



Herramientas y Técnicas de Hacking y Cracking y cómo protegerse ante ellas

Gonzalo Álvarez Marañón

CSIC



Temas a tratar

- ◆ **Herramientas de hacking disponibles en Internet y su funcionamiento**
- ◆ **Cómo proteger servidores para evitar intrusiones de hackers desde Internet**
- ◆ **Herramientas disponibles para minimizar el riesgo de ataque de hackers**



Estructura

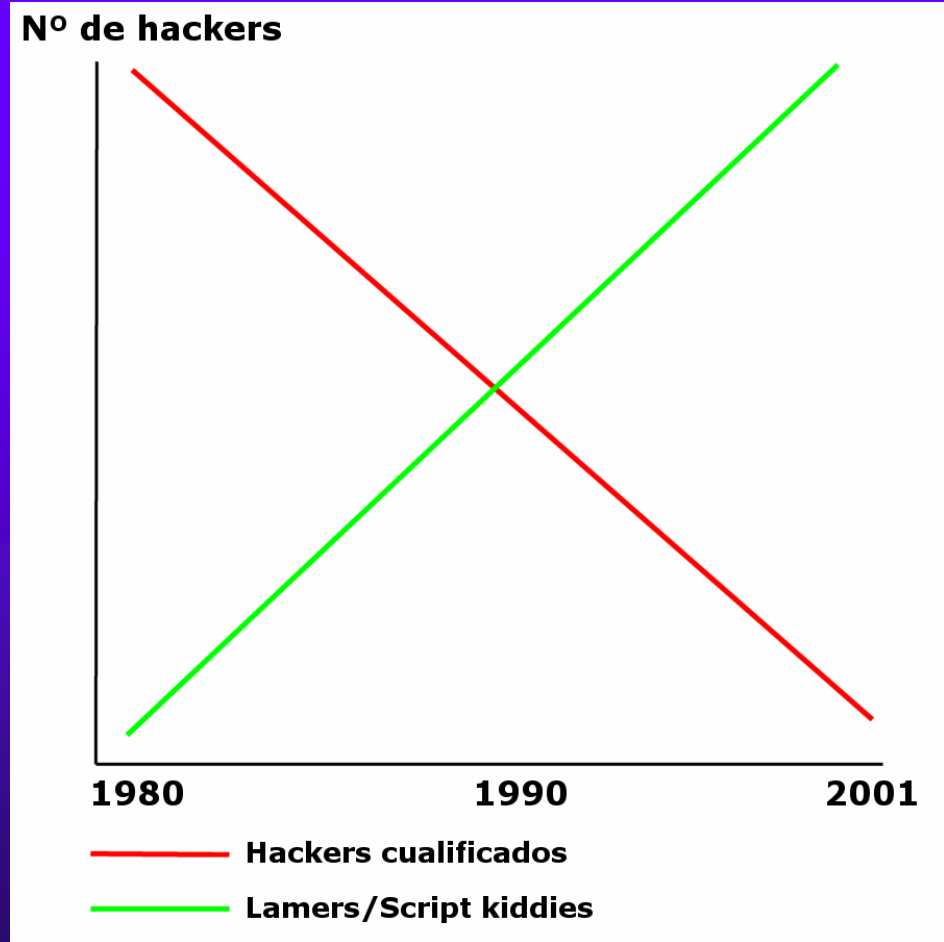
- ◆ Identificación de un objetivo
- ◆ Recopilación de información sobre el blanco
- ◆ Análisis de la información e identificación de vulnerabilidades
- ◆ Obtención del nivel de acceso apropiado
- ◆ Realización del ataque sobre el objetivo
- ◆ Completar el ataque



Introducción

- ◆ Semejanzas con ataque a un objetivo físico
- ◆ Herramientas automatizadas de ataque en Internet
- ◆ Cualquiera puede ser hacker (hasta mi abuela)

Sofisticación del hacker





Identificación de un objetivo

- ◆ Objetivo predeterminado
- ◆ Motivaciones:
 - Empleado descontento
 - Odio visceral contra la compañía o personas
 - Prestigio del objetivo
 - Espionaje industrial
 - Puro aburrimiento
- ◆ ¿Otros objetivos?



Identificación de un objetivo

- ◆ Objetivo aleatorio: ordenador conectado a Internet permanentemente: RDSI, ADSL, etc.
- ◆ Motivaciones:
 - Practicar, para atacar bocados más apetitosos
 - Utilizar su sistema como cabeza de puente
 - Diversión con los amigos
- ◆ ¡¡¡Todos somos víctimas!!!



Ataque

- ◆ Hacerse con la dirección IP o de teléfono de la máquina
- ◆ Herramientas
 - Host scan
 - Barridos de ping (SolarWinds)
 - War dialers
 - Buscadores de Internet



Defensa

- ◆ Cortafuegos
 - Cortan el acceso (filtrado de paquetes en W2000)
- ◆ Sistemas de Detección de Intrusos (IDS)
 - Detectan intentos de acceso, incluso interno
- ◆ Proxy
- ◆ Apagar el ordenador cuando no se usa
- ◆ No dejar líneas telefónicas directas



Recopilación de información

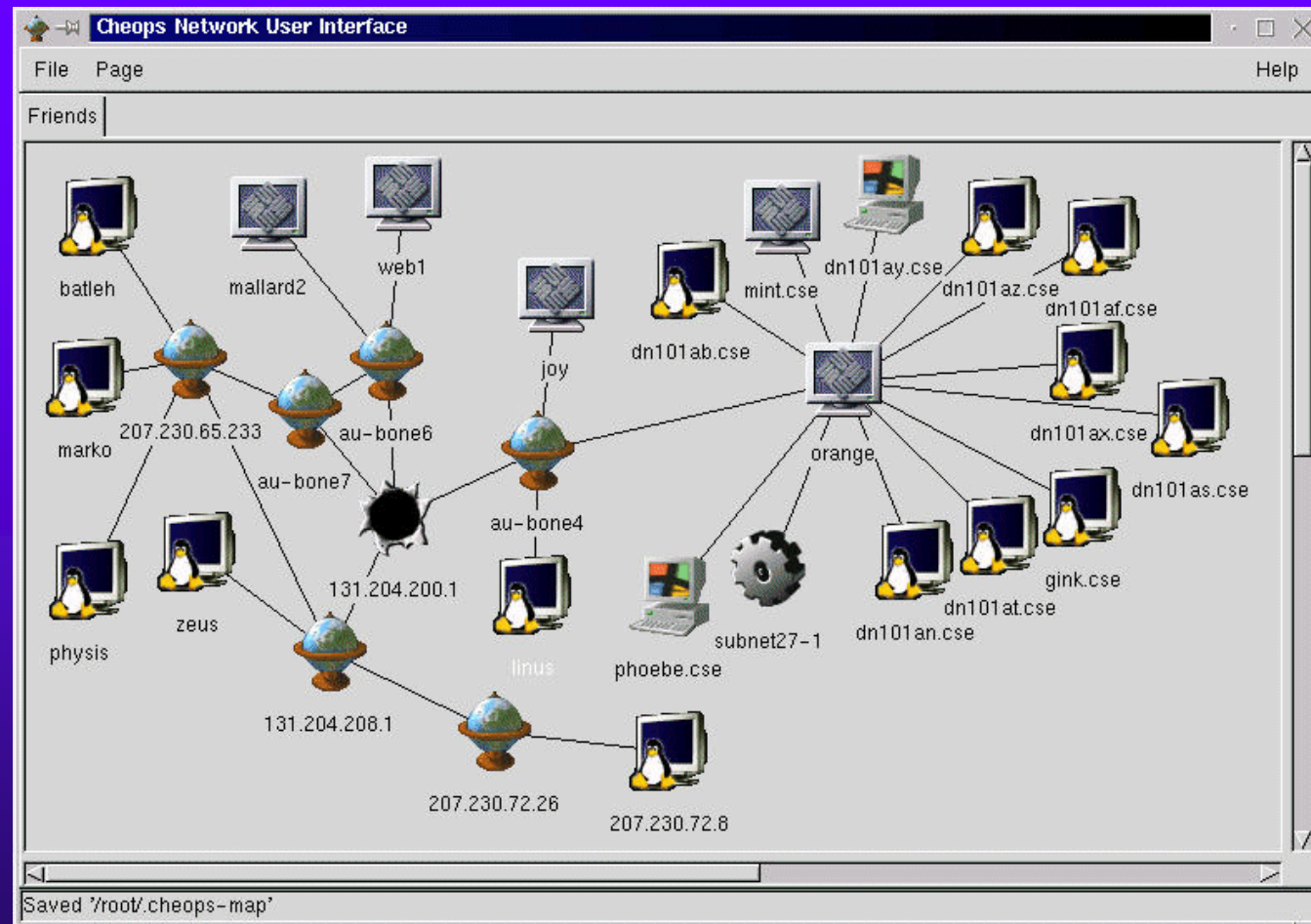
- ◆ Sistema operativo y versión
- ◆ Servicios abiertos y su versión
- ◆ Topología de red: equipos en activo
- ◆ Controladores de dominio
- ◆ Recursos compartidos
- ◆ Información de usuarios
- ◆ Información de la organización



Ataque

- ◆ Exploración de puertos: SuperScan
- ◆ Whois (Sam Spade)
- ◆ NSLookup y dig (Sam Spade)
- ◆ Rastreo de pila (nmap)
- ◆ Trazas (SolarWinds, SO)
- ◆ Captura de cabeceras (wfetch)
- ◆ Sitio web con información de la compañía
- ◆ Ingeniería social
- ◆ Búsqueda en las news

Cheops





Nmap

Nmap Front End v1.6

File Output Help

Host(s): xanadu vectra playground Scan. Exit

Scan Options: General Options:

- connect()
- SYN Stealth
- Ping Sweep
- UDP Port Scan
- FIN Stealth
- Bounce Scan:

- Don't Resolve
- Fast Scan
- Range of Ports:
- Use Decoy(s):

- TCP Ping
- TCP&ICMP
- ICMP Ping
- Don't Ping
- Input File:

- Fragmentation
- Get Identd Info
- Resolve All
- OS Detection
- Send on Device:

Output from: nmap -sS -O -Dantionline.com xanadu vectra playground

Interesting ports on vectra.yuma.net (192.168.0.5):

Port	State	Protocol	Service
13	open	tcp	daytime
21	open	tcp	ftp
22	open	tcp	ssh
23	open	tcp	telnet
37	open	tcp	time
79	open	tcp	finger
111	open	tcp	sunrpc
113	open	tcp	auth
513	open	tcp	login
514	open	tcp	shell

TCP Sequence Prediction: Class=random positive increments
Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net (192.168.0.1):

Port	State	Protocol	Service
------	-------	----------	---------



Defensa

- ◆ Deshabilitar transferencias de zona en DNS
- ◆ Cortafuegos
- ◆ Deshabilitar servicios no usados
 - SNMP, NetBios, Finger, FTP, ...
- ◆ Sistemas de Detección de Intrusos (IDS)
- ◆ Protección física del servidor
- ◆ Aislamiento de protocolo



Análisis de la información e identificación de vulnerabilidades

◆ Hacker autodidacta

- Cortafuegos mal configurado, un servidor web mal instalado, base de datos desprotegida, fallo en un protocolo poco conocido, generador de números aleatorios no tan aleatorio
- Escribe su propio script para automatizar la explotación del agujero
- Requisito: experto en redes, protocolos y programación



Análisis de la información e identificación de vulnerabilidades

◆ Lamer o script kiddie

- Aprovecha vulnerabilidades descubiertas por los primeros y los programas escritos por ellos
- Frecuenta sitios underground
- Requisito: tiempo libre



Ataque

- ◆ Búsqueda de vulnerabilidades en Internet:
 - Buscadores convencionales
 - Astalavista
- ◆ Sondas automatizadas



Defensa

- ◆ Parches y Service Packs actualizados para el servidor
- ◆ Configuración segura de servidores
- ◆ Huir de caminos por defecto
- ◆ Eliminar ejemplos y lo que no se utilice
- ◆ Programación responsable de aplicaciones web
- ◆ Checklists de seguridad



Obtención del nivel de acceso apropiado

- ◆ Normalmente, conexión anónima pública
- ◆ Escalada de privilegios: ascender hacia usuarios con mayor poder sobre la máquina o red
- ◆ Objetivo: administrador del sistema
- ◆ Primer paso: averiguar nombre y contraseña de un usuario válido



Ataque

- ◆ Reventadores de contraseñas: para archivo en local y para red
- ◆ Sortear el cortafuegos: a través del correo, de HTTP, base de datos, etc., buscando agujeros en esos servicios (OSQL, XP)
- ◆ Desbordamientos de buffer
- ◆ Troyanos (EliteWrap)



Defensa

- ◆ Cortafuegos bien configurado
- ◆ Últimas versiones de los programas
- ◆ Parches de seguridad
- ◆ Auditoría (logs)
- ◆ Habilitar políticas para contraseñas fuertes
- ◆ Cuidadoso establecimiento de los permisos NTFS
- ◆ Protección del Registro



Realización del ataque

- ◆ Con una cuenta de privilegio adecuado:
 - Cambiará la página web del sitio atacado
 - Robará la base de datos
 - Modificará un registro que almacena su saldo en una cuenta bancaria
 - Tirará abajo el servidor (ataque DoS)
 - ...
- ◆ Puede olvidarse para siempre del objetivo...
- ◆ ... ¡o regresar de nuevo en el futuro!



Ataque

- ◆ Puertas traseras en cuentas privilegiadas para control remoto
- ◆ Monitores de red
- ◆ Canales subliminales
- ◆ Agentes distribuidos



Defensa

- ◆ Sistemas de Detección de Intrusos (IDS)
- ◆ Integridad del sistema de archivos



Completar el ataque

- ◆ ¿Qué huellas deja un atacante?
 - Eliminar las evidencias
- ◆ Desactivar o parchear el demonio o servicio con el error que permitió entrar
- ◆ Evitar la respuesta



Ataque

◆ Rootkit

- Creación de puertas traseras (puntos de entrada al sistema) para uso futuro
- Manipulación de los ficheros log para borrar toda evidencia
- Modificación o reemplazo de herramientas del sistema para evitar ser detectado por el administrador (`_rootkit_`)
- Monitorización del tráfico de red o de pulsaciones de teclas (Iris)
- Lanzamiento de ataques contra otros sistemas, por ejemplo, de denegación de servicio



Defensa

- ◆ Redirigir la salida de los ficheros de log
- ◆ Programas de detección de rootkit
- ◆ Integridad del sistema de archivos
- ◆ Detección de tarjetas en modo promiscuo



Conclusiones

- ◆ Es muy fácil ser hacker
- ◆ Todos somos víctimas potenciales
- ◆ Es muy fácil protegerse ante ataques de lamers/script kiddies
- ◆ Protección relativa frente a hackers “pata negra” y ataques internos
- ◆ Necesidad de formación del personal de administración y de los usuarios



Contacto

- ◆ Email:

- gonzalo@iec.csic.es

- ◆ Web:

- www.iec.csic.es/cryptonomicon