúsculas	36–Letras y dígitos	52–Mayúsculas y minúsculas	96–Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

Tabla 7.4 – Cantidad de claves generadas según el número de caracteres empleado

Aquí puede observarse la importancia de la utilización de passwords con al menos 8 caracteres de longitud y combinando todos los caracteres disponibles. En el siguiente Capítulo podrá estudiarse las normas de claves relativamente seguras y resistentes.

7.4.6 DENIAL OF SERVICE (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un “crash” del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede “matar” en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DoS deteniendo los servicios.

7.4.6.1 JAMMING O FLOODING

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el “ping de la muerte” (una versión-trampa del comando ping).

Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

7.4.6.2 SYN FLOOD

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Pero, si el paso final no llega a establecerse, la conexión permanece en un estado denominado “semiabierto”.

El SYN Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista under Phrack; y se basa en un “saludo” incompleto entre los dos hosts.

El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el Host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

SYN Flood aprovecha la mala implementación del protocolo TCP, funcionando de la siguiente manera:

Se envía al destino, una serie de paquetes TCP con el bit SYN activado, (petición de conexión) desde una dirección IP Spoofeada. Esta última debe ser inexistente para que el destino no pueda completar el saludo con el cliente.

Aquí radica el fallo de TCP: ICMP reporta que el cliente es inexistente, pero TCP ignora el mensaje y sigue intentando terminar el saludo con el cliente de forma continua.

Cuando se realiza un Ping a una maquina, esta tiene que procesarlo. Y aunque se trate de un proceso sencillo, (no es mas que ver la dirección de origen y enviarle un paquete Reply), siempre consume recursos del sistema. Si no es un Ping, sino que son varios a la vez, la máquina se vuelve mas lenta... si lo que se recibe son miles de solicitudes, puede que el equipo deje de responder (Flood).

Es obligatorio que la IP origen sea inexistente, ya que sino el objetivo, logrará responderle al cliente con un SYN/ACK, y como esa IP no pidió ninguna conexión, le va a responder al objetivo con un RST, y el ataque no tendrá efecto.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones “semiabiertas” que pueden manejar en un momento determinado (5 a 30). Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones “semiabiertas” van caducando tras un tiempo, liberando “huecos” para nuevas conexiones, pero mientras el atacante mantenga el SYN Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

7.4.6.3 CONNECTION FLOOD

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultaneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las

conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

7.4.6.4 NET FLOOD

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil.

Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua. Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas, sin que el usuario llamado pueda hacer nada al respecto.

En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.

En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea.

El siguiente paso consiste en localizar las fuentes del ataque e informar a sus administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento. Si el atacante emplea IP Spoofing, el rastreo puede ser casi imposible, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar (Looping).

7.4.6.5 LAND ATTACK

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows[®].

El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados-recibidos la máquina termina colgándose.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto.

7.4.6.6 SMURF O BROADCAST STORM

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un

Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Gráficamente:

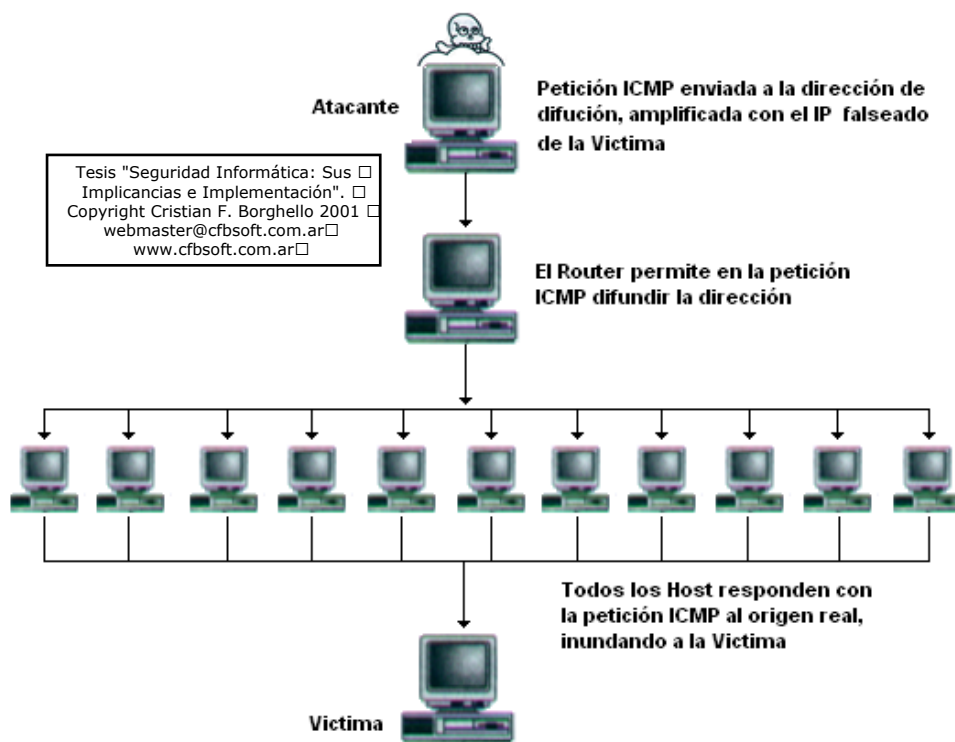


Gráfico 7.4 – Ataque Smurf

Suponiendo que se considere una red de tipo C la dirección de BroadCast sería .255; por lo que el “simple” envío de un paquete se convierte en un efecto multiplicador devastador.

Desgraciadamente la víctima no puede hacer nada para evitarlo. La solución está en manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers para filtrar los paquetes ICMP de petición indeseados (Broadcast); o bien configurar sus máquinas para que no respondan a dichos paquetes. Es decir, que lo que se parchea son las máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no la máquina víctima.

También se podría evitar el ataque si el Router/Firewall de salida del atacante estuviera convenientemente configurado para evitar Spoofing. Esto se haría filtrando todos los paquetes de salida que tuvieran una dirección de origen que no perteneciera a la red interna.

7.4.6.7 OOB, SUPERNUKE O WINNUKE

Un ataque característico, y quizás el más común, de los equipos con Windows[®] es el Nuke, que hace que los equipos que escuchan por el puerto NetBIOS sobre TCP/UDP 137 a

139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados.

Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina víctima detecta como inválidos pasando a un estado inestable. OOB es el término normal, pero realmente consiste en configurar el bit Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido.

Este ataque puede prevenirse instalando los parches adecuados suministrado por el fabricante del sistema operativo afectado. Un filtro efectivo debería garantizar la detección de una inundación de bits Urgentes.

7.4.6.8 TEARDROP I Y II–NEWTEAR–BONK-BOINK

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT[®] 4.0 de Microsoft[®] es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden ser devastadoras.

Los ataques tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

7.4.6.9 E-Mail Bombing–Spamming

El e-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario.

El Spamming, en cambio se refiere a enviar un e-mail a miles de usuarios, hayan estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos.

El Spamming esta siendo actualmente tratado por las leyes europeas (principalmente España) como una violación de los derechos de privacidad del usuario.

7.4.7 ATAQUES DE MODIFICACIÓN–DAÑO

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar□
www.cfbsoft.com.ar□

7.4.7.1 TAMPERING O DATA DIDDLE

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos. Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

Aún así, si no hubo intenciones de “bajar” el sistema por parte del atacante; el administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por Insiders o Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva.

Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA; o la reciente modificación del Web Site del CERT (mayo de 2001).

Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.). La utilización de programas troyanos y difusión de virus esta dentro de esta categoría, y se profundizará sobre el tema en otra sección el presente capítulo.

7.4.7.2 BORRADO DE HUELLAS

El borrado de huellas es una de las tareas mas importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir “tapar el hueco” de seguridad, evitar ataques futuros e incluso rastrear al atacante.

Las **Huellas** son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo.

Los archivos Logs son una de la principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos

7.4.7.3 ATAQUES MEDIANTE JAVA APPLETS

Tesis "Seguridad Informática: Sus Implicancias e Implementación". Copyright Cristian F. Borghello 2001 webmaster@cfbsoft.com.ar www.cfbsoft.com.ar
--

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java.

Estos Applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos¹⁰ especializados en descubrir fallas de seguridad¹¹ en las implementaciones de las MVJ.

¹⁰ Safe Internet Programming: Creadores sobre seguridad en Java <http://www.cs.princeton.edu/sip>

¹¹ Hostile Applets Home Page (HAHP): Seguridad en Java. Dr. Mark D. LaDue.
<http://www.rstcorp.com/hostile-applets>

7.4.7.4 ATAQUES CON JAVASCRIPT Y VBSCRIPT

JavaScript (de la empresa Netscape[®]) y VBScript (de Microsoft[®]) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador.

Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

7.4.7.5 ATAQUES MEDIANTE ACTIVEX

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft[®]. Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft[®] a Java.

ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador.

Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expidió el certificado y/o en el control ActiveX. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia.

Esta última característica es el mayor punto débil de los controles ActiveX ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino.

La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar.

Así, un conocido grupo de hackers alemanes¹², desarrolló un control ActiveX maligno que modificaba el programa de Gestión Bancaria Personal Quicken95[®] de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán.

Otro control ActiveX muy especialmente “malévolo” es aquel que manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto, el sistema de la víctima, a ataques con tecnología ActiveX.

La autenticación de usuarios mediante Certificados y las Autoridades Certificadoras será abordada con profundidad en capítulos posteriores.

¹² Computers Chaos Club. <http://www.ccc.de>

7.4.7.6 VULNERABILIDADES EN LOS NAVEGADORES

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los “Buffer Overflow”¹³.

Los “Buffer Overflows” consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

Los protocolos usados pueden ser HTTP, pero también otros menos conocidos, internos de cada explorador, como el “res:” o el “mk:”. Precisamente existen fallos de seguridad del tipo “Buffer Overflow” en la implementación de estos dos protocolos.

Además la reciente aparición (octubre de 2000) de vulnerabilidades del tipo Transversal en el servidor Web Internet Information Server[®] de la empresa Microsoft[®], explotando fallas en la traducción de caracteres Unicode, puso de manifiesto cuán fácil puede resultar explotar una cadena no validada. Por ejemplo:

```
www.servidor.com/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
```

devuelve el directorio de la unidad c: del servidor deseado.

Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje Assembler y de la estructura interna de la memoria del sistema operativo utilizado o bien, leer la documentación de sitios web donde explican estas fallas.

También se puede citar el fallo de seguridad descubierto por Cybersnot Industries[®] relativo a los archivos “.lnk” y “.url” de Windows 95[®] y NT[®] respectivamente. Algunas versiones de Microsoft Internet Explorer[®] podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima (por ejemplo el tan conocido y temido *format.com*).

Para más información relacionada con los ataques intrínsecos a los navegadores, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer^{®14} como en Netscape Communicator^{®15}.

7.4.8 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN

Muchos sistemas están expuestos a “agujeros” de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de “puertas invisibles” son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informáticos disponibles.

¹³ http://www.newhackcity.net/win_buff_overflow

¹⁴ <http://www.nwnetworks.com/iesf.html>

¹⁵ <http://hplyot.obspm.fr/~dl/netscapesec>

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows[®]). La importancia y ventaja del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente se encuentran en Internet avisos de nuevos descubrimientos de problemas de seguridad, herramientas de Hacking y Exploits que los explotan, por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

7.4.9 IMPLEMENTACIÓN DE ESTAS TÉCNICAS

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

A lo largo de mi investigación he recopilando distinto tipos de programas que son la aplicación de las distintas técnicas enumeradas anteriormente. La mayoría de las mismos son encontrados fácilmente en Internet en versiones ejecutables, y de otros se encuentra el código fuente, generalmente en lenguaje C, Java y Perl.

Cada una de las técnicas explicadas pueden ser utilizadas por un intruso en un ataque. A continuación se intentarán establecer el orden de utilización de las mismas, pero siempre remarcando que un ataque insume mucha paciencia, imaginación acumulación de conocimientos y experiencia dada, en la mayoría de los casos por prueba y error.

1. Identificación del problema (víctima): en esta etapa se recopila toda la información posible de la víctima. Cuanta más información se acumule, más exacto y preciso será el ataque, más fácil será eliminar las evidencias y más difícil será su rastreo.
2. Exploración del sistema víctima elegido: en esta etapa se recopila información sobre los sistemas activos de la víctima, cuales son los más vulnerables y cuales se encuentran disponibles. Es importante remarcar que si la victima parece apropiada en la etapa de Identificación, no significa que esto resulte así en esta segunda etapa.
3. Enumeración: en esta etapa se identificaran las cuentas activas y los recursos compartidos mal protegidos. La diferencia con las etapas anteriores es que aquí se establece una conexión activa a los sistemas y la realización de consultas dirigidas. Estas intrusiones pueden (y deberían) ser registradas, por el administrador del sistema, o al menos detectadas para luego ser bloqueadas.
4. Intrusión propiamente dicha: en esta etapa el intruso conoce perfectamente el sistema y sus debilidades y comienza a realizar las tareas que lo llevaron a trabajar, en muchas ocasiones, durante meses.

Contrariamente a lo que se piensa, los sistemas son difíciles de penetrar si están bien administrados y configurados. Ocasionalmente los defectos propios de la arquitectura de los sistemas proporciona un fácil acceso, pero esto puede ser, en la mayoría de los casos, subsanado aplicando las soluciones halladas.

El anexo III se brinda una lista de herramientas disponibles, las cuales son la implementación de las técnicas estudiadas.

7.4.10 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son “solucionables” en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico “broadcast” desde fuera de nuestra red. De esta forma evitamos ser empleados como “multiplicadores” durante un ataque Smurf.
5. Filtrar el tráfico IP Spoof.
6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, **la capacitación continua del usuario.**

7.5 CREACIÓN Y DIFUSIÓN DE VIRUS

Quizás uno de los temas más famosos y sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los Virus.

Pero como siempre en esta oscura realidad existe una parte que es cierta y otra que no lo es tanto. Para aclarar este enigma veamos porque se eligió la palabra Virus (del latín Veneno) y que son realmente estos “parásitos”.

7.5.1 VIRUS INFORMÁTICOS VS VIRUS BIOLÓGICOS

Un análisis comparativo de analogías y diferencias entre las dos “especies”, muestra que las similitudes entre ambos son poco menos que asombrosas. Para notarlas ante todo debemos saber con exactitud que es un Virus Informático y que es un Virus Biológico.

Virus Informático (VI): Pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica).¹⁶

“Un virus responde al modelo DAS: Dañino, Autorreplicante y Subrepticio.”¹⁷

Virus Biológico (VB): Fragmentos de ADN o ARN cubiertos de una capa proteica. Se reproducen solo en el interior de células vivas, para lo cual toman el control de sus enzimas y metabolismo. Sin esto son tan inertes como cualquier otra macromolécula.¹⁸

Algunas analogías entre ambos son:

1. Los VB están compuestos por ácidos nucleicos que contienen información (programa dañino o VI) suficiente y necesaria para que utilizando los ácidos de la célula huésped (programa infectado por los VI) puedan reproducirse a sí mismos.
2. Los VB no poseen metabolismo propio, por lo tanto no manifiestan actividad fuera del huésped. Esto también sucede en los VI, por ejemplo, si se apaga la máquina o si el virus se encuentra en un disquete que esta dentro de un cajón.
3. El tamaño de un VB es relativamente pequeño en comparación con las células que infectan. Con los VI sucede lo mismo. Tanto los VB como los VI causan un daño sobre el huésped.
4. Ambos virus inician su actividad en forma oculta y sin conocimiento de su huésped, y suelen hacerse evidentes luego de que el daño ya es demasiado alto como para corregirse.

Tesis "Seguridad Informática: Sus Implicancias e Implementación". □ Copyright Cristian F. Borghello 2001 □ webmaster@cfbsoft.com.ar □ www.cfbsoft.com.ar □
--

¹⁶⁻¹⁸ Revista Virus Reports. Ediciones Ubik Número 16-Página 2.

¹⁷ Dr Fred Cohen. Considerado el padre de los VI y de sus técnicas de defensa: <http://all.net>

5. La finalidad de un VB (según la ciencia) es la reproducción y eventual destrucción del huésped como consecuencia. La de los VI pueden ser muchos los motivos de su creación (por parte de su autor), pero también terminan destruyendo o modificando de alguna manera a su huésped.
6. Ambos virus contienen la información necesaria para su replicación y eventual destrucción. La diferencia radica en la forma de contener esta información: en los VB es un código genético y en los VI es código binario.
7. El soporte de la información también es compartida por ambos “organismos”. En los VB el soporte lo brinda el ADN o ARN (soporte orgánico). En los VI el soporte es un medio magnético (inorgánico).
8. Ambos tipos de virus son propagados de diversa formas (y raramente en todas ellas). En el caso de los VB su medio de propagación es el aire, agua, contacto directo, etc. Los VI pueden propagarse introduciendo un disquete infectado en una computadora sana (y ejecutando la zona infectada, ¡claro está!); o viceversa: de RAM infectada a un disquete sano; o directamente aprovechando un flujo de electrones: modem, red, etc.
9. En ambos casos sucede que la reproducción es de tipo replicativo del original y cuya exactitud dependerá de la existencia de mutaciones o no.
10. Ambas entidades cumplen con el patrón de epidemiología médica.
11. El origen de una entidad generalmente es desconocido, pero lo que se sabe con exactitud es que los VI son producidos por seres humanos y que los VB son entidades de origen biológico y últimamente de origen humano (armas biológicas).

Son, sin dudas, muchas más las analogías que pueden encontrarse haciendo un análisis más exhaustivo de ambas entidades, pero que trascenderían los límites de este informe. La idea es solamente dejar bien en claro que no existe ningún extraño, oscuro o sobrenatural motivo que dé explicación a un VI. Simplemente es un programa más, que cualquiera de nosotros sería capaz de concebir... con las herramientas e intenciones apropiadas del caso.

7.5.2 ORIGEN

Tesis "Seguridad Informática: Sus ☐
 Implicancias e Implementación". ☐
 Copyright Cristian F. Borghello 2001 ☐
 webmaster@cfbsoft.com.ar ☐
 www.cfbsoft.com.ar ☐

Los orígenes de los VI se puede establecer al observar investigaciones sobre Inteligencia y Vida Artificial. Estos conceptos fueron desarrollados por John Von Neuman hacia 1950 estableciendo por primera vez la idea de programas autorreplicables.

Luego, en 1960 en los laboratorios de Bell se desarrollaron juegos (programas) que “luchaban” entre sí con el objetivo de lograr el mayor espacio de memoria posible. Estos programas llamados Core Wars hacían uso de técnicas de ataque, defensa, ocultamiento y reproducción que luego adoptaron los VI.

En 1970, John Shoch y Jon Hupp elaboraron, en el Palo Alto Research Center (PARC) de Xerox, programas autorreplicables que servían para controlar la salud de las redes informáticas. Días después de su lanzamiento el programa se propago en todas las máquinas y sus múltiples (miles) copias de sí mismo colapsaron la red. Cabe aclarar que el fin de estos programas era, en un principio, solo experimental y sin fines maléficos.

En los años 80 nacen los primeros VI propiamente dichos y en 1983 se establece una definición para los mismos. En 1985 infectaban el MS-DOS[®] y en 1986 ya eran destructivos

(Brain, Vienna, Viernes 13, etc.). Estos utilizaban disquetes para su propagación y dependían totalmente de la ignorancia del público que hacía copias indiscriminadas de los mismos.

En palabras del Dr Fred Cohen¹⁹:

“El 3 noviembre de 1983, el primer virus fue concebido como un experimento para ser presentado en un seminario semanal de Seguridad Informática. El concepto fue introducido por el autor y el nombre “virus” fue dado por Len Adleman. Después de ocho horas de trabajo sobre un VAX 11/750 ejecutando Unix, el primer virus estuvo listo para la demostración. En esa semana fueron obtenidos los permisos y cinco experimentos fueron realizados. El 10 de noviembre el virus fue mostrado. La infección inicial fue realizada en “vd” (un programa que mostraba la estructura de archivos de Unix gráficamente) e introducido a los usuarios vía un BBS (...).”.

De aquí quizás provenga la ¿leyenda? en donde se sugiere que los VI surgieron como una medida de seguridad de compañías de desarrollo de software para disuadir a los usuarios de la adquisición de software ilegal. Esta versión no ha sido demostrada ni desmentida, pero el tiempo ha demostrado que los verdaderos perjudicados son las mismas compañías acusadas en su momento.

El 2 de noviembre de 1988 se produce el primer ataque masivo a una red (ARPAnet, precursora de Internet). El método utilizado para su autorreplicación era el correo electrónico y en tres horas el gusano se hizo conocer en todo EE.UU. La erradicación de este gusano costó un millón de dólares y demostró qué podía hacer un programa autorreplicable fuera de control.

El autor, Robert Morris (hijo de uno de los programadores de Core Wars), graduado de Harvard de 23 años reconoció su error y lo calificó de “fallo catastrófico”, ya que su idea no era hacer que los ordenadores se relentizaran.

En este mismo año, como consecuencia de lo acontecido y de la concientización, por parte de la industria informática, de la necesidad de defender los sistemas informáticos, aparecen los primeros programas antivirus.

En 1991 aparecen los primeros Kits para la construcción de virus, lo que facilitó su creación e hizo aumentar su número a mayor velocidad. El primero fue el VCL (Virus Creation Laboratory), creado por Nowhere Man.

En 1992 nace el virus Michelangelo (basado en el Stoned), y aunque es un virus no especialmente destructivo, la prensa lo “vendió” como una grave amenaza mundial. Algunos fabricantes de antivirus, aseguraron que cinco millones de computadoras se verían afectadas por el virus. El número no pasó de cinco mil. Pese a ello, la noticia provocó una alarma injustificada entre los usuarios de ordenadores personales, aunque en cierto modo también sirvió para concientizar a estos mismos usuarios de la necesidad de estar alerta frente a los virus, que ya habían dejado definitivamente de ser una curiosidad científica para pasar a convertirse en una plaga peligrosa.

A partir de aquí, los virus alcanzaron notoriedad y son perfeccionados día a día mediante técnicas de programación poco comunes. Su proliferación se debió, principalmente, al crecimiento de las redes y a los medios para compartir información.

¹⁹ Dr Fred Cohen. Considerado el padre de los VI y de sus técnicas de defensa: <http://all.net>

7.5.3 LOS NÚMEROS HABLAN

Tesis "Seguridad Informática: Sus
Implicancias e Implementación". □
Copyright Cristian F. Borghello 2001 □
webmaster@cfbsoft.com.ar □
www.cfbsoft.com.ar □

A mediados de los noventa se produjeron enormes cambios en el mundo de la informática personal que llegan hasta nuestros días y que dispararon el número de virus en circulación hasta límites insospechados. Si a finales de 1994 el número de virus, según la International Computer Security Association (ICSA), rondaba los cuatro mil, en los siguientes cinco años esa cifra se multiplicó por diez, y promete seguir aumentando.

Cientos de virus son descubiertos mes a mes (de 6 a 20 por día), y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada.

La NCSA²⁰ es el principal organismo dedicado al seguimiento del fenómeno de los virus en todo el mundo. Según sus informes, en Estados Unidos más del 99% de las grandes y medianas empresas han sufrido la infección por virus en alguno de sus computadoras. Sólo un 0,67% asegura no haberse encontrado nunca con un virus.

Se calcula que, en término medio, se infectan 40,6% computadoras al año. La proporción de infecciones anuales ha crecido ampliamente, ya que en 1996 este índice era sólo del 12%.

Existen virus adscritos a programa y también a documentos, los conocidos como Macrovirus. Estos últimos, concretamente los que utilizan documentos de MS-Word[®] para la infección comenzaron su propagación en 1995, cuando Microsoft[®] lanza su nueva versión de este popular procesador de texto.

Aprovechando esta innovación tecnológica (las macros), han aparecido más de 1.900 virus diferentes, registrados y catalogados, que utilizan este medio para infectar los documentos. Tal ha sido su crecimiento y extensión, que los principales responsables de la lucha antivirus llegaron a recomendar que no se enviaran ni se aceptaran documentos de MS-Word[®] enviados por Internet, lo que supone una fuerte limitación al uso del correo electrónico. Entre los diez virus más importantes de 1997, cuatro eran macros de Word.

Según la NCSA, si sólo un 30% de todos las PCs del mundo utilizaran un antivirus actualizado y activo de forma permanente, se cortaría la cadena de contagio y se acabaría con el fenómeno de los virus en todo el mundo.

Sin embargo, no todos los usuarios, bien sean de carácter empresarial o doméstico, son conscientes del riesgo que corren. Hace un tiempo bastaba con chequear los nuevos programas o archivos que se introducían en la computadora, teniendo especial cuidado con el software pirateado (principal forma de contagio) y con los disquetes usados provenientes de otras personas. De alguna manera, las vías de transmisión eran menores y estaban más controladas. Pero con Internet, las posibilidades de infección se han multiplicado con creces.

Desde el 17 al 31 de julio del año 2000 el Ministerio de Ciencia y Tecnología de España, la empresa antivirus Panda Software y otras organizaciones montaron la Primera Campaña Nacional Antivirus Informáticos²¹. El propósito de la campaña era ofrecer al usuario

²⁰ NCSA: National Computer Security Association. <http://www.ncsa.com>

²¹ Campaña Nacional Antivirus Informáticos. <http://www.sinvirus.com>

la posibilidad de búsqueda de virus en su sistema (en forma on-line) y desinfección del mismo.

Al finalizar la campaña, se obtuvieron 516.122 visitas al sitio y se eliminaron 348.195 virus. Las vías de infección informadas fueron el 56% vía e-mail, el 31% vía disquete y el 5% vía CD-ROM.

A nivel mundial, en el ámbito de las medianas y grandes empresas, históricamente, la mayor causa de pérdidas de información fue el sabotaje, seguido por los virus informáticos y por último por otras causas como fallas e impericias. Durante 1993 y 1994 las pérdidas por virus superaron las ocasionadas por sabotaje, pero a partir de 1995 el sabotaje volvió a ocupar el primer lugar debido a la utilización de virus específicos.

Según la NCSA en 1995 el volumen de pérdidas causadas en los Estados Unidos por VI era similar al de las pérdidas por Hacking y alcanzaban los U\$S1.000 millones. En 1996 las pérdidas por VI aumentaron en mayor proporción que las causadas por intrusos informáticos alcanzando los U\$S5.000 millones y U\$S6.000 millones respectivamente

7.5.4 DESCRIPCIÓN DE UN VIRUS

Si bien un VI es un ataque de tipo Tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o a través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse rápidamente.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.EXE, .COM, .DLL, etc), los sectores de Boot y la Tabla de Partición de los discos. Actualmente los que causan mayores problemas son los macro-virus y script-virus, que están ocultos en simples documentos, planillas de cálculo, correo electrónico y aplicaciones que utiliza cualquier usuario de PC. La difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no dependen de un sistema operativo en particular, ya que un documento puede ser procesado tanto en Windows® 95/98/NT/2000®, como en una Macintosh u otras.

7.5.4.1 TÉCNICAS DE PROPAGACIÓN

Actualmente las técnicas utilizadas por los virus para logra su propagación y subsistencia son muy variadas y existen aquellos que utilizan varias de ellas para lograrlo.

1. **Disquetes y otros medios removibles.** A la posibilidad de que un disquete contenga un archivo infectado se une el peligro de que integre un virus de sector de arranque (Boot). En este segundo caso, y si el usuario lo deja en la disquetera, infectará el ordenador cuando lo encienda, ya que el sistema intentará arrancar desde el disquete.
2. **Correo electrónico:** el usuario no necesita hacer nada para recibir mensajes que, en muchos casos ni siquiera ha solicitado y que pueden llegar de cualquier lugar del mundo. Los mensajes de correo electrónico pueden incluir archivos, documentos o cualquier objeto ActiveX-Java infectado que, al ejecutarse, contagian la computadora del usuario. En las últimas generaciones de virus se

envían e-mails sin mensajes pero con archivos adjuntos (virus) que al abrirlos proceden a su ejecución y posterior infección del sistema atacado. Estos virus poseen una gran velocidad de propagación ya que se envían automáticamente a los contactos de la libreta de direcciones del sistema infectado.

3. **IRC o Chat:** las aplicaciones de mensajería instantánea (ICQ, AOL Instant Messenger, etc.) o Internet Relay Chat (IRC), proporcionan un medio de comunicación anónimo, rápido, eficiente, cómodo y barato. Sin embargo, también son peligrosas, ya que los entornos de chat ofrecen, por regla general, facilidades para la transmisión de archivos, que conllevan un gran riesgo en un entorno de red.
4. **Páginas web y transferencia de archivos vía FTP:** los archivos que se descargan de Internet pueden estar infectados, y pueden provocar acciones dañinas en el sistema en el que se ejecutan.
5. **Grupos de noticias:** sus mensajes e información (archivos) pueden estar infectados y, por lo tanto, contagiar al equipo del usuario que participe en ellos.

7.5.4.2 TIPOS DE VIRUS

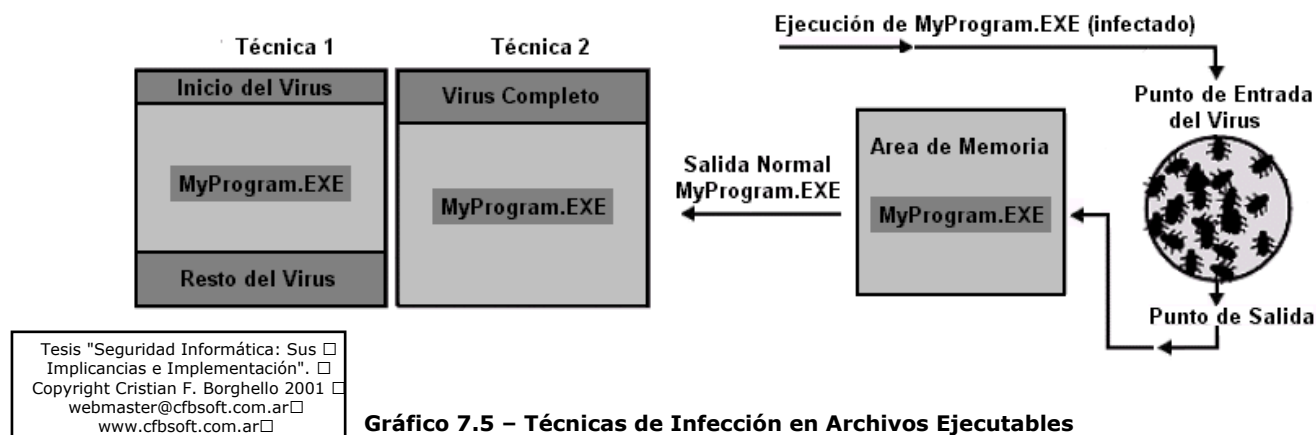
Un virus puede causar daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada y nadie en su sano juicio deseará ejecutarlo. Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para que su “programa” pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas:

7.5.4.2.1 Archivos Ejecutable (virus ExeVir)

El virus se adosa a un archivo ejecutable y desvía el flujo de ejecución a su código, para luego retornar al huésped y ejecutar las acciones esperadas por el usuario. Al realizarse esta acción el usuario no se percata de lo sucedido. Una vez que el virus es ejecutado se aloja en memoria y puede infectar otros archivos ejecutables que sean abiertos en esa máquina.

En este momento su dispersión se realiza en sistema de 16 bits (DOS) y de 32 bits (Windows) indistintamente, atacando programas .COM, .EXE, .DLL, .SYS, .PIF, etc, según el sistema infectado.

Ejemplos: Chernovil, Darth Vader, PHX



7.5.4.2.2 Virus en el Sector de Arranque (Virus ACSO Anterior a la Carga del SO)

En los primeros 512 bytes de un disquete formateado se encuentran las rutinas necesarias para la carga y reconocimiento de dicho disquete. Entre ellas se encuentra la función invocada si no se encuentra el Sistema Operativo. Es decir que estos 512 bytes se ejecutan cada vez que se intenta arrancar (bootear) desde un disquete (o si se dejó olvidado uno en la unidad y el orden de booteo de la PC es A: y luego C:). Luego, esta área es el objetivo de un virus de booteo.

Se guarda la zona de booteo original en otro sector del disco (generalmente uno muy cercano o los más altos). Luego el virus carga la antigua zona de booteo. Al arrancar el disquete se ejecuta el virus (que obligatoriamente debe tener 512 bytes o menos) quedando residente en memoria; luego ejecuta la zona de booteo original, salvada anteriormente. Una vez más el usuario no se percata de lo sucedido ya que la zona de booteo se ejecuta iniciando el sistema operativo (si existiera) o informando la falta del mismo.

Ejemplo: 512, Stoned, Michelangelo, Diablo.

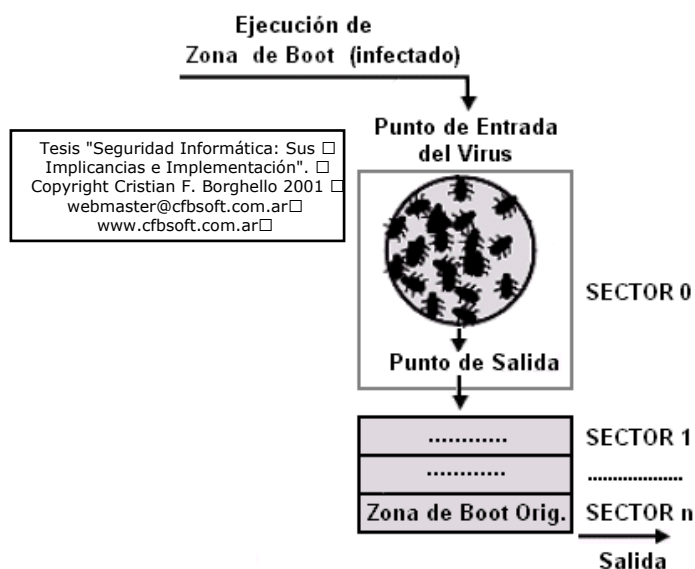


Gráfico 7.6 – Técnica de infección en Zona de Booteo

7.5.4.2.3 Virus Residente

Como ya se mencionó, un virus puede residir en memoria. El objetivo de esta acción es controlar los accesos a disco realizados por el usuario y el Sistema Operativo. Cada vez que se produce un acceso, el virus verifica si el disco o archivo objetivo al que se accede, está infectado y si no lo está procede a almacenar su propio código en el mismo. Este código se almacenará en un archivo, tabla de partición, o en el sector de booteo, dependiendo del tipo de virus que se trate.

Ejemplos: 512, Avispa, Michelangelo, DIR II.

7.5.4.2.4 Macrovirus

Estos virus infectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Últimamente son los más expandidos, ya que todos los usuarios necesitan hacer intercambio de documentos para realizar su trabajo. Los primeros antecedentes de ellos fueron con las macros de Lotus 123[®] que ya eran lo suficientemente poderosas como permitir este tipo de implementación. Pero los primeros de difusión masiva fueron desarrollados a principios de los '90 para el procesador de texto Microsoft Word[®], ya que este cuenta con el lenguaje de programación Word Basic[®].

Su principal punto fuerte fue que terminaron con un paradigma de la seguridad informática: “los únicos archivos que pueden infectarse son los ejecutables” y todas las tecnologías antivirus sucumbieron ante este nuevo ataque.

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macrovirus.

Ejemplos:

De Microsoft Word: CAP I, CAP II, Concept, Wazzu.

De Microsoft Excel: Laroux.

De Lotus Amipro: GreenStripe

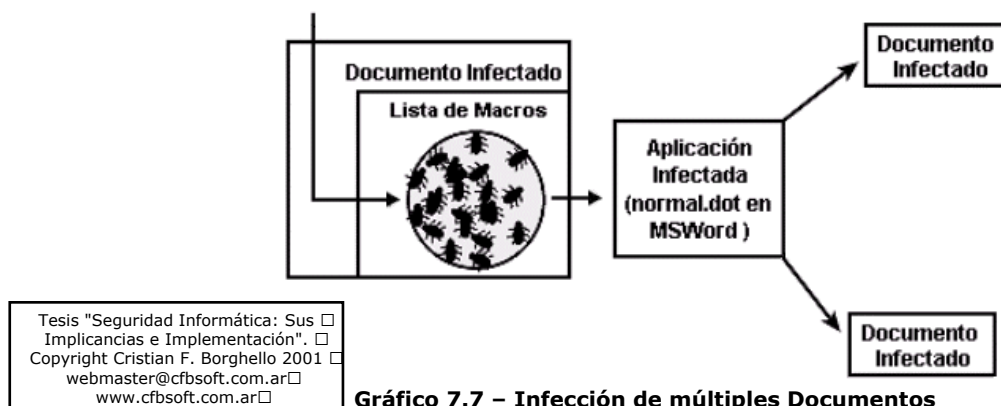


Gráfico 7.7 – Infección de múltiples Documentos

7.5.4.2.5 Virus de Mail

El “último grito de la tecnología” en cuestión de virus. Su modo de actuar, al igual que los anteriores, se basa en la confianza excesiva por parte del usuario: a este le llega vía mail un mensaje con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

Este tipo de virus tomó relevancia estos últimos años con la explosión masiva de Internet y últimamente con el virus Melissa y I Love You. Generalmente estos virus se auto envían a algunas de las direcciones de la libreta. Cada vez que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.

7.5.4.2.6 Virus de Sabotaje

Son virus contruidos para sabotear un sistema o entorno específico. Requieren de conocimientos de programación pero también una acción de inteligencia que provea información sobre el objetivo y sus sistemas.

7.5.4.2.7 Hoax, los Virus Fantasma

El auge del correo electrónico generó la posibilidad de transmitir mensajes de alerta de seguridad. Así comenzaron a circular mensajes de distinta índole (virus, cadenas solidarias, beneficios, catástrofes, etc.) de casos inexistentes. Los objetivos de estas alertas pueden causar alarma, la pérdida de tiempo, el robo de direcciones de correo y la saturación de los servidores con las consecuentes pérdidas de dinero que esto ocasiona.

7.5.4.2.8 Virus de Applets Java y Controles ActiveX

Si bien, como ya se comentó, estas dos tecnologías han sido desarrolladas teniendo como meta principal la seguridad, la práctica demuestra que es posible programar virus sobre ellas. Este tipo de virus se copian y se ejecutan a sí mismos mientras el usuario mantiene una conexión a Internet.

7.5.4.2.9 Reproductores–Gusanos

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

7.5.4.2.10 Caballos de Troya

Tesis "Seguridad Informática: Sus
Implicancias e Implementación".
Copyright Cristian F. Borghello 2001
webmaster@cfbsoft.com.ar
www.cfbsoft.com.ar

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocía, y que tenía una función muy diferente a la que ellos podían imaginar; un Caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

Si bien este tipo de programas NO cumplen con la condición de auto-reproducción de los virus, encuadran perfectamente en las características de programa dañino.

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

Los ejemplos más conocidos de troyanos son el Back Orifice y el Net Bus que, si bien no fueron desarrollados con ese fin, son una poderosa arma para tomar el control de la computadora infectada. Estos programas pueden ser utilizados para la administración total del sistema atacado por parte de un tercero, con los mismos permisos y restricciones que el usuario de la misma.

7.5.4.2.11 Bombas Lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada o dado algún evento particular en el sistema, bien destruye y modifica la información o provoca la baja del sistema.

7.5.4.3 MODELO DE VIRUS INFORMÁTICO

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

1. **Módulo de Reproducción:** es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticamente, permitiendo su transferencia a otras computadoras.
2. **Módulo de Ataque:** Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.
3. **Módulo de Defensa:** Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus.

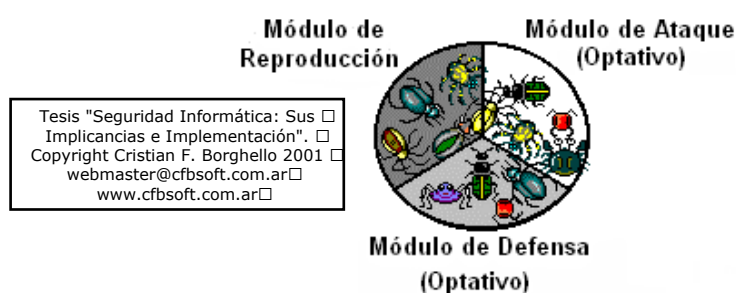


Gráfico 7.8 – Módulos de los Virus Informáticos

7.5.5 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS

Los virus informáticos no afectan (en su gran mayoría) directamente el hardware sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la siguiente clasificación se ha tenido en cuenta que el daño es una acción de la computadora, no deseada por el usuario:

- a. **Daño Implícito:** es el conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar su accionar y propagación. Aquí se debe considerar el

entorno en el que se desenvuelve el virus ya que el consumo de ciclos de reloj en un medio delicado (como un aparato biomédico) puede causar un gran daño.

- b. **Daño Explícito:** es el que produce la rutina de daño del virus.

Con respecto al modo y cantidad de daño, encontramos:

- a. **Daños triviales:** daños que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario. Deshacerse del virus implica, generalmente, muy poco tiempo.
- b. **Daños menores:** daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos. En el peor de los casos se tendrá que reinstalar las aplicaciones afectadas.
- c. **Daños moderados:** los daños que el virus provoca son formatear el disco rígido o sobrescribir parte del mismo. Para solucionar esto se deberá utilizar la última copia de seguridad que se ha hecho y reinstalar el sistema operativo.
- d. **Daños mayores:** algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad también infectadas. Puede que se llegue a encontrar una copia de seguridad no infectada, pero será tan antigua que se haya perdido una gran cantidad de archivos que fueron creados con posterioridad.
- e. **Daños severos:** los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No se sabe cuando los datos son correctos o han cambiado, pues no hay unos indicios claros de cuando se ha infectado el sistema.
- f. **Daños ilimitados:** el virus “abre puertas” del sistema a personas no autorizadas. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en el sistema.

7.5.6 LOS AUTORES

Tesis "Seguridad Informática: Sus Implicancias e Implementación". □ Copyright Cristian F. Borghello 2001 □ webmaster@cfbsoft.com.ar □ www.cfbsoft.com.ar □
--

Tras su alias (nic), los creadores de virus sostienen que persiguen un fin educacional para ilustrar las flaquezas de los sistemas a los que atacan. Pero... ¿es necesario crear un problema para mostrar otro?.

La creación de virus no es ilegal, y probablemente no debería serlo: cualquiera es dueño de crear un virus siempre y cuando lo guarde para sí. Infectar a otras computadoras sin el consentimiento de sus usuarios es inaceptable, esto sí es un delito y debería ser penado, como ya lo es en algunos países.

Inglaterra pudo condenar a ¡18 meses! de prisión al autor de SMEG. Sin embargo, el autor del virus Loverletter no fue sentenciado porque la legislación vigente en Filipinas (su país de origen) no era adecuada en el momento del arresto.

Existen otros casos en que el creador es recompensado con una oferta de trabajo millonaria por parte de multinacionales. Este, y no las condenas, es el mensaje que reciben miles de jóvenes para empezar o continuar desarrollando virus y esto se transforma en una “actividad de moda”, lejos de la informática ética sobre la cual deberían ser educados.

7.5.7 PROGRAMA ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Actualmente existen técnicas, conocidas como heurísticas, que brindan una forma de “adelantarse” a los nuevos virus. Con esta técnica el antivirus es capaz de analizar archivos y documentos y detectar actividades sospechosas. Esta posibilidad puede ser explotada gracias a que de los 6–20 nuevos virus diarios, sólo aparecen unos cinco totalmente novedosos al año.

Debe tenerse en cuenta que:

- Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.
- No será eficaz el 100% de los casos, no existe la protección total y definitiva.

Las funciones presentes en un antivirus son:

1. **Detección:** se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
2. **Identificación de un virus:** existen diversas técnicas para realizar esta acción:
 - a. **Scanning:** técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos del antivirus. Su principal ventaja reside en la rápida y exacta que resulta la identificación del virus. En los primeros tiempos (cuando los virus no eran tantos ni su dispersión era tan rápida), esta técnica fue eficaz, luego se comenzaron a notar sus deficiencias. El primer punto desfavorable es que brinda una solución a posteriori y es necesario que el virus alcance un grado de dispersión considerable para que llegue a mano de los investigadores y estos lo incorporen a su base de datos (este proceso puede demorar desde uno a tres meses). Este modelo reactivo jamás constituirá una solución definitiva.
 - b. **Heurística:** búsqueda de acciones potencialmente dañinas perteneciente a un virus informático. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controlada por el usuario (MBR, Boot Sector, FAT, y otras). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a las base de datos de los antivirus (técnica proactiva). Su desventaja radica en que puede “sospechar” de demasiadas cosas y el usuario debe ser medianamente capaz de identificar falsas alarmas.
3. **Chequeadores de Integridad:** Consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma. Su ventaja reside en la prevención aunque muchas veces pueden ser vulnerados por los

virus y ser desactivados por ellos, haciendo que el usuario se crea protegido, no siendo así.

Es importante diferenciar los términos **detectar**: determinación de la presencia de un virus e **identificar**: determinación de qué virus fue el detectado. Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

7.5.7.1 MODELO DE UN ANTIVIRUS

Un antivirus puede estar constituido por dos módulos principales y cada uno de ellos contener otros módulos.

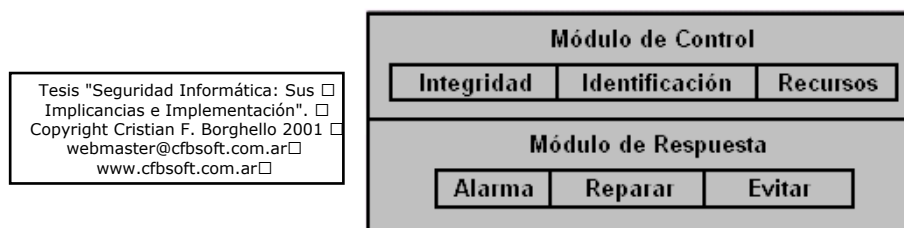


Gráfico 7.9 – Modelo de un Antivirus

- **Módulo de Control:** Este módulo posee la técnica de Verificación de Integridad que posibilita el registro de posibles cambios en las zonas y archivos considerados de riesgo.
- **Módulo de Respuesta:** La función de “Alarma” se encuentra en todos los antivirus y consiste en detener la ejecución de todos los programas e informar al usuario de la posible existencia de un virus. La mayoría ofrecen la posibilidad de su erradicación si la identificación ha sido positiva.

7.5.7.2 UTILIZACIÓN DE LOS ANTIVIRUS

Como ya se ha descrito un VI es un programa y, como tal se ejecuta, ocupa un espacio en memoria y realiza las tareas para las que ha sido programado. En el caso de instalarse un antivirus en una computadora infectada, es probable que este también sea infectado y su funcionamiento deje de ser confiable. Por lo tanto si se sospecha de la infección de una computadora, nunca deben realizarse operaciones de instalación o desinfección desde la misma. El procedimiento adecuado sería reiniciar el sistema y proceder a la limpieza desde un sistema limpio y seguro.

La mayoría de los antivirus ofrecen la opción de reparación de los archivos dañados. Puede considerarse este procedimiento o la de recuperar el/los archivos perdidos desde una copia de seguridad segura.

7.5.8 ASPECTOS JURÍDICOS SOBRE VIRUS INFORMÁTICOS

El análisis de la responsabilidad derivada de la difusión de un virus merece especial atención en estos momentos en que el uso de la redes telemáticas permite un mayor alcance de sus efectos. Prueba de ello tenemos en la reciente difusión por correo electrónico del antes mencionado virus “I Love you”.

Para analizar los diferentes supuestos que generan responsabilidad, debemos tener en cuenta los canales de difusión que contribuyen a potenciar el efecto pirámide en el que los virus basan su efectividad. En todos ellos es aplicable el régimen de la responsabilidad extracontractual establecida en el Código Civil (ver Anexo Leyes) que obliga a reparar los daños a quien, por acción u omisión, causa un perjuicio a otro, interviniendo la culpa o negligencia.

La mera creación de un virus puede obedecer a una intención distinta a la puesta en circulación. Cabe recordar aquí la diferencia que hacen los Hackers entre el creador de un virus y el diseminador del mismo.

En cuanto a la puesta en circulación es difícil obtener una identificación plena del responsable de la misma. Aunque en el caso de redes telemáticas es posible encontrar rastros de la primera aparición del virus, es posible alterar esa información. En cualquier caso, la responsabilidad de la persona que inicia la cadena de efectos nocivos de un virus, planificando la difusión intencionada del mismo a través de un medio está clara, pues el daño es perfectamente previsible (aunque no su magnitud) y seguro.

En cuanto a la introducción intencionada en un sistema específico, por su tipificación como delito de daños, los actos de sabotaje informático pueden generar responsabilidad civil y penal. Pueden tener su origen en personas del interior de la empresa que por un motivo como, por ejemplo, la ruptura de la relación laboral, deciden causar un daño, o en personas del exterior de la empresa, que acceden al sistema informático por medios telemáticos, por ejemplo. En ambos casos se cumplen los requisitos para reclamar una indemnización.

Como ya se ha mencionado, en Argentina, la Información no es considerada un bien o propiedad. Según el Art. 183 del Código Penal “...se castiga al que dañe una cosa, inmueble o animal”. Hasta el momento de la realización del presente este castigo sólo es teórico, ya que en la práctica no existen casos en donde se haya podido probar la culpa de un creador o diseminador de virus dañando una “cosa, inmueble o animal”.

La difusión de un virus entre usuarios de sistemas informáticos puede ser debida a una conducta negligente o la difusión de virus no catalogados. La diligencia debida en el tratamiento de la información obliga a realizar copias de seguridad y a instalar sistemas de detección de virus. En el caso de archivos que se envían a otros usuarios, la ausencia de control previo puede ser calificado como negligente, puesto que el riesgo de destrucción de datos se está traspasando a terceros y ello podía haberse evitado de una manera sencilla y económica. Pero también puede alegarse que el usuario receptor del archivo afectado podría haber evitado el daño pasando el correspondiente antivirus, a lo que cabe replicar que este trámite se obvió por tratarse de un remitente que ofrecía confianza.

Por último, en algunos países en donde se han tratado Leyes de Propiedad Intelectual, se establece la exclusión de los VI de las creaciones protegidas por el derecho de autor. El objetivo de este precepto es facilitar las actividades de análisis necesarias para la creación de un antivirus, aunque esto resulta innecesario por la sencilla razón de que el creador de un virus no acostumbra a reclamar la titularidad del mismo de forma pública.

7.5.9 CONSEJOS

Tesis "Seguridad Informática: Sus ☐
Implicancias e Implementación". ☐
Copyright Cristian F. Borghello 2001 ☐
webmaster@cfbsoft.com.ar ☐
www.cfbsoft.com.ar ☐

Aunque existe una relativa concientización, generalmente no se toman todas las precauciones necesarias para anular el peligro. No basta con tener un antivirus, sino que éste hay que actualizarlo periódicamente para contemplar los nuevos virus que van apareciendo.

Además de poseer la cualidad de chequeo manual, detección y eliminación, debe ser sobre todo capaz de actuar como vacuna o filtro, impidiendo la entrada de los nuevos virus que aparecen cada día. De esta forma, aunque al usuario se le olvide pasar el antivirus, sabe que al menos existe una protección automática. La mayoría de los antivirus que se comercializan poseen estas características.

En la Campaña Nacional Antivirus Informáticos se proponen 15 consejos para evitar el contagio de virus²². A continuación se resumen todas ellas:

- I. Instalar un buen antivirus para la detección y eliminación de nuevos virus. Además es necesario actualizarlo frecuentemente. Como ya se ha explicado la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización (preferentemente diaria).
- II. Comprobar que el antivirus elegido incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta, bien a través de correo electrónico, por teléfono o fax.
- III. Asegurarse que el antivirus esté siempre activo vigilando constantemente todas las operaciones realizadas en el sistema.
- IV. Verificar, antes de abrir, cada nuevo mensaje de correo electrónico recibido. Este medio es el medio de transmisión preferido por los diseminadores de virus. Cualquier correo puede contener virus, aunque no este acompañado de archivos adjuntos. Además no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado, en algunos sistemas basta únicamente con abrir el mensaje. Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual.
- V. Evitar la descarga de programas de lugares no seguros o pocos fiables de Internet. Muchas páginas web permiten la descarga de programas y archivos cabiendo la posibilidad que estos archivos estén infectados. Son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen.
- VI. Rechazar archivos que no se hayan solicitado cuando se esté en chats o grupos de noticias. Hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.
- VII. Analizar siempre con un buen antivirus los disquetes que entran y salen de la computadora. Si se utilizan disquetes propios en otros lugares es aconsejable protegerlos contra escritura.
- VIII. Retirar los disquetes de las disqueteras al apagar o reiniciar el ordenador. Esta tarea es para evitar que se activen los virus de arranque.
- IX. Analizar el contenido de los archivos comprimidos. El antivirus deberá de contar con una funcionalidad que permita detectar el mayor número de formatos comprimidos posibles. Además, antes de abrir uno de estos archivos, es aconsejable guardarlos en carpetas temporales.
- X. Mantenerse alerta ante acciones sospechosas de posibles virus. Hay varios síntomas que pueden delatar la presencia de nuevos virus: aumento del tamaño de los archivos, aviso de macros en documentos, ralentización en ciertos procesos, etc. Como mejor solución a estas sospechas de posibles infecciones, se debe recurrir al servicio de resolución urgente de nuevos virus de la compañía antivirus.

²² Para más información referirse a <http://www.sinvirus.com>

- XI. Añadir las opciones de seguridad de las aplicaciones que se utilizan normalmente en la política de protección antivirus, ya que los programas informáticos más utilizados se convierten, precisamente por esta razón, en blanco de los autores de virus.
- XII. Realizar copias de seguridad frecuentes y periódicas de la información más importante. Esta es una muy buena forma de minimizar el impacto de un virus. De esta manera, una pérdida de datos, causada por un virus, puede ser superada mediante la restauración de la última copia.
- XIII. Ante la gran cantidad de información recibida por diferentes medios, es aconsejable contrastar estos datos con la información completa, actualizada y experta difundida por determinadas compañías y organismos confiables.
- XIV. A la hora de instalar nuevos programas, el riesgo de infección es menor (aunque no nulo) si se trata de software legal. Si el software ha llegado de fuentes piratas nadie puede asegurar que esté libre de virus.
- XV. Exigir a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus. En la lucha contra los virus es precisa la participación de todos los agentes implicados en el sector informático para minimizar el problema de las infecciones provocadas.

AMENAZAS LÓGICAS	1
7.1 ACCESO – USO – AUTORIZACIÓN.....	2
7.2 DETECCIÓN DE INTRUSOS	2
7.3 IDENTIFICACIÓN DE LAS AMENAZAS.....	3
7.4 TIPOS DE ATAQUE	6
7.4.1 INGENIERA SOCIAL	7
7.4.2 INGENIERÍA SOCIAL INVERSA	7
7.4.3 TRASHING (CARTONEO).....	8
7.4.4 ATAQUES DE MONITORIZACIÓN.....	8
7.4.4.1 <i>Shoulder Surfing</i>	8
7.4.4.2 <i>Decoy (Señuelos)</i>	8
7.4.4.3 <i>Scanning (Búsqueda)</i>	9
7.4.4.4 <i>Eavesdropping–Packet Sniffing</i>	11
7.4.4.5 <i>Snooping–Downloading</i>	12
7.4.5 ATAQUES DE AUTENTIFICACIÓN.....	12
7.4.5.1 <i>Spoofing–Looping</i>	12
7.4.5.2 <i>Spoofing</i>	13
7.4.5.3 <i>Web Spoofing</i>	14
7.4.5.4 <i>IP Splicing–Hijacking</i>	14
7.4.5.5 <i>Utilización de BackDoors</i>	15
7.4.5.6 <i>Utilización de Exploits</i>	15
7.4.5.7 <i>Obtención de Passwords</i>	16
7.4.6 DENIAL OF SERVICE (DOS).....	17
7.4.6.1 <i>Jamming o Flooding</i>	17
7.4.6.2 <i>Syn Flood</i>	18
7.4.6.3 <i>Connection Flood</i>	18
7.4.6.4 <i>Net Flood</i>	19
7.4.6.5 <i>Land Attack</i>	19
7.4.6.6 <i>Smurf o Broadcast Storm</i>	19

7.4.6.7 <i>OOB, Supernuke o Winnuke</i>	20
7.4.6.8 <i>Teardrop I y II–Newtear–Bonk-Boink</i>	21
7.4.7 ATAQUES DE MODIFICACIÓN–DAÑO	21
7.4.7.1 <i>Tampering o Data Diddling</i>	21
7.4.7.2 <i>Borrado de Huellas</i>	22
7.4.7.3 <i>Ataques Mediante Java Applets</i>	22
7.4.7.4 <i>Ataques Mediante JavaScript y VBScript</i>	23
7.4.7.5 <i>Ataques Mediante ActiveX</i>	23
7.4.7.6 <i>Vulnerabilidades en los Navegadores</i>	24
7.4.8 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN	24
7.4.9 IMPLEMENTACIÓN DE ESTAS TÉCNICAS.....	25
7.4.10 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?	26
7.5 CREACIÓN Y DIFUSIÓN DE VIRUS	27
7.5.1 VIRUS INFORMÁTICOS VS VIRUS BIOLÓGICOS	27
7.5.2 ORIGEN	28
7.5.3 LOS NÚMEROS HABLAN	30
7.5.4 DESCRIPCIÓN DE UN VIRUS.....	31
7.5.4.1 <i>Técnicas de Propagación</i>	31
7.5.4.2 <i>Tipos de Virus</i>	32
7.5.4.3 <i>Modelo de Virus Informático</i>	36
7.5.5 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS	36
7.5.6 LOS AUTORES	37
7.5.7 PROGRAMA ANTIVIRUS	38
7.5.7.1 <i>Modelo de un Antivirus</i>	39
7.5.7.2 <i>Utilización de los Antivirus</i>	39
7.5.8 ASPECTOS JURÍDICOS SOBRE VIRUS INFORMÁTICOS	40
7.5.9 CONSEJOS	41