Herramientas para hacking

Víctor Nieves Sánchez

Última modificación 26 de julio de 2020

Disclaimer

Este documento se ha elaborado por los autores, obteniendo información de diversos recursos.

El objetivo de este documento es proporcionar una breve referencia de ayuda para el lector.

Índice

1. Introducción

Este documento enumera una serie de herramientas útiles para hacking.

2. Sniffers

Un ***Sniffer*** es un programa que captura y analiza paquetes de red, tanto de entrada como de salida.

- **Wireshark**[42]: *Wireshark* es el *sniffer* de red más popular, con soporte en diversas plataformas.
- **Tcpdump**[17]: *Tcpdump* es un *sniffer* de linea de comandos disponible tanto en Linux como Unix.
- **Windump**[41]: *Windump* es la versión para Windows de *tcpdump*[17].
- **Cain & Abel**[5]: *Cain & Abel* es una herramienta "todo en uno" para capturar paquetes, grabar contraseñas usadas en un ataque *MiTM*[16], crackear hashes de contraseñas utilizando métodos como ataques de diccionario, de fuerza bruta y ataques basados en "criptoanálisis" y ataques de *ARP[39] y DNS[40] poisoning.*
- **Kismet**[14]: *Kismet* es una herramienta para *sniffing* de redes inalámbricas, que sirve para para localizar y descubrir SSID's ocultas. También puede ser usada como un *sniffer* pasivo de tráfico.
- **Ntop**[26]: *Ntop* es una página web para analizar el tráfico web.
- **Network Miner**[24]: *Network Miner* es un *sniffer*, capaz de identificar el sistema operativo. Automáticamente extrae los archivos contenidos en los paquetes capturados, incluyendo imágenes.

3. Scanners

La fase de ***scanning*** usa diversos procedimientos para identificar máquinas "vivas", así como los puertos abiertos, servicios desplegados, sistema operativo, arquitectura, etc. Se utilizan estas herramientas para identificar posibles vulnerabilidades o amenazas.
El escaneo de la red se usa para poder generar un perfil de la organización del objetivo.

- **Nmap**[25]: *Nmap* utiliza paquetes IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y versiones) están ejecutando, qué tipo de paquetes de filtros/*firewalls* están en uso, y docenas de otras características.
- **Zenmap**[43]: *Zenmap* es la versión gráfica de *nmap*[25].
- **Angry IP Scanner**[3]: *Angry IP Scanner* o ***ipscan*** es un *scanner* de red *open-source* diseñado para ser rápido y sencillo de usar. Escanea direcciones IP y puertos además de otras muchas características.
- **hping3**[11]: *hping3* es una herramienta de línea de comandos orientado TCP/ensamblador de paquetes IP/analizador.
- **NetScan Tools**[23]: es una herramienta gráfica "todo en uno" soportada para sistemas Windows.
- **Nessus**[7]: *Nessus* es un escáner de vulnerabilidades usado por pentesters, hackers y empresas centradas en la ciberseguridad.
- **SuperScan**[35]: *SuperScan* nos permite escanear rangos de IP y escaneo de puertos. Soporta *banner grabbing, ping, whois, tracert*, etc.
- **zANTI**[28]: Es un software de *Android* usado para escanear puertos, realizar ataques MiTM[16], robo de sesión, redirecciones, etc.
- **NBTScan** [20]: *NBTScan* es una herramienta de línea de comandos que busca servidores de nombres NETBIOS[21] abiertos en una red TCP/IP local o remota.

4. Enumeration

La enumeración se define como el proceso de extracción de información, como nombres de usuario, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema.

- **DumpSec**[8]: *DumpSec* es un programa de auditoría de seguridad para Windows que sirve para revelar usuarios, grupos, impresoras, recursos compartidos, información de registro y demás en un formato fácil de leer. También es muy útil para encontrar información sobre el sistema operativo para fines de escalada de privilegios.

- **SuperScan** [35]: La misma herramienta mencionada en el apartado anterior. También es usada para enumeración.

- **Sublist3r**[1]: *Sublist3r* es una herramienta escrita en *Python* diseñada para enumerar subdominios de sitios web usando OSINT[37].

- **Netcat**[22]: Es una herramienta simple que puede leer y escribir datos a través de una conexión TCP o UDP. Es muy útil porque puede crear casi cualquier tipo de conexión, incluyendo un enlace de sesión. Eso permite a los actores crear conexiones de *shell* e *shell inversa* entre dos máquinas (*endpoints*). Permite también enviar y recibir archivos, y ejecutar comandos tanto en el host como sistemas comprometidos.

- **Cryptcat**[6]: Es una variante de *Netcat*[22] que encripta las comunicaciones, haciéndola una herramienta útil para evadir los IDS o el *sniffing*.

- **TCPView**[36]: *TCPView* es una herramienta que enumera todas las conexiones TCP y UDP del *endpoing* de la aplicación. Resuelve nombres de dominio para las IPs conectadas al sistema, además permite monitorizar los cambios en las conexiones y también permite cerrarlas.

5. Password Cracking

El descifrado de contraseñas o *password cracking* es el proceso de recuperación de contraseñas que se han almacenado en un equipo. Un acercamiento común es el ataque de fuerza bruta el cual consiste en adivinar repetitivamente la contraseña y corroborar contra un hash criptográfico existente de la contraseña.

El descifrado de contraseñas puede servir para ayudar a un usuario a recuperar alguna contraseña olvidada, para obtener acceso no autorizado a un sistema, o ser implementada como medida preventiva por los administradores del sistema para buscar contraseñas fácilmente manipulables.

- **L0phtCrack**[15]: Esta herramienta es usada para recuperar información sobre usuarios remotos o locales y para recuperar las correspondientes contraseñas.
- **Ophcrack**[27]: Es una versión gratuita de *l0phtcrack*[15], con alguna caracteristica menos.
- **John the Ripper**[13]: es una herramienta gratuita y *open source* que permite crear reglas y usar listas personalizadas de contraseñas para recuperar.
- **Trinity Rescue Kit**[38]: *Trinity Rescue Kit (TRK)* es una distribución Linux que se ejecuta como un *LiveCD* (es decir, se inicia desde el arranque de la máquina) para poder escanear y comprobar los discos duros desde fuera.
- **Medusa**[18]: Es una herramienta rápida y modular que usa fuerza bruta en servicios de red como *HTTP, MySQL, SMB, SMTP,* etc.
- **RainbowCrack**[30]: Esta herramienta usa *rainbow tables*[29] para reducir el tiempo que se invierte en las tareas de fuerza bruta.

6. Wireless Tools

En esta sección se enumeran algunas herramientas que se usan en redes *wireless*

- **Kismet**[14]: Como ya se mencionó en el apartado de *sniffing*, esta herramienta proporciona varias utilidades.
- **inSSIDer**[12]: Esta herramienta es usada como monitor local de tráfico *WiFi*.
- **Reaver**[31]: *Reaver* implementa un ataque de fuerza bruta contra los *WiFi Protected Setup* (WPS) para recuperar las claves WPA/WPA2.
- **Bluesnarfer**[4]: Una herramienta usada para obtener información de un dispositivo móvil a través de conexión bluetooth.
- **Aircrack-ng**[2]: *Aircrack-ng* es un conjunto de herramientas para evaluar redes *WiFi*. Se centra en las áreas de monitorización, ataque, testing y cracking de contraseñas.
- **Airmon-ng**[9]: Herramienta de *sniffing* de *Aircrack-ng*[2].
- **Airodump-ng**[10]: Herramienta de *Aircrack-ng*[2] usada para capturar paquetes *802.11*. Esta herramienta también es capaz de mostrar cordenadas GPS.

7. Otras herramientas

- **Snort**[34]: *Snort* es una herramienta gratuita que sirve como *IDS*[32] e *IPS*[33].
- **Metasploit**[19]: Es un *framework* automatizado capaz de explotar vulnerabilidades en varias plataformas.

8. Referencias

[1] *aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers.* URL: https://github.com/aboul3la/Sublist3r (visitado 13-07-2020).

[2] *Aircrack-ng.* URL: https://www.aircrack-ng.org/ (visitado 19-07-2020).

[3] *Angry IP Scanner - Download for Windows, Mac or Linux.* URL: https://angryip.org/download/%7B%5C#%7Dlinux (visitado 12-07-2020).

[4] *Bluesnarfer — Penetration Testing Tools.* URL: https://tools.kali.org/wireless-attacks/bluesnarfer (visitado 19-07-2020).

[5] *Cain and Abel (software) - Wikipedia.* URL: https://en.wikipedia.org/wiki/Cain%7B%5C_%7Dand%7B%5C_%7DAbel%7B%5C_%7D(software)%7B%5C#%7D:%7B~%7D:text=Cain%20and%20Abel%20(often%20abbreviated,brute%20force%20and%20cryptanalysis%20attacks. (visitado 12-07-2020).

[6] *CryptCat — Alonso Caballero / ReYDeS.* URL: http://www.reydes.com/d/?q=CryptCat (visitado 13-07-2020).

[7] *Descargue la Evaluación de vulnerabilidades Nessus — Tenable®.* URL: https://es-la.tenable.com/products/nessus (visitado 12-07-2020).

[8] *DumpSec – SecTools Top Network Security Tools.* URL: https://sectools.org/tool/dumpsec/ (visitado 13-07-2020).

[9] *es:airmon-ng [Aircrack-ng].* URL: https://www.aircrack-ng.org/doku.php?id=es:airmon-ng (visitado 19-07-2020).

[10] *es:airodump-ng [Aircrack-ng].* URL: https://www.aircrack-ng.org/doku.php?id=es:airodump-ng (visitado 19-07-2020).

[11] *Hping3 « Kali Linux – Documentación en español.* URL: https://kali-linux.net/article/hping3/ (visitado 12-07-2020).

[12] *inSSIDer - Defeat Slow WiFi.* URL: https://www.metageek.com/products/inssider/ (visitado 19-07-2020).

[13] *John the Ripper password cracker.* URL: https://www.openwall.com/john/ (visitado 26-07-2020).

[14] *Kismet - Kismet.* URL: https://www.kismetwireless.net/ (visitado 12-07-2020).

[15] *L0phtCrack Password Security – Auditing and Cracking – Auditing, cracking and recovering passwords.* URL: https://www.l0phtcrack.com/ (visitado 26-07-2020).

[16] *Man-in-the-middle attack - Wikipedia.* URL: https://en.wikipedia.org/wiki/Man-in-the-middle%7B%5C_%7Dattack (visitado 12-07-2020).

[17] *Manpage of TCPDUMP.* URL: https://www.tcpdump.org/manpages/tcpdump.1.html (visitado 12-07-2020).

[18] *Medusa - Penetration Testing Tools.* URL: https://en.kali.tools/?p=200 (visitado 26-07-2020).

[19] *Metasploit — Penetration Testing Software, Pen Testing Security — Metasploit.* URL: https://www.metasploit.com/ (visitado 26-07-2020).

[20] *nbtscan - NETBIOS nameserver scanner.* URL: http://www.unixwiz.net/tools/nbtscan.html (visitado 13-07-2020).

[21] *NetBios - EcuRed.* URL: https://www.ecured.cu/NetBios (visitado 13-07-2020).

[22] *Netcat, la navaja suiza de TCP/IP.* URL: https://crysol.github.io/recipe/2005-10-10/netcat-la-navaja-suiza-de-tcp-ip.html%7B%5C#%7D.XwymhHUzaA0 (visitado 13-07-2020).

[23] *NetScanTools® Network Engineering Tools and the Managed Switch Port Mapping Tool.* URL: https://www.netscantools.com/ (visitado 12-07-2020).

[24] *NetworkMiner - The NSM and Network Forensics Analysis Tool.* URL: https://www.netresec.com/?page=NetworkMiner (visitado 12-07-2020).

[25] *Nmap: the Network Mapper - Free Security Scanner.* URL: https://nmap.org/ (visitado 12-07-2020).

[26] *ntop – High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware.* URL: https://www.ntop.org/ (visitado 12-07-2020).

[27] *Ophcrack.* URL: https://ophcrack.sourceforge.io/ (visitado 26-07-2020).

[28] *Penetration Testing for Mobile Applications Pentesting Toolkit — zANTI.* URL: https://www.zimperium.com/zanti-mobile-penetration-testing (visitado 13-07-2020).

[29] *Rainbow table - Wikipedia.* URL: https://en.wikipedia.org/wiki/Rainbow%7B%5C_%7Dtable (visitado 26-07-2020).

[30] *RainbowCrack — Penetration Testing Tools.* URL: https://tools.kali.org/password-attacks/rainbowcrack (visitado 26-07-2020).

[31] *Reaver — Penetration Testing Tools.* URL: https://tools.kali.org/wireless-attacks/reaver (visitado 19-07-2020).

[32] *Sistema de detección de intrusos - Wikipedia, la enciclopedia libre.* URL: https://es.wikipedia.org/wiki/Sistema%7B%5C_%7Dde%7B%5C_%7Ddetecci%7B%5C'%7Bo%7D%7Dn%7B%5C_%7Dde%7B%5C_%7Dintrusos (visitado 26-07-2020).

[33] *Sistema de prevención de intrusos - Wikipedia, la enciclopedia libre.* URL: https://es.wikipedia.org/wiki/Sistema%7B%5C_%7Dde%7B%5C_%7Dprevenci%7B%5C'%7Bo%7D%7Dn%7B%5C_%7Dde%7B%5C_%7Dintrusos (visitado 26-07-2020).

[34] *Snort - Network Intrusion Detection & Prevention System.* URL: https://www.snort.org/ (visitado 26-07-2020).

[35] *Superscan – SecTools Top Network Security Tools.* URL: https://sectools.org/tool/superscan/ (visitado 13-07-2020).

[36] *TCPView for Windows - Windows Sysinternals — Microsoft Docs.* URL: https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview (visitado 19-07-2020).

[37] *Técnicas y herramientas OSINT para la investigación en Internet — WeLiveSecurity.* URL: https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/%7B%5C#%7D:%7B~%7D:text=OSINT%20significa%20Open%20Source%20Intelligence,correlacionar%20los%20datos%20y%20procesarlos. (visitado 13-07-2020).

[38] *Trinity Rescue Kit — CPR for your computer - Trinityhome.* URL: https://trinityhome.org/ (visitado 26-07-2020).

[39] *What is ARP Spoofing — ARP Cache Poisoning Attack Explained — Imperva.* URL: https://www.imperva.com/learn/application-security/arp-spoofing/ (visitado 12-07-2020).

[40] *What is DNS Spoofing — Cache Poisoning Attack Example — Imperva.* URL: https://www.imperva.com/learn/application-security/dns-spoofing/ (visitado 12-07-2020).

[41] *WinDump - Home.* URL: https://www.winpcap.org/windump/ (visitado 12-07-2020).

[42] *Wireshark · Go Deep.* URL: https://www.wireshark.org/ (visitado 12-07-2020).

[43] *Zenmap - Official cross-platform Nmap Security Scanner GUI.* URL: https://nmap.org/zenmap/ (visitado 12-07-2020).