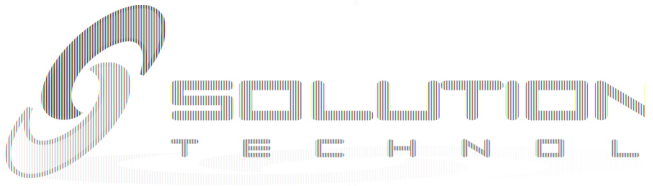
Ethical Hacking

Andrés Angulo Dávila
MCSE+S, CEH



AGENDA

- Introducción
- Fases del Hacking
- Hacking de Sistemas
- Troyanos & Sniffers
- Hacking de Servidores Web

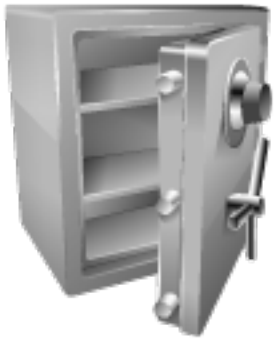
INTRODUCCION

Introducción

- Ethical Hacking
- Hacktivismo
- Tipos de Ataques
- Investigación de Vulnerabilidades
- Realizando Hacking Ético

Ethical Hacking

- Un hacker ético es una profesional de seguridad quien participa en evaluar amenazas de los atacantes, tiene excelentes conocimientos de computación, y se lo llama así por su confiabilidad.



Clases de Hackers

Black Hat - Cracker
Hacker quien usa sus conocimientos para asuntos de propósito ilegal o actividades maliciosas.

White Hat – Analista de Seguridad
Hacker quien usa sus conocimientos y habilidades para propósitos defensivos creando contramedidas.

Gray Hat
Hacker que es ofensivo y defensivo, cree en la divulgación total de la información.

Hacker Suicida
Tiene por objeto atacar por una “causa”, sin importar las consecuencias.

Clases de Hacker Ético

Black Hat en Reformación

- Cracker Reformado
- Tienen acceso a redes de hackers
- Se percibe menos credibilidad

White Black

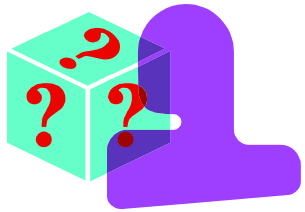
- Consultores independientes de seguridad
- Principios de ética profesional bien cimentados

Firma Consultora

- Hacker formados
- Consultores ICT Certificados

¿Qué hace un Hacker Ético?

- Un hacker ético de evaluación de sistemas de seguridad responde a tres preguntas:
  - Qué puede ver el intruso en el sistema objetivo?
  - Qué puede hacer un intruso con esa información?
  - Esta siendo notificado el sistema objetivo con los intentos o éxitos del intruso?



¿El Hacking puede ser Ético?

El término “hacking" a través del tiempo ha ganado una reputación negativa y se ha asociado con actividades destructivas o no deseadas

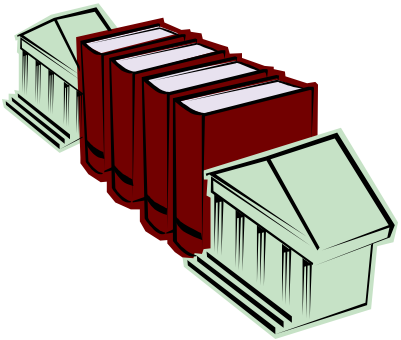
Hacker se refiere a la persona quien disfruta de aprender los detalles de un sistema de cómputo

Cracker se refiere a la persona quien usa sus habilidades para propósitos ofensivos

Hacking describe el desarrollo de nuevos programas o ingeniería reversa de software existente para hacer el código más seguro y eficiente

Ethical Hacker se refiere un profesional de seguridad quien aplica sus habilidades de hacking para propósito defensivo

Como ser un Hacker Ético?



- Ser competente en programación y hábil en redes de computación
- Conocimiento en investigación de vulnerabilidades
- Ser master en técnicas de hacking
- Seguir un estricto código de ética

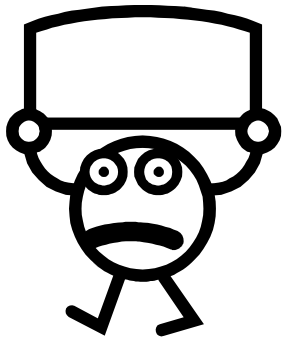
Habilidades de un Hacker Ético

- Un experto en computación, adepto a técnicas
- Tener un profundo conocimiento de plataformas como Windows, Unix y Linux
- Tener conocimiento ejemplar de networking y temas relacionados a software y hardware
- Conocimiento acerca de áreas de seguridad y los problemas relacionados
- “Altamente Técnico” para lanzar ataques sofisticados

Hacktivismo

Se refiere a una clase de desobediencia civil electrónica en la cual los activistas toman acción directa sobre los sistemas de computo del gobierno o empresas privadas como un acto de protesta

"Hackear por una causa"



Tipos de Ataques de Hacker

- Hay varias formas como un atacante puede acceder al sistema
- El atacante debe saber explotar debilidades y vulnerabilidades de los sistemas
- Tipos de Ataque:

  - **Sistemas Operativos**
  - **Ataques a nivel de Aplicación**
  - **Librería de código**
  - **Mala Configuración**

Que es la Investigación de Vulnerabilidades?

- El descubrimiento de vulnerabilidades y debilidades de diseño que permiten abrir un sistema operativo y las aplicaciones para atacar
- Mantenerse al día de los últimos productos y tecnologías de los fabricantes relacionados a los exploits existentes
- Chequear sitios web “underground” por nuevos exploits
- Innovaciones que se liberan en forma de avisos dentro de las mejoras del producto para los sistemas de seguridad

Por qué un Hacker necesita Investigación de Vulnerabilidades?

- Para identificar y corregir las vulnerabilidades de red
- Para proteger la red de ser atacada por intrusos
- Para obtener información que ayude a prevenir issues de seguridad
- Para obtener información acerca de virus
- Par encontrar debilidades en la red y alertar al administrador antes de un ataque
- Para saber recuperar de un ataque

Objetivos de un Hacking Ético

- Redes Remotas
- Redes dial-up
- Redes locales
- Redes Wireless
- Robo de equipos
- Ingeniería social
- Entrada Física

Pruebas de Hacking Ético

Hay diferentes formas de pruebas de seguridad, por ejemplo, escaneo de vulnerabilidades, hacking ético, pruebas de penetración

Black Box sin ningún conocimiento previo de la infraestructura objetivo de prueba

White Box con completo conocimiento de la infraestructura de red objetivo de prueba

Gray Box examina el grado de acceso de personas con información privilegiada dentro de la red

Demo

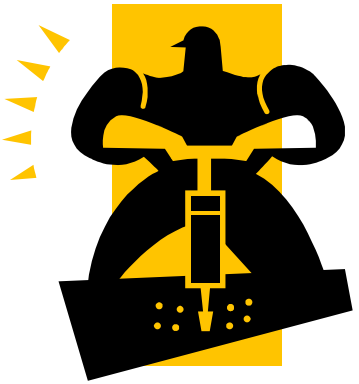
FASES DE UN HACKEO

Fases de un Hackeo

- Fases
- Fase I: Reconocimiento
- Fase II: Escaneo

Fases

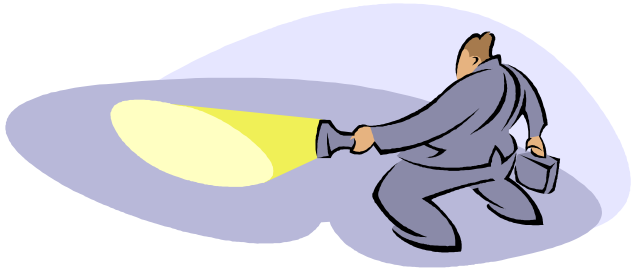
- Reconocimiento
- Escaneo
- Ganar Acceso
- Mantener Acceso
- Borrar Huellas



Fase 1 - Reconocimiento

– Es la fase de preparación

- Footprinting
- Dumpster Diving
- Fingerprinting
- Ingeniería Social



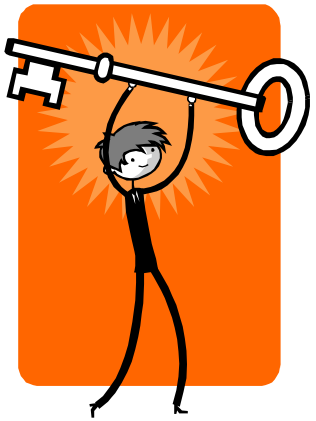
Fase 2 - Escaneo

- Es la fase de pre-ataque donde el hacker escanea la red para obtener información especifica generada en la fase de reconocimiento

  - Escaneo de Puertos
  - Escaneo de Red
  - Escaneo de Vulnerabilidades

Fase 3 – Ganar Acceso

- Se refiere a la fase de penetración, el hacker explota vulnerabilidades en el sistema
- El hacker puede ganar acceso a nivel del sistema operativo, aplicación o red
  - Desbordamiento
  - Denegación de Servicio
  - Secuestro de Sesión
  - Crackeo de contraseñas



"Es la fase mas importante en términos de daño potencial"

Fase 4 – Mantener Acceso

- El hacker intenta conservar su propiedad del sistema
- El hacker puede subir, descargar o manipular datos, aplicaciones y configuraciones
  - Backdoors
  - Rootkits
  - Troyanos

Fase 5 – Borrar Huellas

- Se refiere a la fase en la que hacker destruye evidencias y actividades

  - Steganography
  - Tunneling
  - Alterar Logs

Reconocimiento

- Definición
  - Es la fase de preparación donde el hacker obtiene la mayor cantidad de información posible del objetivo antes de ejecutar el ataque

Tipos de Reconocimiento

- Reconocimiento Pasivo
  - Involucra obtener información sin interactuar directamente con el objetivo de ataque
- Reconocimiento Activo
  - Interactúa directamente con el objetivo de ataque a través de cualquier medio

Footprinting

Es el blueprint del perfil de seguridad de la organización con respecto las redes (Internet, Intranet, Extranet, Wireless) y sus sistemas

El hacker utiliza el 90% del tiempo en perfilar la organización y el 10% en ejecutar el ataque

Encontrando Información Inicial

Es el proceso de detectar y extraer información del objetivo de ataque

Incluye:

- Nombres de dominio
- Bloques de red
- Servicios de Red y aplicaciones
- Arquitectura del sistema
- IDS
- Direcciones IP
- Mecanismos de control de acceso
- Números telefónicos
- Direcciones de correo
- Locaciones
- Etc

Fuentes de Información:

- Open Source
- Google
- Whois
- Nslookup
- Herramientas de hacking
- Sitios Web de trabajo
- Buscadores de personas
- archive.org

Escaneo

- Definición
  - Es una de las fases mas importantes de obtención de información para un hacker. En este proceso, el hacker intenta obtener información acerca de direcciones ip’s, el sistema operativo, arquitectura del sistema y servicios corriendo en cada computador

Objetivos del Escaneo

- Detectar sistemas vivos en la red
- Descubrir puertos activos
- Descubrir el sistema operativo
- Descubrir los servicios ejecutándose y presentes en el sistema
- Descubrir direcciones ip’s

Tipos de Escaneo

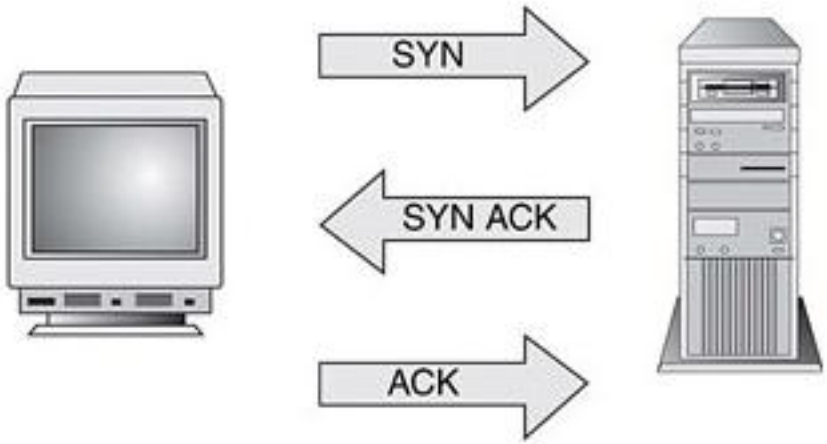
- Escaneo de Puertos
  - Es comprobar los servicios corriendo en le objetivo enviando una secuencia de mensajes en un intento de entrar
- Escaneo de red
  - Es el proceso de identificar host activos en la red
- Escaneo de vulnerabilidades
  - Es un método automático usado para identificar las vulnerabilidades presentes en el sistema y la red

Comunicación TCP

- La comunicación TCP esta controlada por banderas en el encabezado TCP
  - SYS
  - ACK
  - PSH
  - URG
  - FIN
  - RST

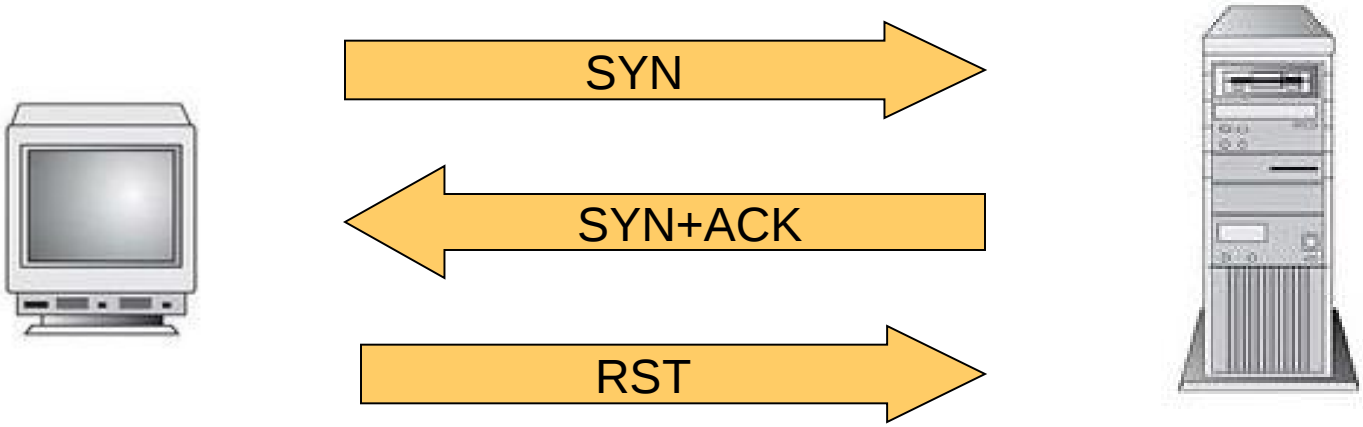
Three Way Handshake

TCP es orientado a la conexión, lo cual implica el establecimiento de la conexión, es prioritario a la transferencia entre aplicaciones.



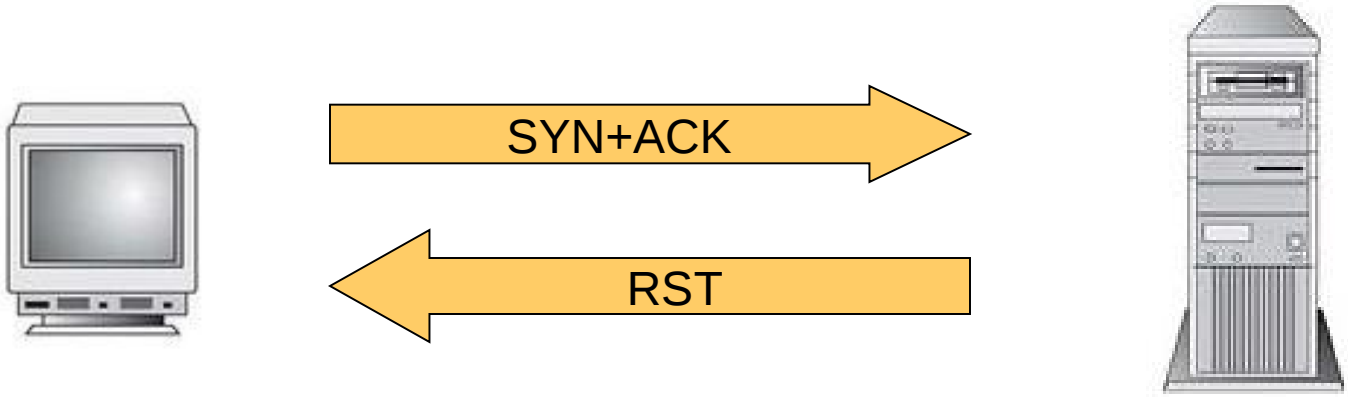
Half Open Scan

Se llama así porque este escaneo no abre una conexión TCP full



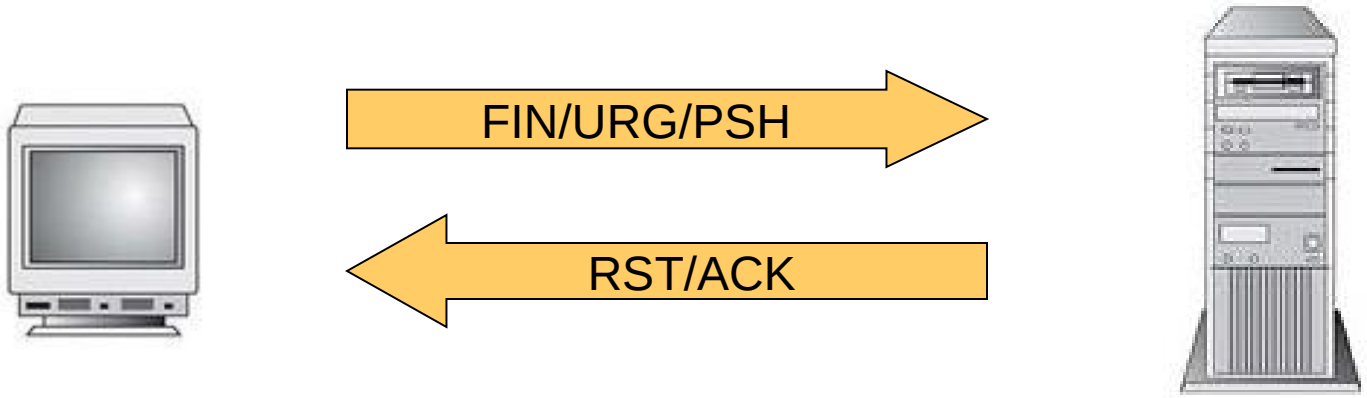
SYN/ACK Scan

Se envía un paquete con las banderas SYN/ACK a un puerto cerrado el cual responderá con un RST



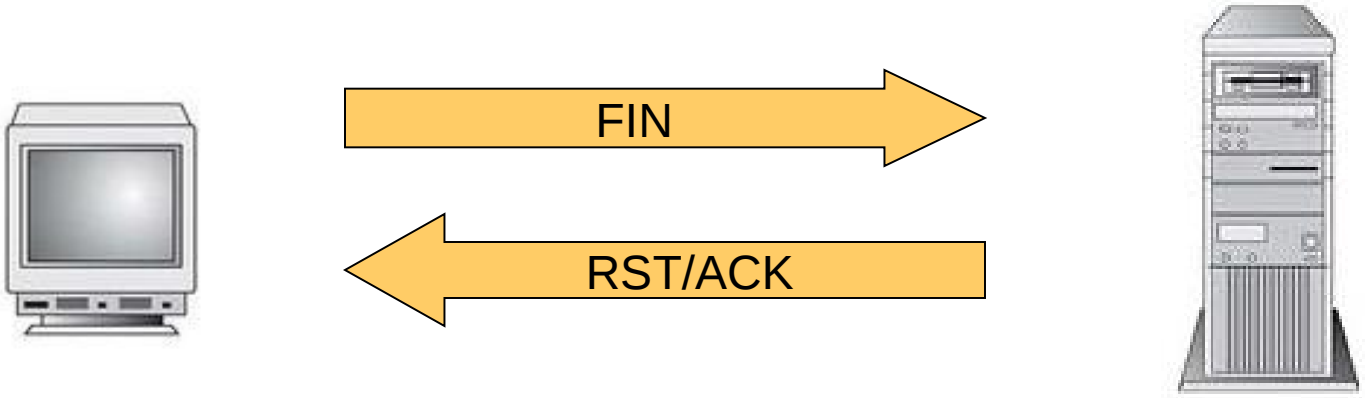
XMAS Scan

Es una técnica que envía todas las banderas en el paquete, cuando un mensaje es enviado a un puerto cerrado, el puerto responde con RST, indicando que el puerto esta cerrado



FIN Scan

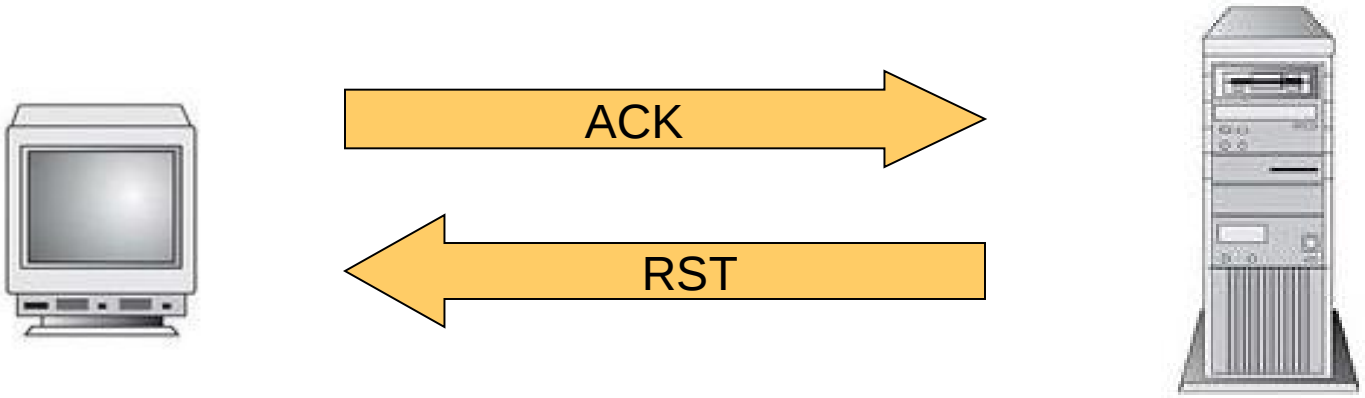
Se envía un paquete con la bandera FIN a un puerto cerrado el cual responderá con un RST



- Este escaneo explota las vulnerabilidades de los sistemas operativos basados en BSD
- No trabaja con sistemas operativos Windows, muestra como que todos los puertos están cerrados

ACK Scan

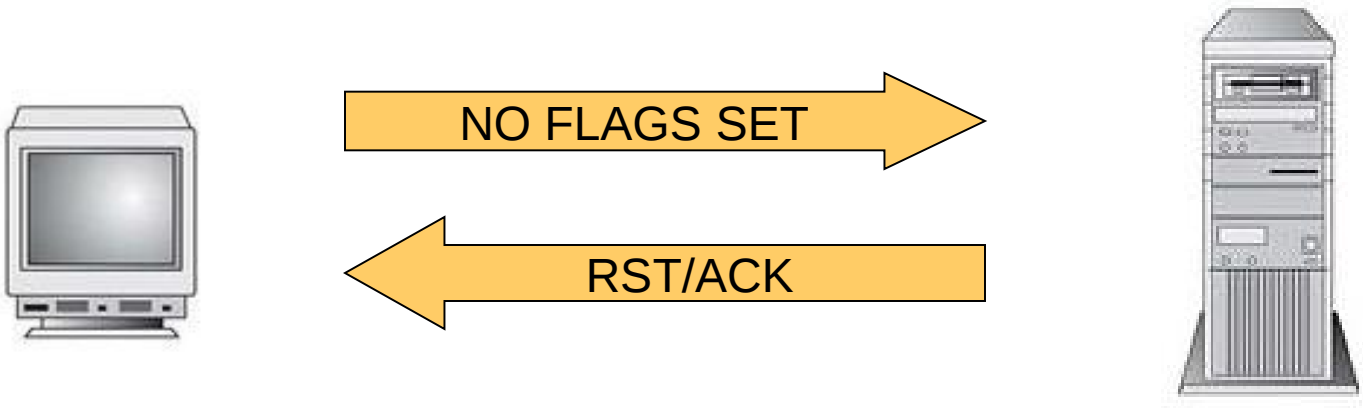
En este tipo de escaneo, la función de enrutamiento IP es usada para deducir el estado del puerto desde el valor TTL, decrementando cuando el puerto esta filtrado



- Trabaja en sistemas Unix

NULL Scan

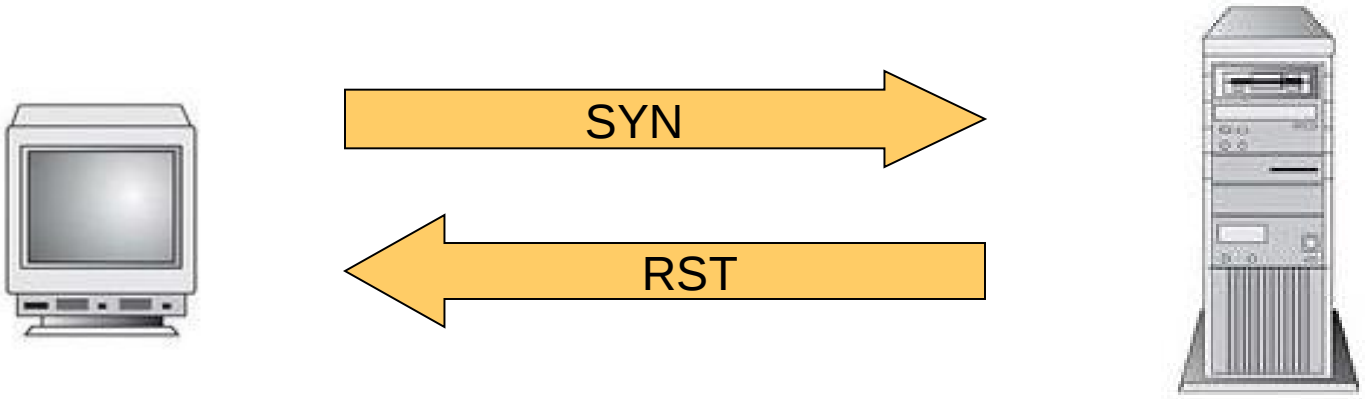
Es una técnica que apaga todas las banderas en el paquete, este asume que cada puerto cerrado envía un RST



- Evita IDS y TCP three handshake
- Trabaja solo para sistemas Unix
- No trabaja con sistemas operativos Windows, muestra como que todos los puertos están cerrados

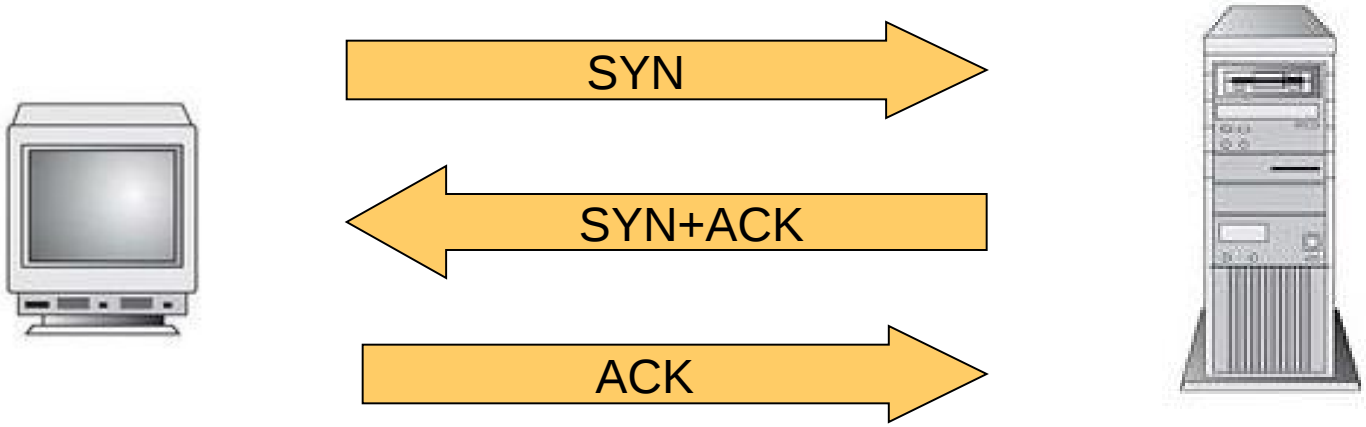
IDLE Scan

En este escaneo los paquetes no se originan con la ip del hacker sino a través de una ip Spoofed, este escaneo se lo llama zombie, si le puerto esta cerrado el equipo zombie (ip spoof) responde con un RST



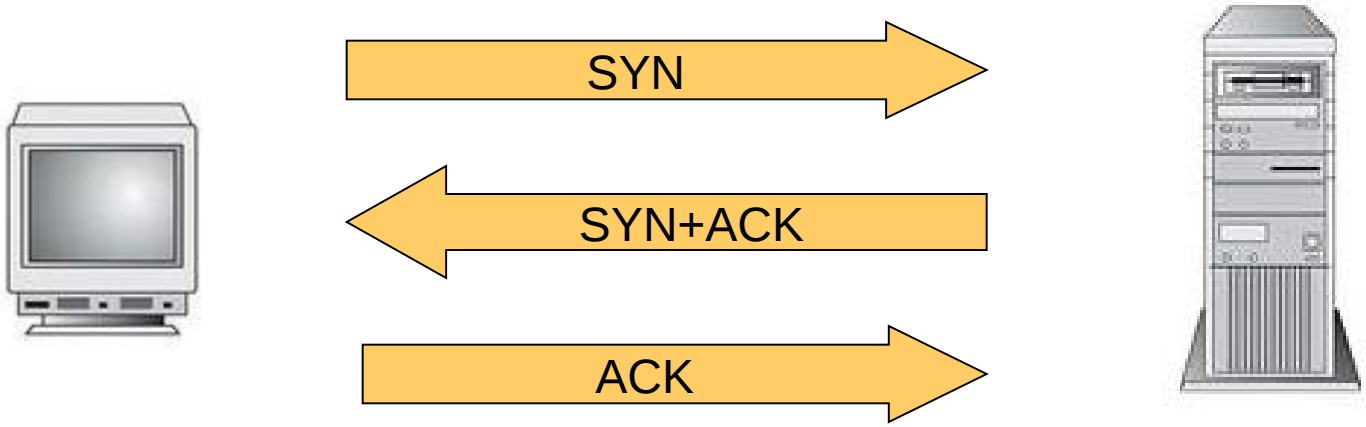
Full Open Scan

Es la forma mas confiable de escaneo, abre una conexión en cada puerto abierto en la maquina



Full Open Scan

Es la forma mas confiable de escaneo, abre una conexión en cada puerto abierto en la maquina



OS Fingerprinting

Es un método para determinar el sistema operativo que esta corriendo en el sistema.

- Activo
  - Paquetes específicos son enviados al sistema operativo, y la respuesta es notada
- Pasivo
  - Escaneo indirecto par revelar el sistema operativo del servidor, usa técnicas de sniffing

Herramientas para Escaneo

- HPING2
- Firewalk
- NMAP
- Netscan
- Megaping
- Global Network Inventor
- Telnet
- Httprint
- Nessus

HPING2

Aun si el host bloquea paquetes ICMP, esta herramienta ayuda a determinar si el host esta arriba.

Ejemplo:

- hping2 –a 192.168.1.15 –S –p 81 192.168.1.5
  - Envia paquetes SYN spoofed al objetivo a traves de un tercero al puerto 81

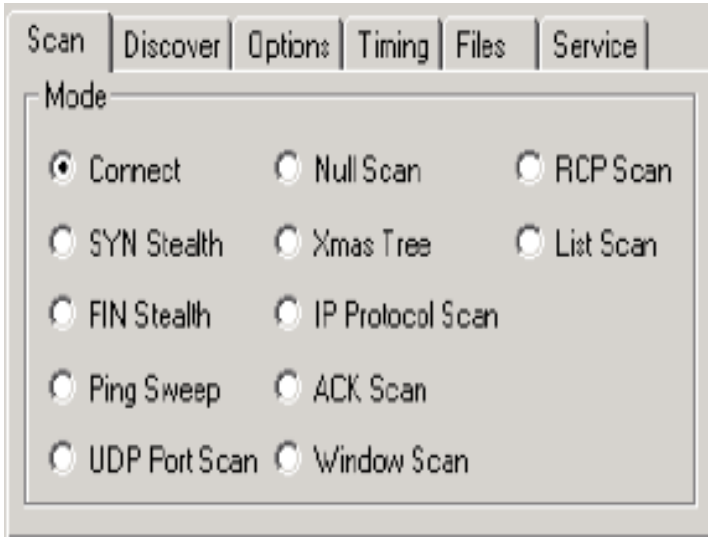
Firewalk

Es una herramienta que emplea traceroute como técnica para analizar las respuestas de paquetes IP para determinar los filtros ACL de un gateway, determina si existen filtros en un dispositivo

NMAP

- Es una herramienta de código abierto para explorar una red, soporta todos las técnicas de escaneo
- Es usada para escaneo de puertos, detección de sistema operativo, detección de versión y cualquier otra técnica
- Correo sobre Windows o Linux

NMAP



Ejemplo

- Nmap –A –T4 www.abc.com
  - Permite detección de sistema operativo y versión, escaneo de puertos con ejecución rápida

NetScan

- Consiste de muchas funciones de red independientes
- Determina el propietario de una dirección IP
- Traduce direcciones IP a nombres
- Escanea redes
- Prueba por puertos y servicios abiertos
- Valida direcciones de correo
- Determina la propiedad de dominios
- Lista computadores en un dominio

Megaping

- Es un set de herramientas que consisten de un escáner de seguridad, monitoreo de host y puertos y otras utilidades de red
  - Escaneo
  - Monitoreo
  - Información del Sistema
  - Utilidades de red

Global Network Inventor

- Es un software de inventario de hardware y software que puede ser utilizado como un escaneador de auditoria sin agentes en ambientes de zero implementación

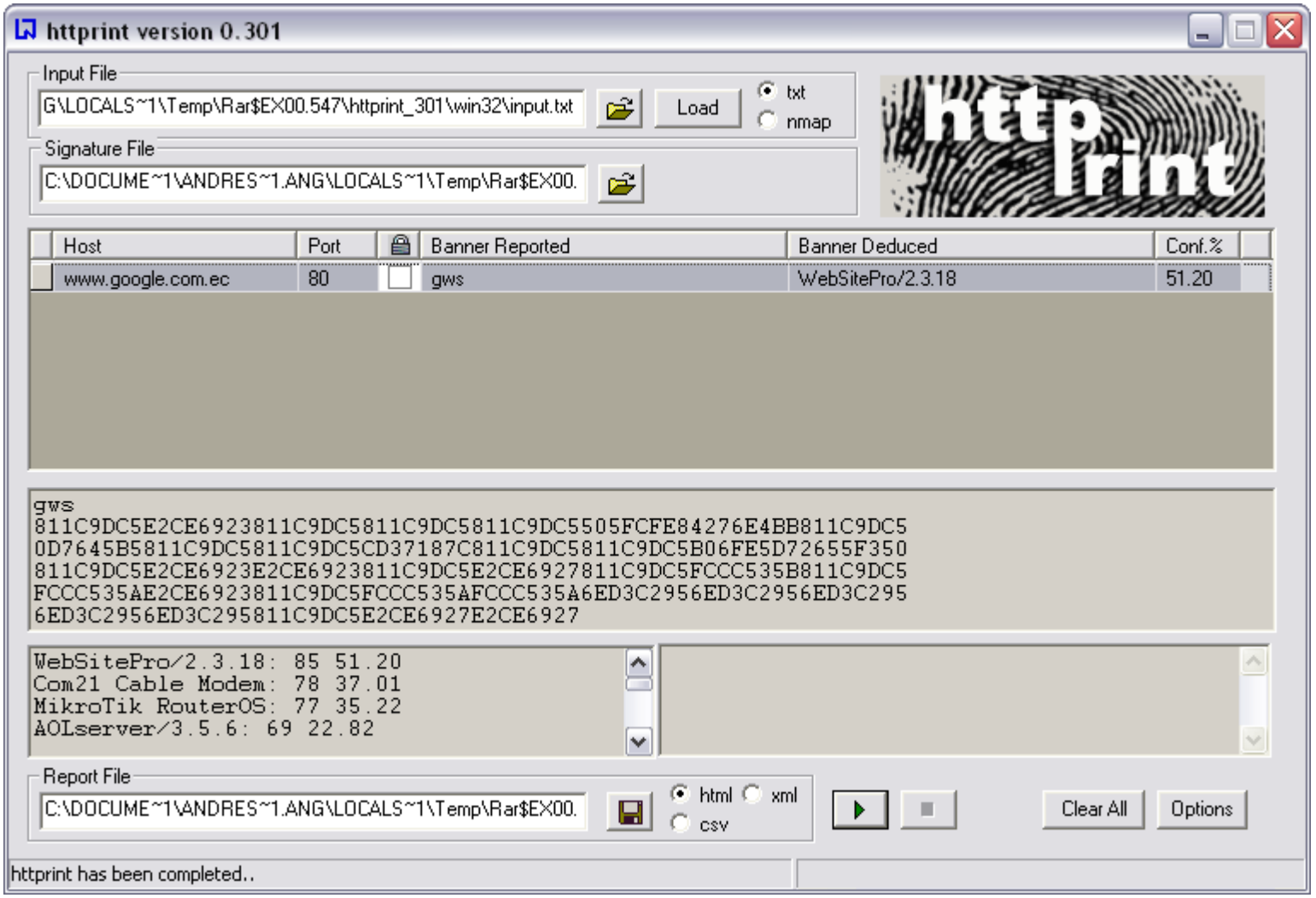
- Puede auditar estaciones, redes, impresorar, hubs y otros dispositivos

Telnet

- Se puede usar el Telnet para hacer un OS Fingerprinting de un sitio Web, es un escaneo activo

```
telnet www.abc.com 80
HEAD / HTTP/1.0
```

Httprint


httprint version 0.301
Input File
G\LOCALS~1\Temp\Rar$EX00.547\httprint_301\win32\input.txt
Load
txt
nmap
Signature File
C:\DOCUME~1\ANDRES~1.ANG\LOCALS~1\Temp\Rar$EX00.
http print
Host
Port
Banner Reported
Banner Deduced
Conf.%
www.google.com.ec
80
gws
WebSitePro/2.3.18
51.20
gws
811C9DC5E2CE6923811C9DC5811C9DC5811C9DC5505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C811C9DC5811C9DC5B06FE5D72655F350
811C9DC5E2CE6923E2CE6923811C9DC5E2CE6927811C9DC5FCCC535B811C9DC5
FCCC535AE2CE6923811C9DC5FCCC535AFCCC535A6ED3C2956ED3C2956ED3C295
6ED3C2956ED3C295811C9DC5E2CE6927E2CE6927
WebSitePro/2.3.18: 85 51.20
Com21 Cable Modem: 78 37.01
MikroTik RouterOS: 77 35.22
AOLserver/3.5.6: 69 22.82
Report File
C:\DOCUME~1\ANDRES~1.ANG\LOCALS~1\Temp\Rar$EX00.
html
xml
csv
Clear All
Options
httprint has been completed..

Demo

HACKING DE SISTEMAS

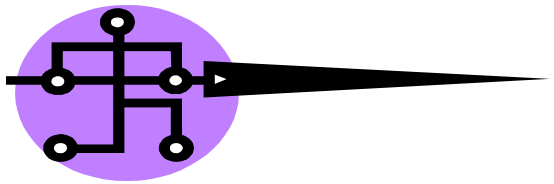
Hacking de Sistemas

- Crack de contraseñas
- Escalar privilegios
- Ejecutar aplicaciones
- Esconder archivos
- Cubrir huellas

Tipos de contraseñas

- Letras
  - Asdef
- Números
  - 64574
- Caracteres especiales
  - *@%&
- Letras y números
  - 453fGd6
- Letras y caracteres especiales
  - m@$
- Números y caracteres especiales
  - &$3@9
- Letras, caracteres especiales y números
  - n@(5MF%$

Tipos de ataques de contraseñas



- Ataques pasivos en línea
- Ataques activos en línea
- Ataques fuera de línea
- Ataques no electrónicos

Password Guessing: Ejemplo

```
C:\> for /f “token=1, 2*” %i in (pass.txt)
  do net use \\sistema_objetivo\IPC$ %i /u:
  %j
```

Herramientas para Cracking

- NAT
- SmbCrack
- PWdump2, PWdump3
- Lopthcrack LC4, LC5
- KerbCrack
- Rainbowcrack
- John the Ripper
- SMB Grind

Escalar Privilegios

Si un intruso tiene acceso al sistema objetivo con una cuenta de usuario y una contraseña válida, éste intenta elevar sus privilegios escalando la cuenta a privilegios de administrador

Ejecutar aplicaciones

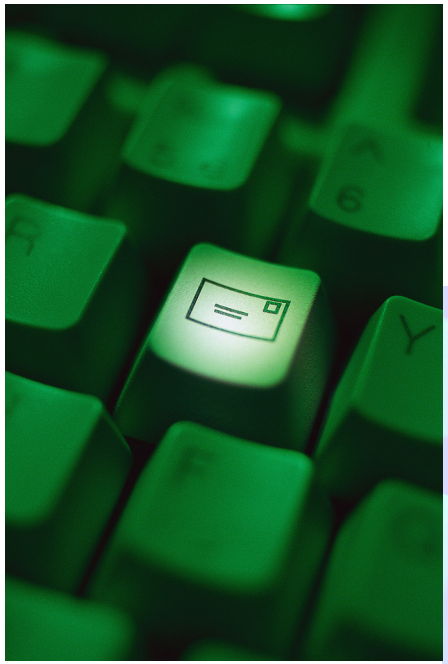
La ejecución de aplicaciones de forma remota se la puede realizar con propias herramientas de soporte, ejemplo, psexec

psexec permite la ejecución de procesos en otros sistemas, trabaja a través de una consola sin la necesidad de instalar ningún cliente

psexec \\sistema_objetivo cmd

psexec \\sistema_objetivo ipconfig

Keytroke Loggers



Keystroke loggers son paquetes de software que interactúan entre el teclado y el sistema operativo, almacenando cada tecleada

Keylogger de hardware

- Es un dispositivo de hardware diminuto que se conecta en el computador
- Almacena todos los tecleados hechos sobre el teclado, el proceso de almacenamiento es totalmente transparente
- Tipos:
  - PS/2
  - USB

Herramientas

- E-mail keylogger
- Perfect keylogger
- SpyTector FTP Keylogger
- Spector
- Stealth Voice Recorder
- Desktop Spy
- Telephone Spy
- Print Monitor Spy Tool
- Wiretap Professional
- FlexiSpy
- PC PhoneHome

Esconder archivos

Todos los archivos tienen un conjunto de atributos, entre ellos el atributo “hidden”, un hacker puede esconder o cambiar el atributo de los archivos de la víctima, y solo el hacker pueda tener acceso a esos archivos, sean los del sistema o los creados por el hacker.

Rootkits

Los rootkits son programas de kernel que permiten esconderse así mismos y cubrir las actividades de otro programa

- Por qué los rootkits?
  - El hacker requiere acceso root al sistema instalando un virus, troyano, spyware
  - Mantener acceso root, el hacker necesita esconder lo que hace modificando comandos del sistema
  - Permite que el hacker mantenga escondido el acceso al sistema

ADS (Alterate Data Streams)

ADS son otro tipo de flujo de datos con nombre que pueden estar presentes dentro de cada archivo.

Escondiendo un archivo:

c:\>notepad file.txt:hidden.txt

Escondiendo un troyano:

c:\>type c:\troyano.exe > c:\file.txt:troyano.exe

c:\>start c:\file.txt:troyano.exe

Extrayendo el archivo:

c:\>cat c:\file.txt:hidden.txt > c:\hidden.txt

c:\>cat c:\file.txt:troyano.exe > c:\troyano.exe

Steganography

El proceso de esconder datos en imágenes es llamado Steganography

Los hackers pueden incrustar información como:

- Información Secreta
- Planes de negocio
- Herramientas de hacking
- Planes de Ataques terroristas (Al Qaeda)

Herramientas

- Fu
- Nuclear
- ADS Spy
- Invisible Secrets
- Merge Streams
- Snow.exe
- MP3Stego

Cubrir Huellas

- Una vez que el hacker entró al sistema, debe cubrir la detección de su presencia
- Cuando toda la información de interés ha sido despojada del objetivo, el hacker instala backdoors para fácil acceso en el futuro

Deshabilitando Auditoria

- El primer paso de un hacker es determinar el estatus de la auditoria, localizar archivos sensibles, e implantar herramientas de obtención automática de información

```
c:\>auditpol \\sistema_objetivo
c:\>auditpol \\sistema_objetivo /disable
c:\>auditpol \\sistema_objetivo /enable
```

Limpiando el Log de Eventos

- Los intrusos pueden borrar fácilmente los de eventos
- Este proceso limpia todos los logs, pero deja un evento indicando que el log de eventos fue limpiado

```
c:\>elsave –l system –F d:\system.log –C
c:\>elsave –s \\sistema_objetivo –l “Security” -C
```

Demo

TROYANOS
&
SNIFFERS

Troyanos & Sniffers

- Troyanos
- Sniffers

Qué es un Troyano?

Es un programa pequeño que correo escondido en un sistema infectado

El troyano tiene dos partes
Servidor. Es parte del programa que es instalado en el equipo de la víctima
Cliente. Es la parte del programa que se instala en el equipo del hacker.

Canales abiertos y cubierto

Canal Abierto

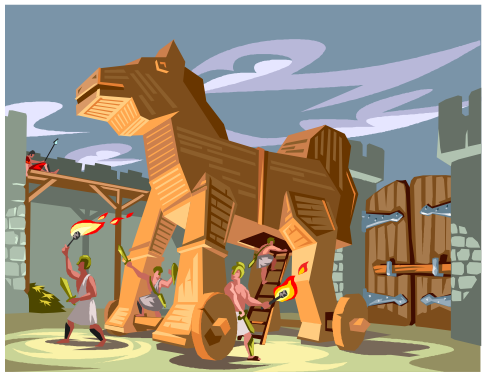
- Vía de comunicación legítima en un computador o red para transferencia de datos
- Un canal abierto puede ser usado para crear la presencia de un canal cubierto

Canal Cubierto

- Un canal que transfiere información en un computador o red violando las políticas de seguridad
- La forma simple de un canal cubierto es un troyano

Tipos de Troyanos

- Troyanos de acceso remoto
- Troyanos de envío de datos
- Troyanos destructivos
- Troyanos de DoS
- Troyanos Proxy
- Troyanos FTP
- Troyanos que deshabilitan software



Por qué los troyanos?

Los troyanos son escritos para roban información de otros sistemas y ejecutar control sobre ellos.

- Información de Tarjetas de crédito
- Documentos confidenciales
- Direcciones de email, contraseñas, cuentas de usuario, etc.
- Datos financieros
- Usar el equipo de la víctima para propósito ilegal, como hack, escaneo, filtrados, etc.

Vías por donde entra el troyano al Sistema

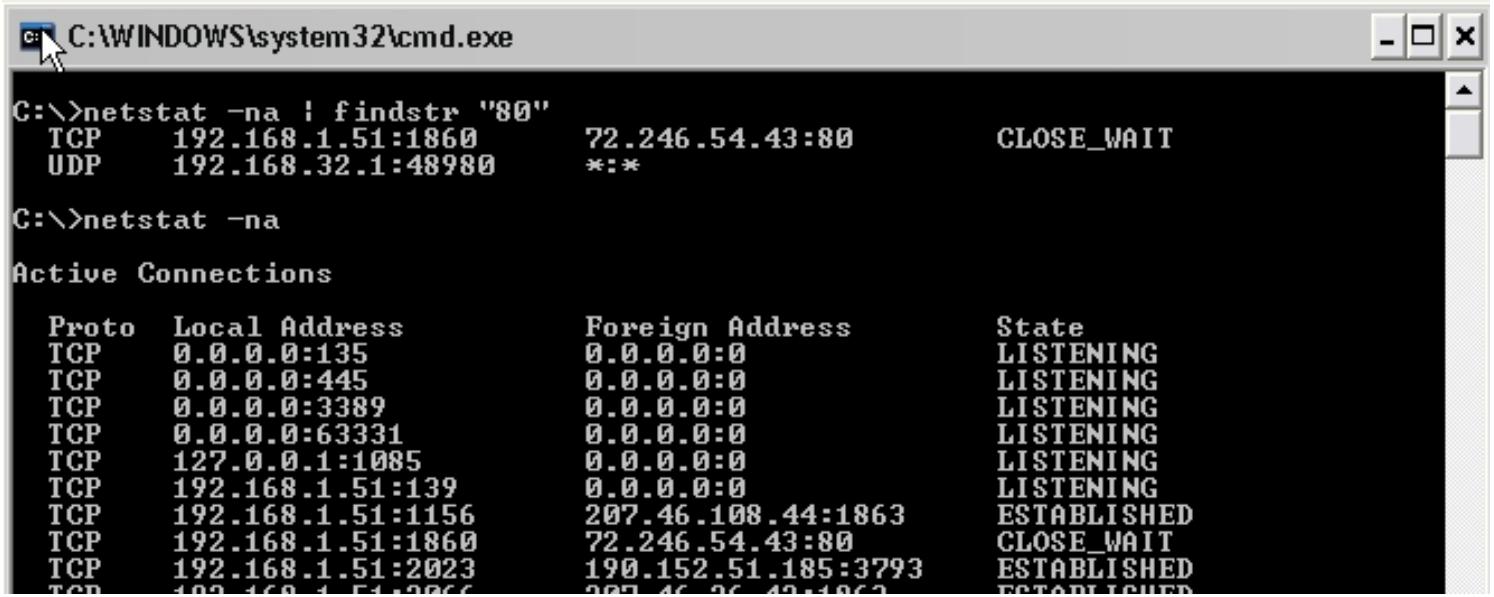
- Aplicaciones de mensajería instantánea
- IRC
- Archivos adjuntos
- Programas malos
- E-mail
- Acceso físico
- Sitios Web desconfiados
- Software Freeware
- Archivos, juegos, screensavers descargos desde Internet
- Netbios
- Paquetes de código

Indicadores de un ataque de troyanos

- El puntero del mouse desaparece
- El cd-rom se abre y cierra
- El Taskbar desaparece
- No trabaja el CTRL+ALT+DEL
- El computador se resetea
- El botón Inicio desaparece
- La pantalla parpadea
- Se conecta a páginas Web desconocidas
- Personas chateando con la víctima saben mas de lo permitido
- Estados de cuenta de compras no realizadas
- Etc

Como determinar que puertos están en “escucha”

- netstat –na
- En Windows netstat –na | findstr <numero_puerto>
- En Linux netstat –na | grep <numero_puerto>



Wrappers

Programas que permiten ligar un Troyano con un archivo legítimo

- Un Wrapper adjunta una aplicación .exe al ejecutable del Troyano
- Los dos programas son juntados en un solo archivo
- Cuando la víctima ejecuta este archivo, se instala el Troyano en background y ejecuta la aplicación en foreground
- La víctima solamente ve la aplicación legítima

Algunos Troyanos

- Netcat (nc)
- Tini
- MoSucker
- Beast
- Netbus
- Nuclear

Por qué los troyanos?

Los troyanos son escritos para roban información de otros sistemas y ejecutar control sobre ellos.

- Información de Tarjetas de crédito
- Documentos confidenciales
- Direcciones de email, contraseñas, cuentas de usuario, etc.
- Datos financieros
- Usar el equipo de la víctima para propósito ilegal, como hack, escaneo, filtrados, etc.

Qué es Sniffing?

Un Sniffer es un programa o dispositivo que monitorea los datos transfiriéndose sobre la red. Los Sniffers pueden ser utilizados para actividades lícitas como la administración de la red, así como también para actividades ilícitas para robar información de la red

El objetivo de Sniffing es para robar:

- Contraseñas
- E-mail
- Archivos en transferencia

Protocolos vulnerables a Sniffing

- Telnet
- Rlogin
- HTTP
- SMTP
- NNTP
- POP
- FTP
- IMAP

Tipos de Sniffing

- Hay dos tipos de Sniffing:
  - Sniffing Pasivo
    - Sniffing a través de un Hub
  - Sniffing Activo
    - Sniffing a través de un switch
      - ARP Spoofing
      - MAC Flooding
      - MAC Duplicating

ARP Spoofing

- ARP Resuelve direcciones IP a direcciones MAC de la interfase que envía el dato
- Los paquetes ARP pueden ser forjados a enviar datos al equipo del hacker
- Un hacker puede usar ARP Poisoning para interceptar tráfico de red
- Haciendo un MAC Flooding en la tabla ARP de un Switch con paquetes ARP reply hechos spoffing, éste se sobrecarga y se pone en “modo forwarding” permitiendo hacer un Sniffing libre

MAC Flooding

- MAC Flooding involucra inundar el switch con numerosos requisitos
- Los switches tienen limitada memoria para administrar todos esos requisitos de direcciones MAC a puertos físicos
- MAC Flooding hace uso de esa limitación para bombardear el switch
- El switch actúa como hub permitiendo hacer un broadcast de todos los paquetes, así el sniffing es fácilmente ejecutado

MAC Duplicating

- Inicia haciendo un sniffing en la red para encontrar direcciones MAC de clientes que están asociadas con un puerto en el switch, y re-usa una de estas direcciones
- Un usuario malicioso puede interceptar y usar una dirección MAC legítima
- El hacker recibe todo el tráfico destinado al usuario legítimo

Herramientas

Ethereal es un analizador de protocolos de red para UNIX y Windows, examina paquetes en tiempo real en la red

tcpdump permite interceptar y desplegar paquetes TCP/IP y otros paquetes siendo transmitidos o recibidos en la red

Ettercap permite hacer sniffinig IP en redes con switches, permite tambíen MAC Sniffing, OS Fingerprinting, ARP Poisoning

Herramientas adicionales

- Arpspoof
- Macof
- Etherflood
- Nemesis
- Dsniff
- Dnsspoof
- Mailsnarf

Demo

HACKING DE SERVIDORES WEB

Hacking de Servidores Web

- Hacking Web
- Vulnerabilidades en Aplicaciones Web
- Inyección SQL

Demo

GRACIAS