FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

CURSOS A DISTANTANCIA

SEGURIDAD EN LA OPERACIÓN DE REDES DE DATOS

DEL 30 DE NOVIEMBRE AL 4 DE DICIEMBRE DE 1998

CLAVE (CA 172)

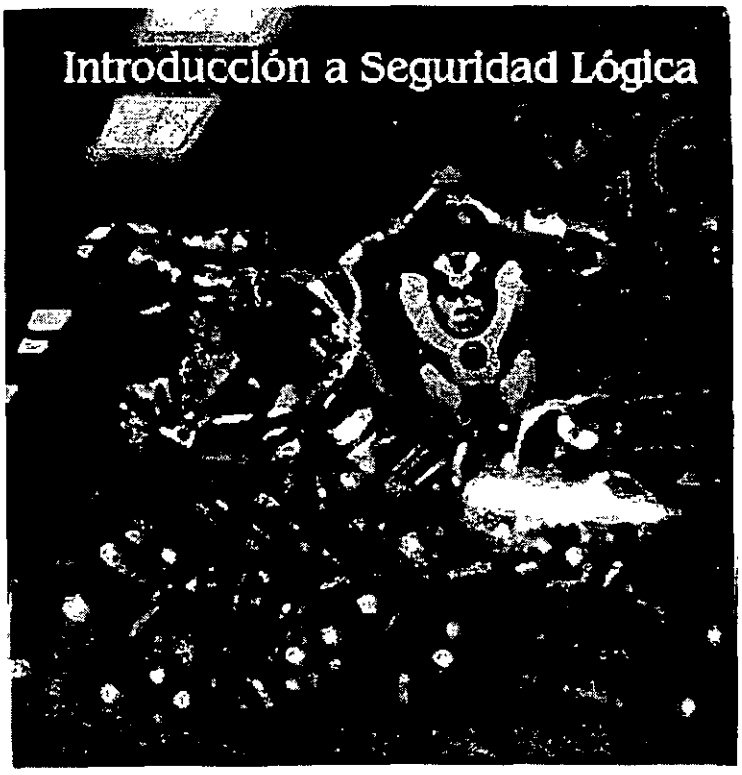
PROFESOR:

ING. JAMES PATRICK KELLEGHAN MONGE.

Palacio de Mineria Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F APDO Postal M-2285
Teléfonos. 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

ING. JAMES PATRICK KELLEGHAN MONGE.

Seguridad en la operación de Redes de Datos



Noviembre 1998

Seguridad

Introducción

Los dos motivos más comunes que causan violaciones de seguridad:

- Configuración errónea del host de la víctima.
- Fallas en los sistemas o deficiencia en la respuesta del fabricante.

Estados de inseguridad de software:

Activo

Primordialmente afecta software de red. Muchos servicios que son habilitados por default representan graves riesgos, por ejemplo impresión en red, compartir archivos, passwords por omisión, código de red muestra, etc.

Pasivo

Mecanismos de seguridad del sistema operativo no habilitados (como por ejemplo logs) o aquellos habilitados pero poco prácticos como seguridad avanzada de archivos.

Educación sobre seguridad

Tradicionalmente es un tema controlado por expertos.

¿Los usuarios deben de ser educados?

Sector Corporativo

Haciendo a un lado el espionaje industrial, el principal problema es costo.

Coso de licencia de Bases de Datos, programación, mantenimiento, actualizaciones, etc.

Al conectarse a la red, el número de atacantes potenciales crece de pocos a incontables.

El número de pasos utilizado para accesar la Base de Datos desde HTML implica un enorme peligro.

Gobierno

El folklore indica que el personal de Gobierno sabe mas sobre seguridad.

La sensibilidad de la información contenida en sus Bases de Datos es enorme.

Sistemas Operativos

UNIX, VMS y los operativos de IBM tienen más agujeros de seguridad que las Mac´s y las PC´s.

Los agujeros de Mac y PC son considerablemente mas difíciles de tapar.

Es más fácil hackear sistemas abiertos.

Objetivos del Curso

Al administrador de Sistemas: Asistir en defender su red aprendiendo como atacar y defenderse en situaciones reales.

Al Hacker: Conocimiento general de las herramientas disponibles en la red.

Al Craker: Ahorro en tiempo de investigación.

Al negociante: Ahorro al contratar asesores.

Al usuario.- Como evitar ser atacado

Hackers y Crackers

Un Hacker es una persona con un intenso interés en las operaciones arcanas y recónditas de los sistemas operativos. Generalmente son programadores y obtienen conocimientos avanzados de los sistemas operativos y lenguajes. Conocen los agujeros y los motivos por los que existen. Siempre buscan mas conocimiento, comparten sus conocimientos y nunca dañan datos intencionalmente.

Un Craker es una persona que viola un sistema con intención maliciosa. Destruyen datos, niegan servicio o causan problemas.

Mixtos. El caso de Randal Schwartz cocreador de Perl y arrestado por violar el sistema de seguridad de Intel mientras trabajaba para ellos

como especialista en seguridad.
(http://www.lightlink.com/spacenka/fors/intro.html)

Historia del Hackeo

Phreaks de los '50s.

Roja	simular el sonido de monedas cayendo en un teléfono (3.57954MHz)
Azul	generar un tono de 2600MHz, adquiriendo una troncal y otorgando privilegios de operador
Dayglo	utilizar la línea de un vecino
Aqua	drenar el voltaje de una línea
Malva	intervenir una línea

Jueves Negro: Noviembre 3 de 1988

Los administradores encontraron que sus equipos tenían una carga de trabajo gigantesca. Cientos de procesos shell se estaban ejecutando y se creaban nuevos y más rápido de lo que se les podía matar.

El programa fue lanzado por Robert Morris Jr. Como un experimento que fallo. Causo que la mayoría de los sistemas a nivel mundial se cayeran o se volvieran catatónicos. Denominado Gusano de Morris. Demostró la vulnerabilidad de la red.

La situación actual es una red en guerra.

Hackers famosos

Richard Stallman, fundador del Free Software Foundation

Dennis Ritchie, Ken Thompson, Brian Kernigan. Programadores de Bell Labs, creadores de UNIX y C. Trabajando en Plan 9.

Paul Baran, Rand Corporation. Hackeo el concepto de Internet. Su trabajo es la base de la teoría de seguridad moderna.

Eugene Spafford, Investigador de Purdue University. Creador de COPS (Computer Oracle Password and Security System) sistema semi automatizado de seguridad.

Dan Farmer de Carnegie Mellon, cocreador de COPS y creador de SATAN (System Administrator Tool for Analyzing Networks)

Wieste Venema de Eidenhoven University of Technology. Coautor de SATAN y creador TCP Wrapper.

Linus Torvalds. Tomo clases de UNIX y Programación C a principios de los 90's. Un Año después liberó Linux.

Bill Gates y Paul Allen.

Crackers famosos

Kevin Mitnik, conocido como Cóndor comenzó con phreak. Ha violado... todo. Actualmente en la cárcel.

Kevin Poulsen, violador de sistemas de telefonía y de defensa. Encarcelado y liberado en 1996. Aparentemente reformado.

Justin Tanner Peterson, Agent Steal. Hackeo el sistema VISA en múltiples ocasiones. Actualmente encarcelado.

Referencias:

Security requirenments for Automated Information Systems:
http://140.229.1.16:9000/htdocs/directives/soft/5200.28.html

DoD Evaluated Products List:
http://www.radium.ncsc.mil/tcpip/epl/index.html

Correos Anónimos: http://www.well.com/user/abacard/remail.html

Firmas digitales en contenido activo:
http://www.packet.com/packet/garfinkel

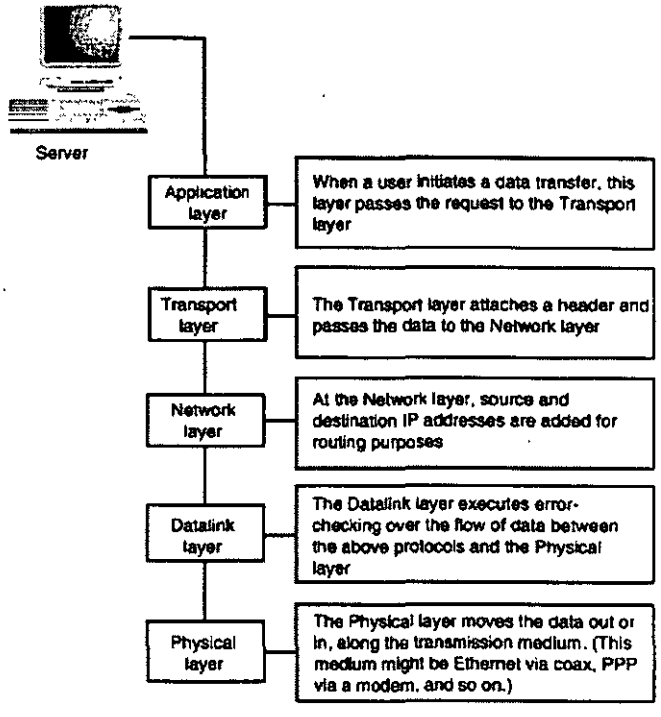
Principios de TCP/IP

Funcionamiento

Plataformas Soportadas

Plataforma	Soporte TCP/IP
UNIX	Nativo
DOS	Piper/IP por Ppswitch
Windows	TCPMAN por Trumpet Software
Windows 95	Nativo
Windows NT	Nativo
Macintosh	MacTCP o OpenTransport(Sys 7.5+)
OS/2	Nativo
AS/400 OS/400	Nativo

Funcionamiento



Protocolos de Red

ARP (Address Resolution Protocol)

Mapea direcciones de Internet en direcciones físicas

Se envía la solicitud de ARP como broadcast a la subred. El ruteador la recibe y contesta con la dirección solicitada

Ver: http://www.freesoft.org/Connected/RFC/826 y

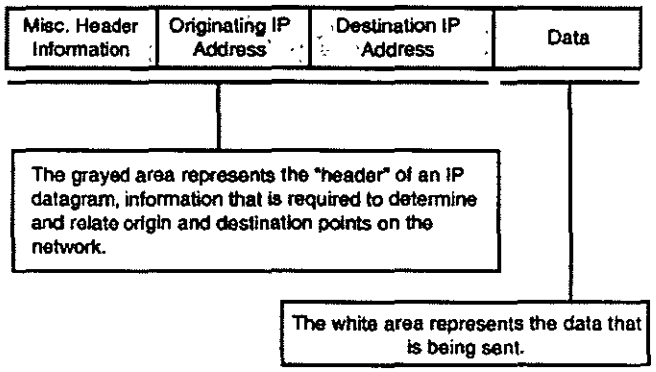
http://www.alexia.net.au/~www/vendor/internetinfo/index.html

ICMP (Internet Control Message Protocol)

Maneja errores y mensajes de control entre dos o más computadoras durante la transferencia de datos.

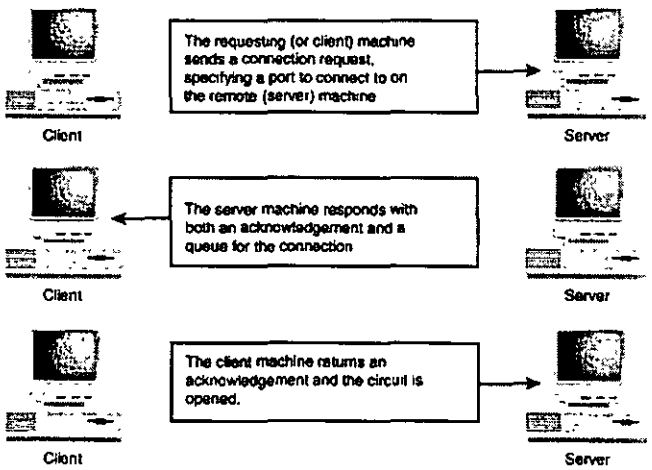
http://sunsite.auc.dk/RFC/rfc/rfc792.html

IP (Internet Protocol)



http://sunsite.auc.dk/RFC/rfc/rfc760.html

TCP (Transmission Control Protocol)



Telnet, FTP, SMTP, Gopher, HTTP y NNTP

http://sunsite.auc.dk/RFC/rfc/rfc792.html

http://www.freesoft.org/Connected/RFC/959/index.html

http://sunsite.auc.dk/RFC/rfc/rfc821.html

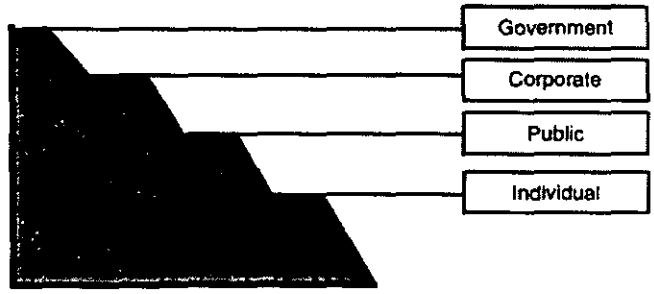
http://sunsite.auc.dk/RFC/rfc/rfc1436.html

ftp://ds.internic.net/rfc/rfc2068.txt

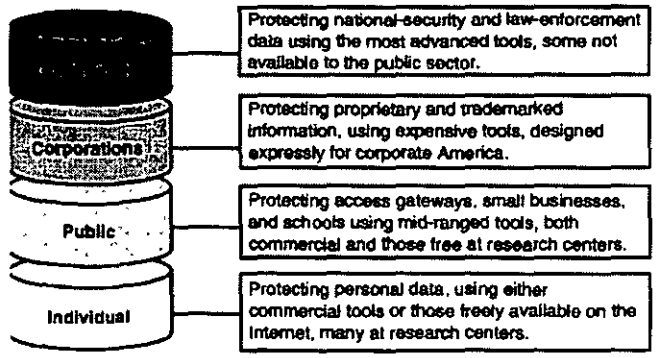
http://sunsite.auc.dk/RFC/rfc/rfc850.html

La Guerra en Internet

Niveles de Tecnología



Level of Technology in Internet Warfare



Guerra entre individuos

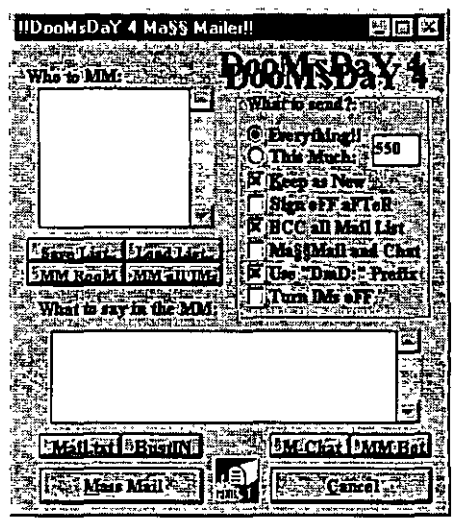
Bomba de Correo

Consta de reenviar el mismo mensaje a un individuo miles de veces.

Ejemplos: MailBomber (bomb02.zip)

Y

Doomsday:



Ligado a Listas

Consta en ligar a usuarios a múltiples listas de Correo.

Ej.: El 18 de marzo de 1996 Time público un incidente en el que el Presidente de EEUU, editores de dos revistas de computación, un editor de Time y un Senador americano fueron ligados a listas.

Utileriás de IRC

Diseñadas para eliminar a un usuario de un Chat.

Ver (flash.c, flash.c.gz, flash.gz y megaflash.

Virus y Troyanos

¿Qué es un Virus?

¿Qué es un Troyano?

¿Qué es un Gusano?

Guerra a Proveedores de Internet

Son los segundos más susceptibles a ataques después de las Universidades.

Utilizan utilerías defensivas basadas en bitácoras como:

Utilería	Función
L5	Analiza directorios en UNIX o DOS, guardando información sobre archivos. Se utiliza para determinar cambios en la estructura de los directorios.
Clog	Escucha puertos para tratar de determinar si Hackers externos están intentando buscar agujeros.
LogCheck	Automatiza el análisis de bitácoras para determinar si ha sucedido una violación
Netlog	Escucha y graba transacciones de TCP/IP sospechosas
DumpACL	Utilería de NT que formatea información de control importante para poderla leer.

Referencias

Ver: http://www.fas.org/irp/wwwinfo.html

Herramientas

Scanners

Se dice que un analizador de puertos vale mas que mil passwords de usuarios!

Un escáner es un programa que automatiza el proceso de encontrar debilidades en una máquina remota.

Logran esto atacando los puertos y servicios de TCP/Ip grabando la respuesta de la víctima. De esta manera se obtiene información valiosa sobre el host.

Otros escanners son utilerías de UNIX como: rusers, hosts y finger-.

Aunque estas herramientas son mas comunes en UNIX, están empezando a aparecer en NT.

Como requerimientos, se recomienda un sistema operativo de 32 bits (preferiblemente un UNIX) con una conexión de mínimo 28.8 Kbaud, 32Mbytes de RAM.

Para escribir un Escáner se necesitan conocimientos a profundidad de TCP/IP.

C.f.: http://tecstar.cv.com/~dan/tec/primer/socket_programming.html

Y http://149.17.36.24/prog/sockets.html

Un escáner revela debilidades inherentes el host atacado. Para poderlos aprovechar sin embargo, se debe ser capaz de reconocer el agujero. El escáner no da instrucciones de cómo explotar lo encontrado ni el grado en que el proceso de análisis ha sido registrado.

Para poder explotar la información obtenida es necesario reconocer los agujeros. Ver:

Recurso	Lista
Lista de Firewalls	Firewalls@GreatCircle.COM
Lista de Sneakers	Sneakers@CS.Yale.EDU
Lista de seguridad de WWW	WWW-security@ns2.rutgers.edu
Lista de seguridad NT	Ntsecurity@ISS
Bugtraq	BUGTRAQ@NETSPACE.ORG

Para instrucciones de suscripción, y otras listas ver:

http://www.cs.purdue.edu/coast/hotlist/

El funcionamiento es similar al de un WarDialer.

Ejemplo:

En 1995, Silicon Graphics liberó el modelo WebForce.

WebForce corre sobre IRIX el cual, en algunas versiones asigna un password en blanco a la cuenta lp.

Para explotar el agujero, un Craker entraba a la cuenta, ejecutaba:

cat /etc/password

Y cat /etc/shadow

Copiaba el contenido de las pantallas con cortar y pegar a un archivo local y corría un password Craker.

Para encontrar modelos WebForce basto con buscar un archivo común en los directorios de FTP de estos modelos. A decir, se corría una búsqueda en Excite con la cadena:

EzSetup + root: lp:

Esto retornaba un lista de servidores WebForce.

Otro mecanismo utilizado fue usar un escáner para iniciar secciones Telnet en un rango de direcciones IP y grabar las pantallas de saludo en un archivo para análisis posterior.

Para determinar quien fue la última persona en explotar este agujero en una SGI, corra finger lp@the.sgi.box.

Otro ejemplo

Si se corre el comando host –l –v –t any bu.edu

Obtendrá un listado similar al siguiente:

Found 1 addresses for BU.EDU

Found 1 addresses for RS0.INTERNIC.NET

Found 1 addresses for SOFTWARE.BU.EDU

Found 5 addresses for RS.INTERNIC.NET

Found 1 addresses for NSEGC.BU.EDU

Trying 128.197.27.7

bu.edu 86400 IN SOA BU.EDU HOSTMASTER.BU.EDU(

961112121 ;serial (versión)

900 ;refresh period

900 ;retry refresh this often

604800 ;expiration period

86400 ;minimum TTL

)

bu.edu 86400 IN NS SOFTWARE.BU.EDU

bu.edu 86400 IN NS RS.INTERNIC.NET

bu.edu 86400 IN NS NSEGC.BU.EDU

bu.edu 86400 IN A 128.197.27.7

Hasta aquí, no se obtiene más información de lo que se puede encontrar con WHOIS.

bu.edu 86400 IN HINFO SUN-SPARCSTATION-10/41 UNIX

PPP-77-25.bu.edu 86400 IN A 128.197.7.237

PPP-77-25.bu.edu 86400 IN HINFO PPP-HOST PPP-SW

PPP-77-26.bu.edu 86400 IN A 128.197.7.238

PPP-77-26.bu.edu 86400 IN HINFO PPP-HOST PPP-SW

ODIE.bu.edu 86400 IN A 128.197.10.52

ODIE.bu.edu 86400 IN MX 10 CS.BU.EDU

ODIE.bu.edu 86400 IN HINFO DEC-ALPHA-3000/300LX OSF1

Aquí se nos indica que se trata de una DEC Aplpha corriendo OSF1 (`ODIE.bu.edu`).

STRAUSS.bu.edu 86400 IN HINFO PC-PENTIUM DOS/WINDOWS

BURULLUS.bu.edu 86400 IN HINFO SUN-3/50 UNIX (Ouch)

GEORGETOWN.bu.edu 86400 IN HINFO MACINTOSH MAC-OS

CHEEZWIZ.bu.edu 86400 IN HINFO SGI-INDIGO-2 UNIX

POLLUX.bu.edu 86400 IN HINFO SUN-4/20-SPARCSTATION-SLC UNIX

SFA109-PC201.bu.edu 86400 IN HINFO PC MS-DOS/WINDOWS

UH-PC002-CT.bu.edu 86400 IN HINFO PC-CLONE MS-DOS

SOFTWARE.bu.edu 86400 IN HINFO SUN-SPARCSTATION-10/30 UNIX

CABMAC.bu.edu 86400 IN HINFO MACINTOSH MAC-OS

VIDUAL.bu.edu 86400 IN HINFO SGI-INDY IRIX

KIOSK-GB.bu.edu 86400 IN HINFO GATORBOX GATORWARE

CLARINET.bu.edu 86400 IN HINFO VISUAL-X-19-TURBO X-SERVER

DUNCAN.bu.edu 86400 IN HINFO DEC-ALPHA-3000/400 OSF1

MILHOUSE.bu.edu 86400 IN HINFO VAXSTATION-II/GPX UNIX

PSY81-PC150.bu.edu 86400 IN HINFO PC WINDOWS-95

BUPHYC.bu.edu 86400 IN HINFO VAX-4000/300 OpenVMS

Hemos obtenido información crucial sobre todas las máquinas en un dominio. Ahora sabemos que:

ODIE.bu.edu puede ser susceptible a un ataque con: mount –d –s bug enviando dos llamadas iguales en un período muy corto de tiempo.

CHEEZEWIZ.bu.edu es susceptible a ataques de lp y Telnet, además del ataque montar un floppy en /usr/etc/msdos.

POLLUX.bu.ede es una máquina vieja, si reinstalaron SunOS 4.1 y no aplicaron el parche Patch-ID# 100376-01 puede ser posible explotarla a través de división de enteros.

PSY81-PC150.bu.edu corre bajo Windows95. Si el protocolo SMB está corriendo y hay directorios compartidos se puede ejecutar un attach en Linux para agregar esos directorios a nuestro File System. Adicionalmente, esta máquina tiene DCOM.

A través de herramientas como rusers, traceroute y finger se puede identificar a usuarios que desean permanecer anónimos.

Analizando los resultados de llamadas de finger a cuentas como lp, UUCP, root y mail se puede, con el tiempo construir una Base de Datos de relaciones de confianza entre máquina. Si una máquina que está altamente protegida se comunica cotidianamente con una que no, quizá valga la pena atacar a la no protegida para entrar desde ahí al equipo protegido.

Showmount –c nos indica todos los directorios exportables que quizá sean montables en una máquina remota.

Se pueden obtener herramientas en:

Win95

http://www.eskimo.com/~nwps/index.html

ftp://wuarchive.wurstl.edu/systems/ibmpc/win95/netutil/wssrv32n.zip

http://www.jriver.com/netbox.html

UNIX

Strobe

http://sunsite.kth.se/Linux/system/Network/admin

Es un escáner muy rápido diseñado para encontrar puertos abiertos en una máquina.

SATAN

Es la herramienta gratuita más poderosa existente.

http://www.fish.com

Nota: Tiene problemas para correr en LINUX. Para modificar el código, ver ftp://ftp.lod.com y ftp://sunsite.unc.edu/pub/Linux/system/Networks/admin/sata-linux.1.1.1.diff.gz

Jakal

Un stealth escáner que analiza puertos detrás de Firewalls utilizando llamadas SYN/ACK incompletas.

http://www.giga.or.at/pub/hacker/uniz

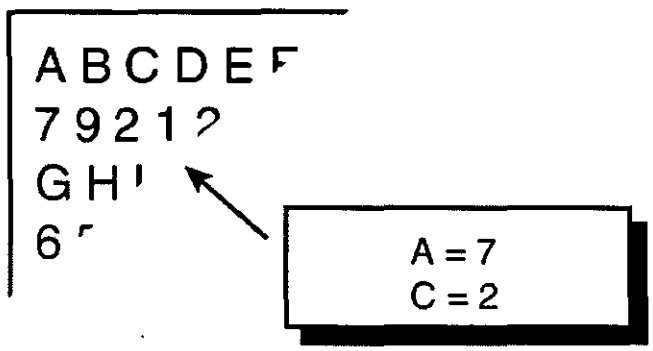
IdentTCPScan

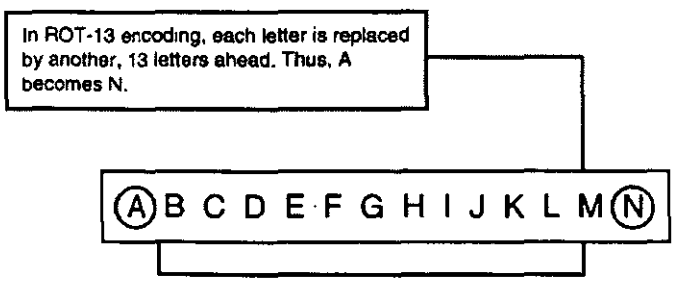
http://www.giga.or.at/pub/hacker/unix

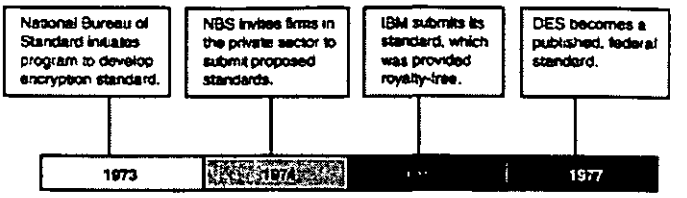
Identifica los dueños de los demonios de los diferentes puertos. Sis se determina, por ejemplo, que root es el dueño del puerto HTTP, se podría escribir un CGI que explote este hecho.

Crackers de Passwords

Los Crackers de passwords generan password según diferentes heurística y los comparan un archivo /etc/shadow.







Brief Timeline of the Data Encryption Standard Development

Para listas de palabras, ver:
http://sdg.ncsa.uiuc.edu/~mag/Misc/Wordlists.html y

http://www.cs.purdue.edu/coast

Crack

Correr una búsqueda sobre:

Crack-4.1.tar.gz o crack-4.1.tar.Z

Hades

Buscar hades.zip o hades.arj

Claymore para Windows

Ataque de fuerza bruta.

http://www.ilf.net/~toast/files/claym10.zip

Sniffers

Un sniffer es cualquier dispositivo que tome información que viaje a través de una red en cualquier protocolo (ethernet, TCP/IP, IPX, etc., o cualquier convinación). Su propósito es poner a la NIC en modo promiscuo y al hacerlo capturar todo el tráfico de la red.

El modo promiscuo se refiere al modo en el que todas las estaciones de una red, escuchan todo el tráfico y no únicamente el propio.

Un sniffer, no es más que un hardware o software que escucha todos los paquetes enviados por el cable. En este aspecto, cada máquina o ruteador es un sniffer en potencia. Para que una máquina sea un sniffer, se necesita o un controlador promiscuo o software de red que permita el modo promiscuo.

El sniffer se coloca dentro de un bloque de red o red de confianza.

Los sniffer fueron diseñados para diagnosticar conexiones de red. A diferencia de los escaners están diseñados para analizar los protocolos a profundidad.

Existen en todas las plataformas de red, es de esperarse que pronto empiecen a aparecer sniffers para Windows 95 escritos en Visual Basic.

La mayoría de los sniffers, afortunadamente son comerciales.

En febrero de 1994, una persona no identificada instaló en numerosos hosts y elementos de back bone en Internet y Milnet un sniffer. Recolectó más de 100,000 nombres de cuentas y passwords. Cualquier host que permita FTP, Telnet o Rlogin debe de considerarse comprometido

(c.f.: http://www.chpis.navy.mil/chips/archives/94_jul/file14.html)

Para más información sobre el incidente Stanislaos en la Universidad Estatal de California, ver http://yahi.csustan.edu/studnote.html) para información sobre el incidente en el campo de proyectiles de White Sands ver el reporte GAO en
http://www.securitymanagement.com/library/000215.html

Un ataque de snifffer no es tan fácil como parece requiere de conocimientos de redes para lanzarse efectivamente Una red pequeña puede generar miles de paquetes en una hora así que no se puede simplemente colocar un sniffer.

Normalmente, un sniffer solo registra los primeros 200 o 300 bytes de cada paquete, que usualmente contienen cuentas y passwords.

Gobbler

Corre en MSDOS y Win95

http://www.cse.rmit.edu.au/~rdssc/courses/ds738/watt/other/gobbler.zip

ETHLOAD

Escrito en C para tarjetas Novell ODI, 3Com/Microsoft Protocol Manager y PC/TCP/Clarkson/Crynwr para analizar TCP/IP, DECnet, OSI, XNS, NetWare y NetBEUI.

ftp://oak.oakland.edu/SimTel/msdos/lan/ethld104.zip

linux_siffer.c

Consiste de 175 líneas en C distribuida principalmente en sitios de hackers.

www.catch22.com/Twilight.NET/phuncnet/hacking/proggies/sniffers/

http://mygale.org/08/datskewl/elite/

La pregunta obvia en está etapa es como se detecta un sinffer. La respuesta corta, es que, dado que son dispositivos pasivos, no se pueden detectar.

Ocasionalmente la ejecución de comandos como ps –aux o ps –augx pueden funciona, otro mecanismo es similar al de las vacunas para procesos en memoria. Desafortunadamente si el sniffer es propietario o el comando ps ha sido víctima de un troyano la detección se vuele imposible.

La única manera de protegerse de un sniffer es la incripción.

Ataques destructivos

Bombas de Correo

Up Yours

Es el más popular y se puede encontrar buscando los comandos upyours.exe, upyours.zip o upyours3.zip. Si uno de estos tres archivos existe en la cuenta de un usuario, el usuario planea atacar.

KaBoom

Es bastante más sofisticado que el anterior. Entre otras cosas permite inscribir a la víctima a cientos de listas de correo. Se puede encontrar buscando kaboom!3.zip o kaboom3.exe.

Avalanche

Más amigable que kaboom y permite seleccionar las listas de correo. Sus firmas son alanch10.zip, avalache20.zip y avalanche.exe.

Unabomber

Herramienta simple y humorística que incluye archivo de ayuda. Sus firmas son unabomb.zip y unabomb.exe.

Negación de Servicio

Ping de la Muerte

Diseñado para matar servidores WinNt 3.51 que consta en mandar miles de paquetes grandes de ping.

Ver http://www.microsoft.com/kb/aticles/q132/4/70.htm para la solución.

Syn_Flooder

Utilería distribuida en lenguaje C utilizada para atacar servidores UNIX, que inunda a la máquina, creando conexiones medio abiertas y volviendo al servidor inoperable. Se considera una violación Federal con pena de cárcel en varios países del mundo.

DNSKiller

Rutina en C para Linux diseñada para matar servidores DNS WinNT 4.0.

arnudp100.c

Falsifica la dirección IP de paquetes.UDP creando negación de servicio en los puertos 7, 13,19 y 37 (ruteo).

c.f.: http://cio.cisco.com/warp/public/707/3.html

Agujeros

Escala de vulnerabilidad

Existen agujeros que permiten negación de servicio, acceso con privilegios limitados para incrementar privilegios sin autorización, accesos no autorizados, etc.

Por su seriedad se clasifican en :

A) Agujeros que pueden dañar potencialmente el sistema completo, permitiendo acceso ilimitado a personas fuera de la red.

B) Agujeros que permiten a usuarios locales acceso incrementado y tomar control del sistema.

C) Agujeros que permiten a cualquier usuario interrumpir, degradar o interferir con la operación del sistema.

Los agujeros de clase C son de baja prioridad. Casi siempre se basan en el sistema operativo, es decir existen dentro de las porciones de red del sistema operativo. Generalmente sólo pueden ser arreglados por el fabricante.

Un ejemplo simple de un ataque de negación de servicio de este tipo es escribir un programa en Java Script que lance múltiples ventanas, cada una solicitando una conexión a un servidor con applets de Java. En menos de 40 segundos un sistema Win 95 o UNIX con menos de 64 MB de memoria se paralizaría.

Otra forma de atacar Win 95 y NT en el ataque CHARGEN que lanza múltiples solicitudes al puerto 19 colgando la máquina.

A nivel de clase B podemos mencionar a sendmail. Cuando arranca solicita la identidad del usuario dado que solo root está autorizado para arrancarlo y darle mantenimiento. Desafortunadamente puede ser invocado en modo demonio de manera que se ignore la revisión. Además, a partir de la versión 8.7 sé rearranca a sí mismo cuando recibe una señal SIGHUP. Dado que la reejecución se efectúa a nivel de root el usuario puede manipular el ambiente para ejecutar programas arbitrarios.

Para más información ver http://info.pitt.edu/HOME/Security/pitt-advisories/95-05-sendmail-vulnerabilities.html y http://www.crossroads.fi/~tkantola/hack/unix/sendmail.txt

Los agujeros de clase A son los más peligrosos y generalmente resultan de la mala administración y/o configuración.

El ejemplo más conocido es un script CGI llamado test-cgi que se distribuyó con las primeras versiones de Apache, Este programa permitía leer archivos del directorio CGI.

Ver http://www.sec.de/sec/bug.testcgi

Otro programa llamado convert.bas permite a un usuario leer cualquier archivo del sistema en algunos servidores HTTP de NOVELL.

Otro ejemplo es que la versión 1.0 de MS IIS asocia todos los archivos con extensión bat o cmd con el programa cmd.exit.