

Escaneo y Enumeración

Escaneo: Generalidades

- Junto al Footprinting, el Escaneo y la Enumeración son las tres fases de obtención de información previas a un ataque.
- Estas tres fases, tienen por objeto encontrar sistemas o redes objetivo.
- El proceso de Enumeración, comienza apenas finalizado el de Escaneo y su objetivo es el de enumerar e identificar los nombres de los equipos, usuarios y recursos compartidos entre otra información de valor.
- Ambas fases suelen ser estudiadas en conjunto, puesto que la mayoría de las herramientas disponibles, realizan ambas tareas.

Escaneo: Generalidades (Cont.)

- Escaneo es el proceso de localización de sistemas que estén online en una red.
- El Ethical Hacker utiliza este proceso para encontrar las IP de sistemas objetivos
- En esta etapa, el atacante continua recopilando información de la red y de los hosts.
- Los siguientes datos ayudan al atacante a poder decidirse por el tipo de exploit que tiene que usar para obtener acceso a un sistema:
 - Dirección IP
 - Sistema operativo
 - Servicios Disponibles
 - Aplicaciones instaladas

Escaneo de Puertos, Red y Vulnerabilidades

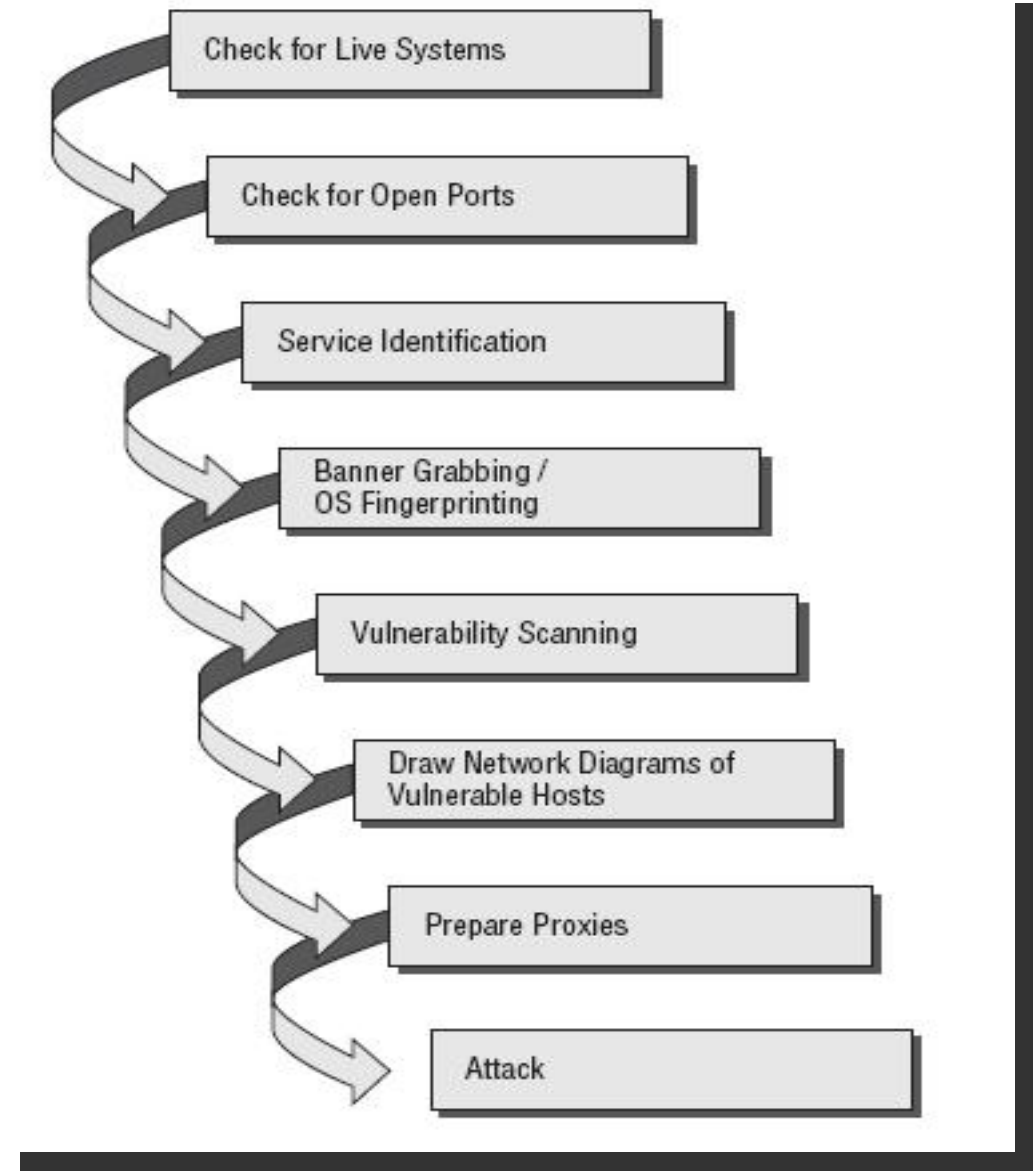
- De acuerdo a la metodología CEH, existen tres tipos de Escaneos:
 - **Escaneo de Puertos:** Determina los puertos TCP/IP abiertos y disponibles.
 - **Escaneo de Red:** Determina los hosts que se encuentran activos y sus correspondientes direcciones IP.
 - **Escaneo de Vulnerabilidades:** Determina la existencia de vulnerabilidades conocidas en los host/dispositivos evaluados.
- Las herramientas de escaneo pueden encontrarse elaboradas para cubrir uno o varios de estos tipos.
- Dichas herramientas envían paquetes a los distintos puertos a fin de detectar cuales se encuentran abiertos.
- Es importante conocer que existen herramientas que pueden detectar cuando se esta realizando un escaneo.

Puertos y Aplicaciones

Puerto	Nombre	Descripción
20	ftp-data	Puerto de datos FTP
21	ftp	Puerto del Protocolo de transferencia de archivos (FTP)
22	ssh	Servicio de shell seguro (SSH)
23	telnet	El servicio Telnet
25	smtp	Protocolo simple de transferencia de correo (SMTP)
53	domain	Servicios de nombres de dominio
69	tftp	Protocolo de transferencia de archivos triviales (TFTP)
80	http	Protocolo de transferencia de hipertexto (HTTP)
110	pop3	Protocolo Post Office versión 3
115	sftp	FTP Seguro
137	netbios-ns	Servicios de nombres NETBIOS
138	netbios-dgm	Servicios de datagramas NETBIOS
139	netbios-ssn	Servicios de sesión NETBIOS
161	snmp	Protocolo simple de administración de redes (SNMP)
443	https	Protocolo de transferencia de hipertexto seguro (HTTP)

Metodología de Escaneo CEH

- Metodología CEH utilizada a la hora de conducir el proceso de escaneo de una red.
- Su principal objetivo, es el de asegurar que ningún sistema o vulnerabilidad es pasada por alto.



Ping Sweep

- Una de las técnicas mas simples de realizar un escaneo, es aquella denominada: Ping Sweep.
- Consiste en enviar paquetes ICMP request (*pings*) a todos los hosts de una red.
- Si un host responde, implica que está online y se lo considera posible objetivo de ataque.
- La gran ventaja de esta técnica es que permite enviar paquetes en forma simultanea, esto implica que todo el sistema es escaneado al mismo tiempo.
- La mayoría de las herramientas de escaneo incluyen una opción de ping sweep.

Ping Sweep (Cont.)

- Por otra parte, si bien ping sweep es considerada la técnica más sencilla, a la vez puede ser poco efectiva, ya que es simple de bloquear por Firewalls (de red y aplicación) y proxies.
- Asimismo, la mayoría de los IDS/IPS detectan y alertan al administrador de seguridad de la presencia de ping sweep en la red.
- Si un escaneo realizado solamente con la técnica de ping sweep, no detecta hosts online, esto no implica que dichos dispositivos no existan.
- Es una técnica rápida que se suele utilizar como complemento de escaneos más complejos y otros métodos alternativos de identificación.

Ping Sweep (Cont.)

- Algunas de las herramientas conocidas por implementar técnicas de Ping Sweep son:
 - Pinger
 - Friendly Pinger
 - WS_Ping_Pro
 - Nmap

Escaneo de Puertos

- Es el método utilizado para detectar puertos abiertos en un sistema.
- Implica testear cada puerto de cada host para determinar cuales están abiertos.
- En la metodología de escaneo CEH, es la segunda etapa.
- Usualmente brinda información más valiosa que el uso del ping sweep.
- La identificación de servicios es el tercer paso dentro de dicha metodología, pero las mismas herramientas suelen realizar ambas tareas.
- A partir de la identificación de los puertos abiertos, como regla general, un hacker puede identificar los servicios asociados a cada puerto.

Escaneo de Puertos: Contramedidas

- Respecto de Escaneo de Puertos, las contramedidas son procesos o herramientas que los administradores de seguridad configuran para detectar posibles intentos de escaneos en sus redes.
- Algunas de las contramedidas necesarias para prevenir que un atacante obtenga información de la red son las siguientes:
 - Implementar una arquitectura de seguridad apropiada, que contenga firewalls a distintos niveles e IDS.
 - Los Ethical Hackers utilizan sus herramientas para auditar las contramedidas implementadas.
 - Por ejemplo, una vez que el firewall está ubicado donde corresponde, una herramienta de escaneo de puertos ayudará a determinar si el firewall detecta y detiene dichos intentos de escaneo.

Escaneo de Puertos: Contramedidas (Cont.)

- El firewall debe trabajar en modo *statefull*, es decir, debe permitir analizar los datos dentro de los paquetes y no solo las cabeceras TCP.
- Los sistemas NIDS, se utilizan entre otras cosas para identificar métodos de detección de sistemas operativos llevados a cabo por distintas herramientas (Ej: nmap)
- Solamente se deben tener abiertos los puertos que se van a utilizar. El resto, deberían estar cerrados o filtrados.
- Los empleados de la organización, deben estar correctamente concientizados respecto a la seguridad y también estar al tanto de las distintas políticas que deben seguir.

Nmap: Generalidades

- Es una herramienta de software libre muy flexible, que realiza en forma rápida y eficiente, entre otras las siguientes acciones:
 - Ping sweeps
 - Escaneo de puertos
 - Identificación de servicios
 - Detección de direcciones IP
 - Detección del sistema operativo
- Permite analizar una gran cantidad de equipos en un única sesión.
- Existen versiones para varios sistemas operativos, entre ellos Windows, Linux y Unix.
- Posee tanto una versión por línea de comandos como con GUI.

Nmap: Generalidades

```
C:\WINDOWS\system32\cmd.exe
D:\Tools\nmap>nmap -sS -sU 172.16.1.96

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2005-06-15 13:10 Hora est. de Sudam rica E.
Interesting ports on lab.honeynet.com (172.16.1.96):
<The 3121 ports scanned but not shown below are in state: closed>
PORT      STATE      SERVICE
21/tcp    open       ftp
25/tcp    open       smtp
80/tcp    open       http
135/tcp   open       msrpc
135/udp   open|filtered msrpc
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1025/tcp  open       NFS-or-IIS
1026/tcp  open       LSA-or-ntern
1029/tcp  open       ms-lsa
1030/udp  open       iad1
1433/tcp  open       ms-sql-s
1434/udp  open|filtered ms-sql-m
3372/tcp  open       msdtc
3389/tcp  open       ms-term-serv
3456/udp  open|filtered IISrpc-or-vat
MAC Address: 00:50:04:9D:0D:FB (3com)

Nmap finished: 1 IP address (1 host up) scanned in 3.636 seconds
D:\Tools\nmap>
```

Nmap: Generalidades (Cont.)

- Según Nmap, el estado que pueden presentar un puerto es abierto, filtrado o no filtrado.
 - **Abierto** implica que el equipo objetivo acepta peticiones a ese puerto.
 - **Filtrado** significa que un firewall u otro dispositivo de red enmascara el puerto y previene que nmap determine si está abierto o no.
 - **No filtrado** implica que el puerto está cerrado y ningún dispositivo interfiere con el escaneo de nmap

Nmap: Modificadores de Consola

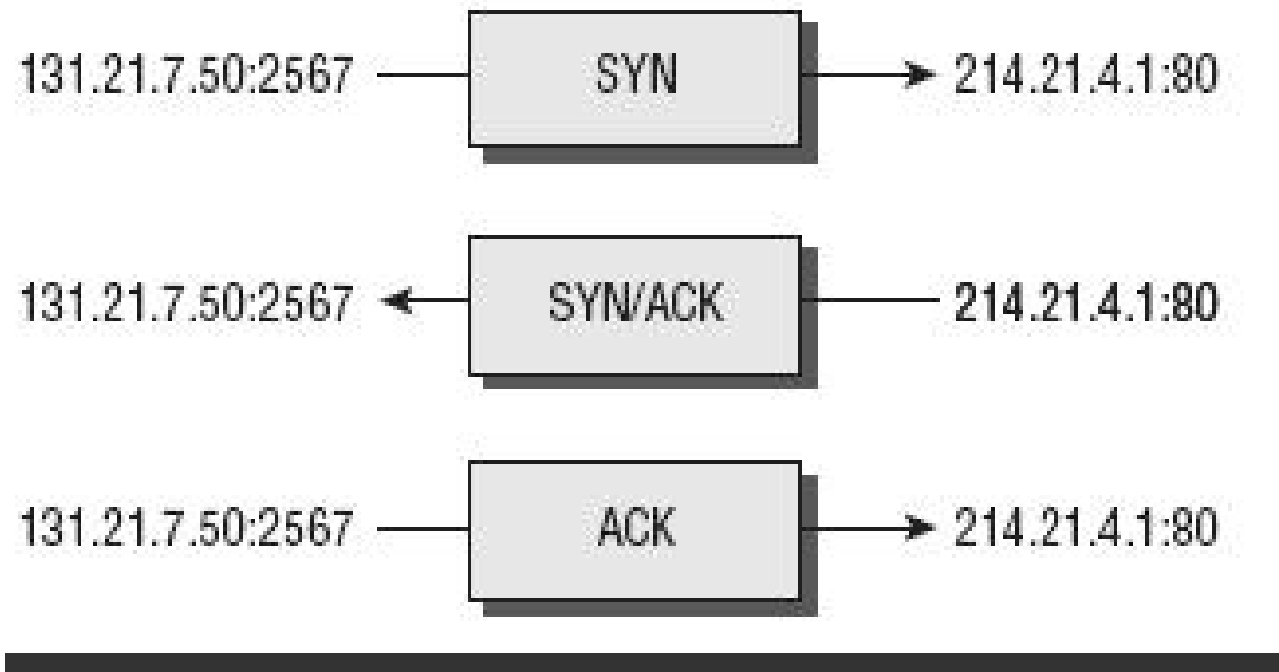
-sT	TCP connect scan	-sR	RPC scan
-sS	SYN scan	-sL	List / DNS scan
-sF	FIN scan	-sl	Idle scan
-sX	XMAS tree scan	-Po	Don't ping
-sN	Null scan	-PT	TCP ping
-sP	Ping scan	-PS	SYN ping
-sU	UDP scan	-PI	ICMP ping
-sO	Protocol scan	-PB	TCP and ICMP ping
-sA	ACK scan	-PB	ICMP timestamp
-sW	Windows scan	-PM	ICMP netmask

Nmap: Modificadores de Consola (Cont.)

-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, and 1.25 sec/probe
-T Insane	Parallel scan, 75 sec timeout, and .3 sec/probe

Flags en Conexiones TCP

- Los tipos de escaneos se basan en las conexiones TCP.
- Estas requieren llevar adelante el Three-way Handshake o saludo de tres vías, previamente a cualquier transferencia de datos entre emisor y receptor.



Flags en Conexiones TCP (Cont.)

- Dado que el protocolo TCP es orientado a la conexión, el proceso por el cual se establecen, reinician y finalizan las conexiones están contempladas en el protocolo.
- Para esto se utilizan distintas notificaciones denominadas flags.
- Un atacante intentará saltarse los procesos de detección manipulando dichos flags en lugar de establecer conexiones TCP normales.

Flags en Conexiones TCP (Cont.)

- El protocolo TCP incluye seis flags distintos:
 - **SYN** (Synchronize): Es el encargado de iniciar una conexión entre dos hosts.
 - **ACK** (Acknowledge): Luego del flag SYN, es el encargado de establecer la conexión.
 - **PSH** (Push): El sistema reenvía datos en el buffer.
 - **URG** (Urgent): Los datos deben procesarse rápidamente.
 - **FIN** (Finish): Termina la conexión según un proceso establecido.
 - **RST** (Reset): Corta abruptamente la conexión.

Tipos de Escaneo: SYN

- **SYN:** El SYN o escaneo stealth no completa el TCP three-way handshake. Un atacante envía un paquete SYN al objetivo, si se recibe de vuelta la respuesta con el SYN/ACK, se asume que se podría completar la conexión y que el puerto está escuchando.
 - Si se recibe un RST desde el objetivo, se asume que el puerto está cerrado o bien no está activo.
 - La ventaja de este escaneo es que suele dejar menos registros de logueo en los IDS.

Tipos de Escaneo: XMAS y FIN

- **XMAS:** Envían un paquete con los flags FIN, URG y PSH activados. Si el puerto está abierto, este no responde. Pero si está cerrado, el objetivo responde con un paquete RST/ACK.
 - Solo funciona sobre sistemas objetivo que cumplan con la implementación TCP/IP dada por el RFC 793 y no bajo ninguna versión de Windows.
- **FIN:** Es similar al XMAS pero solamente envía un paquete con el flag FIN activado. Recibe las mismas respuestas y posee las mismas limitaciones que el XMAS.

Tipos de Escaneo: NULL e IDLE

- **NULL:** También es similar al XMAS y al FIN en las limitaciones y respuestas, pero este envía un paquete sin ningún flag activado.
- **IDLE:** Utiliza una IP spoofed para enviar un paquete SYN a un objetivo. Dependiendo del tipo de respuesta, se puede determinar que el puerto está abierto o no. Esto lo hace monitoreando los números de secuencia de las cabeceras IP.

Técnicas de War Dialing

- Es el proceso por el cual un atacante marca a distintos módems hasta encontrar alguna conexión abierta que provea acceso remoto a una red.
- Se incluye como método de escaneo ya que permite encontrar otros accesos a redes por medios que usualmente no están tan protegidos como los enlaces principales.
- Las herramientas de war dialing parten de las premisas que las organizaciones no controlan tan estrictamente los puertos de acceso telefónico como lo hacen con los del firewall y además, los módems aún están presentes en varias equipos aunque no estén en uso.
- Por otro lado, muchos servidores utilizan módems con líneas telefónicas como backup, en caso que el enlace principal falle.

Técnicas de War Dialing (Cont.)

- Algunas Herramientas:
 - THC-Scan
 - Phonesweep
 - War dialer
 - Telesweep

Herramienta: Phonesweep

The screenshot displays the PhoneSweep 4.4 application window titled "PhoneSweep 4.4 - BOSTON_OFFICE1_JUN2002". The interface includes a menu bar (File, View, Help), a toolbar with icons for Start, Stop, Rescan, Save, Revert, Default, Import, Export, Report, Graph, and a help icon. A progress bar at the top right shows 2% completion. Below the toolbar are tabs for Phone Numbers, Results, Status, History, and Setup. The main area is divided into two sections: a summary table and a modem activity log.

Estimated Progress		Actual Progress	
Calls Per Hour:	00002368		
Calls Remaining:	00016709		
Total Calls:	00017084	Calls Completed:	00000375
Time Until Finish:	7:05:17	Elapsed Time:	00:09:35

Modem	Activity
1	Dialing "9,617-555-1036" (Single Call Detect)
2	--
3	--
4	--
5	--
6	--
7	--
8	--

At the bottom of the window, a status bar shows "Sweeping" and several control icons, including a green light, a red 'X' over a modem icon, two "-OFF-" indicators, a red arrow, and a checkmark next to phone numbers "555-1212" and "555-1213".

Banner Grabbing y OS Fingerprinting

- Ambas técnicas están contempladas en el cuarto paso de la metodología de escaneo CEH
- El proceso de fingerprinting permite a un atacante identificar objetivos vulnerables o aquellos que posean alto valor respecto al tipo de información que manejan. El atacante siempre va a buscar el método más sencillo para lograr este objetivo.
- Banner Grabbing es el proceso por el cual se abre una conexión y se leen los banners o respuestas enviados por la aplicación. La mayoría de los emails, FTP y webservers, responden a una simple conexión telnet con el nombre y la versión del software que se está ejecutando.
- Esta información es vital, ya que a partir de una determinada aplicación se puede deducir cual es el sistema operativo sobre el cual se está ejecutando.

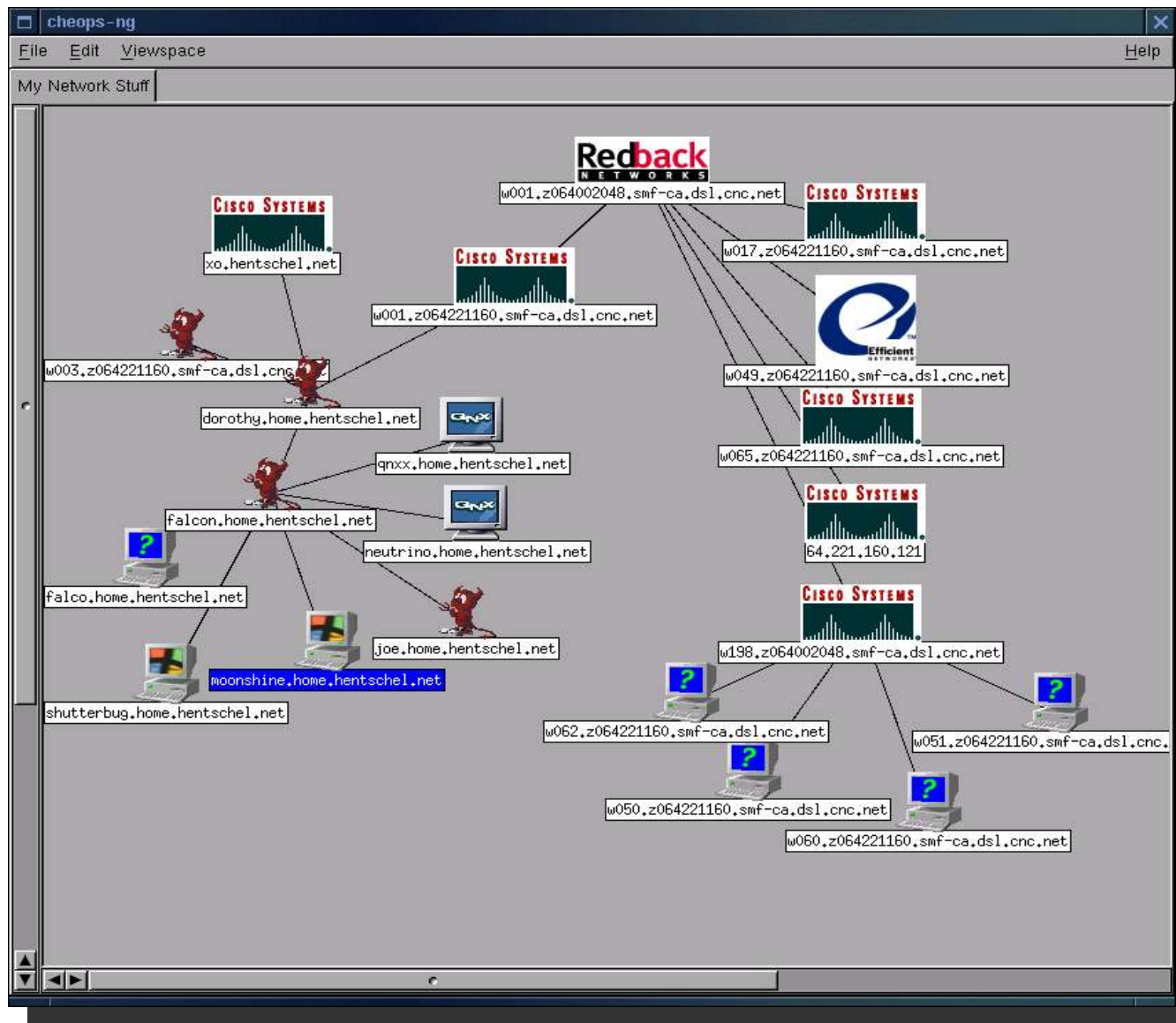
Banner Grabbing y OS Fingerprinting (Cont.)

- Podemos diferenciar dos métodos de fingerprinting:
 - El **Active Stack fingerprinting** es el método más común de fingerprinting. Por medio de este se envían datos a un sistema para analizar como son las respuestas del mismo. Dado que cada sistema implementa el stack TCP de forma diferente, las respuestas a determinados paquetes también será diferente, a partir de esto de determina cual es el sistema que esta corriendo en ese equipo. Debido a que trabaja en forma activa, es fácilmente detectable por IDS.
 - El **Passive Stack Fingerprinting** es más discreto y se basa en analizar el tráfico sobre la red para determinar el sistema operativo. Al no basarse en el envío de paquetes suele pasar desapercibido frente a IDSs, pero es menos exacto en la detección que el fingerprinting activo.

Banner Grabbing y OS Fingerprinting (Cont.)

- Herramientas que contemplan OS fingerprinting, banner grabbing y armado de diagramas de red:
 - SolarWinds Toolset
 - Queso
 - Harris Stat
 - Cheops
 - Netcraft
 - HTTrack
 - HTTPrint

Herramienta: Cheops-NG



Herramienta: Netcraft

Netcraft - Search Web by Domain - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://searchdns.netcraft.com/?position=limited&host=microsoft.com

Site Search

NETCRAFT HOB HOB RD VPN Desktop on Demand browser-based solution

Netcraft News

Search Web by Domain

Explore 6,534,940 web sites visited by users of the Netcraft Toolbar 19th September 2008

Search: search tips

site contains microsoft.com lookup!

example: site contains .sco.com

Results for microsoft.com

Found 355 sites

Site	Site Report	First seen	Netblock	OS
1. www.microsoft.com		August 1995	Microsoft Corp	unknown
2. update.microsoft.com		February 2005	Microsoft Corp	Windows Server 2003
3. download.microsoft.com		August 1999	Level 3 Communications, Inc.	Linux
4. v5.windowsupdate.microsoft.com		January 2004	Microsoft Corp	Windows Server 2003
5. search.microsoft.com		January 1997	ADSL endpoints NAT conections only	Linux
6. windowsupdate.microsoft.com		February 1999	Microsoft Corp	Windows Server 2003
7. msdn.microsoft.com		September 1998	Microsoft Corp	unknown
8. go.microsoft.com		November 2001	Microsoft Corp	Windows Server 2003
9. v4.windowsupdate.microsoft.com		November 2001	Microsoft Corp	Windows Server 2003
10. oca.microsoft.com		November 2001	Microsoft Corp	Windows Server 2003
11. r.office.microsoft.com		November 2003	MS Hotmail	Windows Server 2003
12. msdn2.microsoft.com		November 2004	Microsoft Corp	Windows Server 2003
13. technet.microsoft.com		August 1999	Microsoft Corp	unknown

Done Proxy: None

Servers Now Hosted In Three Data Centers

Dallas, TX

Seattle, WA

Washington, DC

INFO Visit Us Today SoftLayer.com

SOFTLAYER

Herramienta: HTTPrint

httprint version 0.202

Input File: D:\Tools\WebServer Assessment\httprint\win32\input.txt

Signature File: D:\Tools\WebServer Assessment\httprint\win32\signatures.txt

Host	Port	Banner Reported	Banner Deduced	Conf.%
www.argentina.com	80	Apache/1.3.33 (Unix) PHP/5.0.3	GoGoGadgetWebserver/0.3	57.83

httprint_gui

! httprint completed..

Aceptar

Apache/1.3.33 (Unix) PHP/5.0.3
811C9DC56ED3C295811C9DC5811C9DC5811C9DC5811
0D7645B5811C9DC5811C9DC5811C9DC5811
6ED3C295E2CE69236ED3C295811C9DC568D17AAE2576B7696ED3C2959E431BC8
6ED3C2956ED3C2952A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923
E2CE69236ED3C295626420C068D17AAEE2CE6923

GoGoGadgetWebserver/0.3: 96 57.83
Apache/1.3.26: 88 42.44
Apache/1.3.27: 88 42.44
Apache/1.3.[4-24]: 87 40.73

Report File: D:\Mis Documentos\Mis Papers\Revista Arroa\Numero IV\httprint

html xml csv

Clear All Options

httprint has been completed..

Uso de Proxies en Launchingan Attack

- Según la metodología CEH, la preparación de un proxy server es el último paso.
- Un proxy, es un equipo que hace de intermediario entre el atacante y el equipo víctima. Su objetivo es que el atacante sea anónimo dentro de la red.
- El atacante primero realiza la conexión al proxy y desde allí solicitar la conexión hacia el equipo objetivo.
- Esto permite al atacante navegar por la web en forma anónima o por el contrario, esconder sus ataques.
- Herramientas: SocksChain

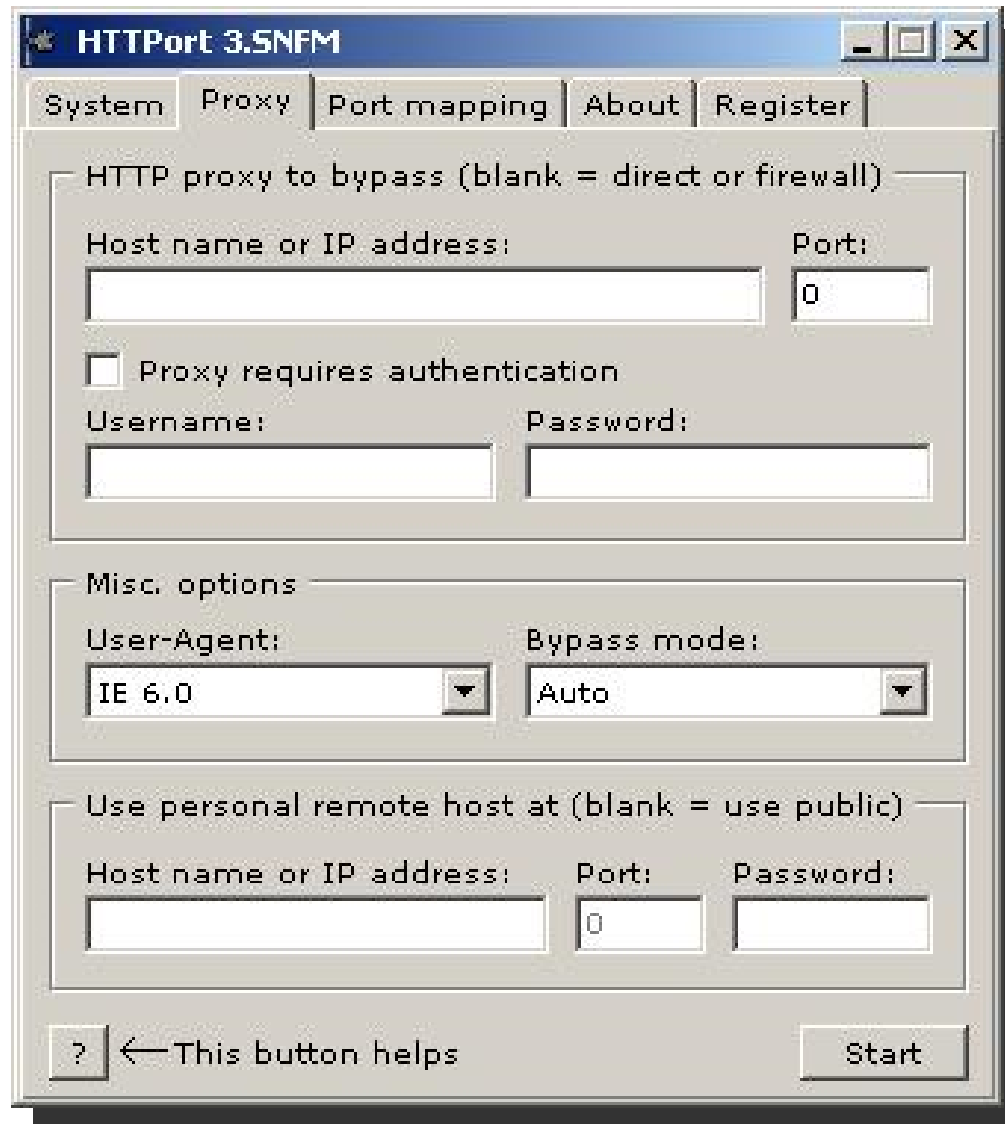
Como Trabajan los Anonymizers?

- Son servicios que buscan anonimizar la navegación web utilizando un website que actúa como proxy para el cliente web.
- Remueven todo tipo de información que pueda identificar en internet a un usuario mientras este navega.
- El atacante ingresa en su cliente web el website del software anonymizer, y este es quien realiza la petición de conexión a todos los sites a los que se quiera ingresar.
- Todas las peticiones a las páginas web son reenviadas a través del website del anonymizer, dificultando el posterior tracking para determinar la dirección real del atacante.

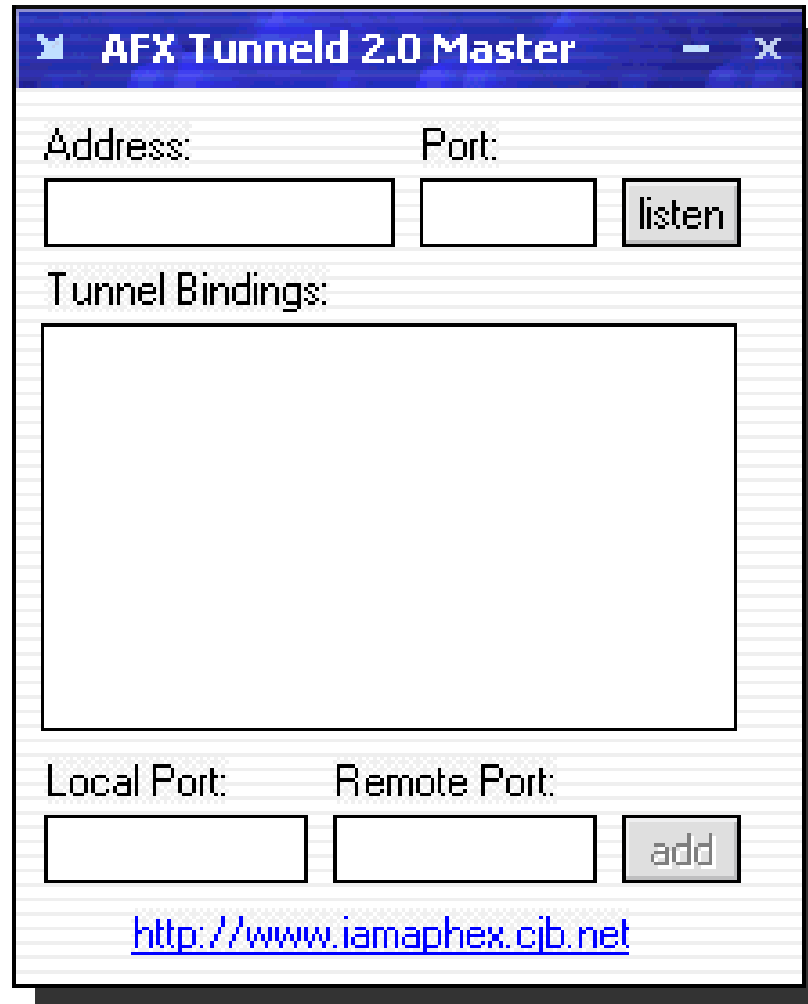
Técnicas de Tunnelizado por HTTP

- Un método efectivo de saltar firewalls o IDSs es tunelizar un protocolo bloqueado a través de uno permitido (por ejemplo SMTP a través de HTTP)
- La mayoría de los IDS y firewalls actúan como proxies entre la PC cliente e Internet, solo dejando pasar el tráfico definido como permitido.
- La mayoría de las organizaciones permite el tráfico HTTP ya que por lo general contiene tráfico benigno.
- Pero a través del tunnelizado HTTP, un atacante puede pasar el proxy escondiendo protocolos potencialmente peligrosos. Por ejemplo tunelizar protocolos de mensajería instantánea.
- Ejemplos de herramientas que tunelizan por HTTP son:
 - HTTPort
 - Tunneld
 - BackStealth

Herramienta: HTTPort



Herramienta: Tunneld



Técnicas de IP Spoofing

- Un atacante puede spoofear una dirección IP al momento de escanear potenciales sistemas víctimas, con el objetivo de minimizar las posibilidades de detección.
- Una desventaja de la técnica de IP spoofing es que no puede completarse una sesión TCP, ya que la dirección de origen está modificada.
- Una Source Routine permite al atacante especificar una ruta para los paquetes que pasan por Internet.
- Esto también minimiza las probabilidades de detección debido a IDSs y firewalls. Las source routines utilizan una respuesta en la cabecera IP que devuelve el paquete a una dirección spoofeada en lugar de la dirección real del atacante.

Enumeración

- Es la extracción de nombres de usuarios y de grupo, nombres de equipos, recursos de red, recursos compartidos y servicios.
- Implica conexiones activas a los sistemas y consultas directas para obtener dicha información.
- Las técnicas de enumeración usualmente se realizan dentro de la red interna.

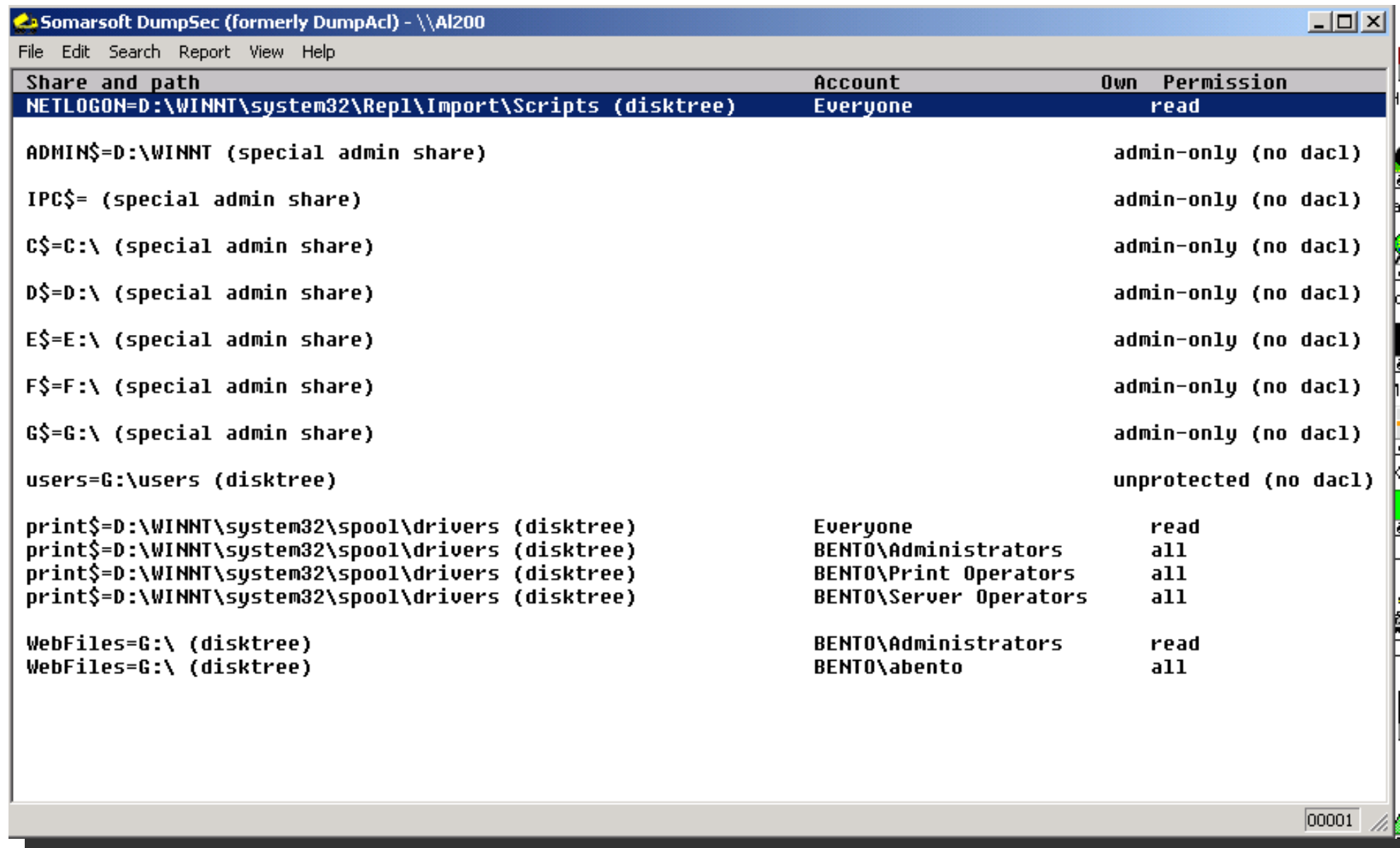
Enumeración (Cont.)

- ¿Qué información se enumera?
 - Recursos compartidos y de red.
 - Usuarios y grupos.
 - Versiones aplicaciones y banners.
 - Configuraciones.

Enumeración (Cont.)

- Técnicas para Realizar Enumeración:
 - Extraer nombres de usuario en Windows.
 - Extraer nombres de usuario utilizando SNMP.
 - Extraer nombres de usuario utilizando ID de e-mails.
 - Extraer información utilizando contraseñas default.
 - Extraer información de AD mediante fuerza bruta.
- Herramientas:
 - DumpSec
 - Hyena
 - The SMB Auditing Tool
 - The NetBIOS Auditing Tool

Herramientas: DumpAcl



Somarsoft DumpSec (formerly DumpAcl) - \\AI200

File Edit Search Report View Help

Share and path	Account	Own Permission
NETLOGON=D:\WINNT\system32\Repl\Import\Scripts (disktree)	Everyone	read
ADMIN\$=D:\WINNT (special admin share)		admin-only (no dacl)
IPC\$= (special admin share)		admin-only (no dacl)
C\$=C:\ (special admin share)		admin-only (no dacl)
D\$=D:\ (special admin share)		admin-only (no dacl)
E\$=E:\ (special admin share)		admin-only (no dacl)
F\$=F:\ (special admin share)		admin-only (no dacl)
G\$=G:\ (special admin share)		admin-only (no dacl)
users=G:\users (disktree)		unprotected (no dacl)
print\$=D:\WINNT\system32\spool\drivers (disktree)	Everyone	read
print\$=D:\WINNT\system32\spool\drivers (disktree)	BENTO\Administrators	all
print\$=D:\WINNT\system32\spool\drivers (disktree)	BENTO\Print Operators	all
print\$=D:\WINNT\system32\spool\drivers (disktree)	BENTO\Server Operators	all
WebFiles=G:\ (disktree)	BENTO\Administrators	read
WebFiles=G:\ (disktree)	BENTO\abento	all

00001

Herramientas: The NetBIOS Auditing Tool

```
Command Prompt (2)
D:\security\nat-enum>nat
usage: nat [-o filename] [-u userlist] [-p passlist] <address>

D:\security\nat-enum>nat 192.168.0.9

[*]--- Checking host: 192.168.0.9
[*]--- Obtaining list of remote NetBIOS names
[*]--- Remote systems name tables:

    L500
    BENT0
    L500
    L500
    BENT0

[*]--- Attempting to connect with name: *
[*]--- Unable to connect

[*]--- Attempting to connect with name: L500
[*]--- CONNECTED with name: L500
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Tue Sep 11 14:37:56 2001
[*]--- Timezone is UTC-4.0
[*]--- Remote server wants us to encrypt, telling it not to

[*]--- Attempting to connect with name: L500
[*]--- CONNECTED with name: L500
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: ' Password: 'ADMINISTRATOR'
[*]--- Attempting to connect with Username: ' Password: 'GUEST'
[*]--- Attempting to connect with Username: ' Password: 'ROOT'
[*]--- Attempting to connect with Username: ' Password: 'ADMIN'
[*]--- Attempting to connect with Username: ' Password: 'PASSWORD'
[*]--- Attempting to connect with Username: ' Password: 'TEMP'
[*]--- Attempting to connect with Username: ' Password: 'SHARE'
[*]--- Attempting to connect with Username: ' Password: 'WRITE'
[*]--- Attempting to connect with Username: ' Password: 'FULL'
[*]--- Attempting to connect with Username: ' Password: 'BOTH'
[*]--- Attempting to connect with Username: ' Password: 'READ'
[*]--- Attempting to connect with Username: ' Password: 'FILES'
```

Null Sessions

- Se da cuando está permitido loguearse a un sistema sin usuario o password.
- Las Null Session de NetBIOS son vulnerabilidades que se encuentran en el Common Internet File System (CIFS) o SMB, dependiendo el sistema operativo.
- Una vez que el atacante realizó una conexión NetBIOS usando una Null Session, fácilmente puede obtenerse la lista de todos los usuarios, grupos, recursos compartidos, permisos, políticas, servicios, etc; solamente utilizando la cuenta de usuario Null.
- Los estándares SMB y NetBIOS en Windows, incluyen APIs que brindan información acerca de un sistema a través del puerto TCP 139.

Null Sessions (Cont.)

- Un método de conexión por Null Session de NetBIOS a un sistema Windows es a partir de los recursos ocultos Inter Process Communication (IPC\$)
- Este recurso oculto es accesible utilizando el comando net use. Por ejemplo, para realizar una Null Session por NetBIOS a la IP 192.168.1.100, la sintaxis sería:

```
C: \> net use \\192.168.1.100 \IPC$ /u:"" ""
```

- Las comillas vacías indican que se quiere conectar sin usuario ni password, y se realizará con el usuario anónimo que viene incluido en el sistema.
- Una vez que se estableció la conexión por medio del comando net use, el atacante tiene un canal sobre el cual puede utilizar otras técnicas y/o herramientas.

Null Sessions: Contramedidas

- Las Null Sessions requieren acceso a los puertos TCP 135, 137,139, y/o 445. La primera medida es cerrar dichos puertos.
 - Esto se puede implementar deshabilitando los servicios SMB en los hosts o bien bloqueandolos a partir de un Firewall.

- También se puede restringir el acceso del usuario anónimo. Para ellos es necesario modificar la siguiente informacion en el registro de windows:
 1. Acceder a la cadena del registro
HKLM\SYSTEM\CurrentControlSet\Control\LSA.
 2. Ingresar estos valores:
 - Value name: **RestrictAnonymous**
 - Data Type: **REG_WORD**
 - Value: **2**

Null Sessions: Contramedidas (Cont.)

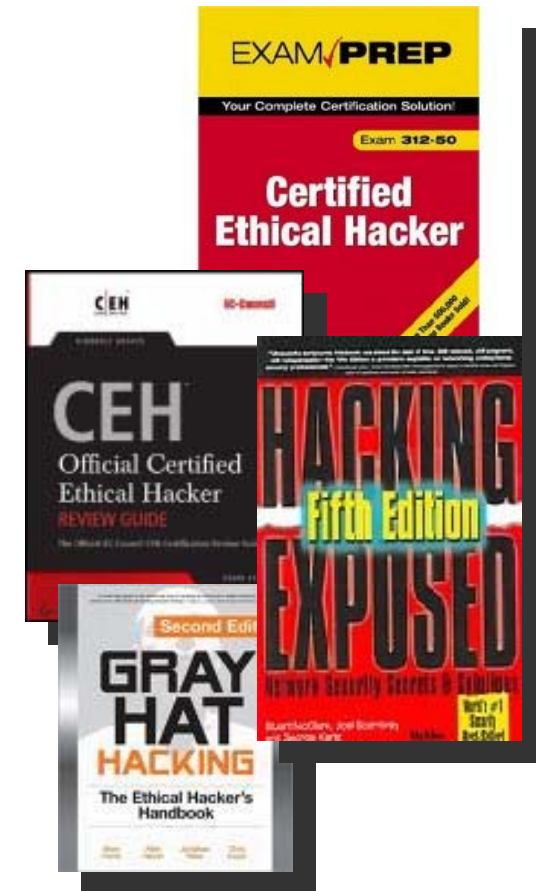
- Adicionalmente, el sistema puede actualizarse a Windows XP parcheado con las últimas actualizaciones de seguridad, lo cual mitiga el riesgo de ocurrencia de esta vulnerabilidad.

Escaneo y Enumeración

Links, Referencias y
Lecturas Complementarias

Referencias y Lecturas Complementarias

- **CEH Official Certified Ethical Hacker Review Guide**
By Kimberly Graves
(Sybex) ISBN: 0782144373
- **Certified Ethical Hacker Exam Prep**
By Michael Gregg
(Que) ISBN: 0789735318
- **Hacking Exposed, Fifth Edition**
By S.McClure, J.Scambray, and G.Kurtz
(McGraw-Hill Osborne Media) ISBN: 0072260815
- **Gray Hat Hacking, Second Edition**
By S.Harris, A.Harper, C.Eagle, J.Ness
(McGraw-Hill Osborne Media) ISBN: 0071495681



Escaneo y Enumeración

Preguntas?