sepian

Seguridad Digital
de Andalucía

Pentesting con Kali Linux

Junta de Andalucía

Recolección de información.

- La recolección de información se ubica en la primera etapa del proceso de ethical hacking y su finalidad es extraer cuanta más información mejor sobre la infraestructura que estamos evaluando.

- Existen innumerables fuentes de información que ayudarán al hacker a probar la seguridad de los sistemas y que son de notable ayuda para usar Kali Linux.

Recolección de información.

- Kali Linux ofrece una miríada de soluciones de reconocimiento, todas ellas OSINT.
- Netcraft, Whois, Reconocimiento de DNS, Maltego,…
- Vamos a echar un vistazo a lo que Kali ofrece.

Recolección de información.

- Bases de datos de vulnerabilidades (externas a Kali). Visita la página www.cve-details.com, www.exploit-db.com

- Las vulnerabilidades se etiquetan según diferentes estándares internacionales. https://www.youtube.com/watch?v=GEKSdEFBZAQ

Recolección de información.

- Nessus: De la empresa Tenable Security
  https://es-la.tenable.com/products/nessus

- Se instala en Kali como servicio y descarga la base de datos de vulnerabilidades.

- https://Kali:8834

Recolección de información.

- **Nikto**: Escáner de vulnerabilidad web incluido en Kali

- Especializado en OSVDB (Open Source Vulnerability Database) https://en.wikipedia.org/wiki/Open_Source_Vulnerability_Database

Recolección de información.

- **Maltego**: Permitirá al hacker hacerse una idea de cómo funciona la organización víctima y le ayudará a determinar el punto más apropiado para realizar el ataque (sistemas o personas)

- No se trata de vulnerabilidades al uso, sino de descubrir relaciones entre los componentes de una organización.

Recolección de información.

- Podemos usar los **scripts de nmap** para obtener información de calidad

Pentesting con Kali

- Las vulnerabilidades pueden estar presentes en el sistema operativo o en las aplicaciones.

- El ecosistema **metasploit** es el producto estrella de Kali, pero no es el único.

Pentesting con Kali

- Las vulnerabilidades pueden estar presentes en el sistema operativo o en las aplicaciones.

- El ecosistema **Metasploit** es el producto estrella de Kali, pero no es el único.

Pentesting con Kali

- Necesitamos encontrar una vulnerabilidad presente en el sistema operativo de la víctima (pe MS08-067)
- Requiere que la víctima no disponga de antivirus activo (Más adelante trataremos la evasión de antivirus)
- Hacer práctica con MS08-067 y Windows XP

Pentesting con Kali

- Idealmente necesitamos una vulnerabilidad en aplicación instalada (no es estrictamente necesario, p.e. PowerShell).
- Necesitamos la colaboración de un usuario (Ingeniería social)
- El ataque requiere dos partes: Crear un **malware** y un **listener**.
- Hacer práctica de standalone payload

Pentesting con Kali

- Es la base de todos los ataques MitM.
- Permite al hacker recibir el tráfico que transfieren dos máquinas a pesar de usar switches.
- Son detectados muy fácilmente por los sistemas IDS de la electrónica de red (switches de gama alta)
- Práctica de **arpspoof**

Pentesting con Kali

- **MitM** en una conexión SSL provoca advertencias de certificado. Hacer práctica
- ¿Es posible hacer un MitM “limpio” que no muestre errores de certificado?
- Hacer práctica de **sslstrip**

Pentesting con Kali

- Robar hashes con **Meterpreter**
- Obtener los hashes con **sampdump2** desde **system** y **sam**
- ¿Cómo podrías robar hashes con acceso físico a un equipo?

Pentesting con Kali

- **John the Ripper**
- La criptografía, el ajedrez, los hashes y las **Rainbow Tables** http://project-rainbowcrack.com/
- Reventar passwords con el Editor de Credenciales de Windows https://www.ampliasecurity.com/research/windows-credentials-editor/

Pentesting con Kali

- **Acrobat reader** presenta históricamente muchas vulnerabilidades porque es interesante hacerle ingeniería inversa al ser muy utilizada.

- Hacer práctica **adobe_utilprintf**

Pentesting con Kali

- SET (Social-Engineer ToolKit)
- Incrustación de malware el ejecutables.
- Hacer práctica de **radmin**

Pentesting con Kali

- www.virustotal.com
- Ofuscación de malware con **msfvenom** y **encoders** de Metasploit
- Usar encoders personalizados.
- **Veil** https://github.com/Veil-Framework/Veil-Evasion

Pentesting con Kali (recursos adicionales)

Anonimizar el tráfico de Kali:
https://hacking-etico.com/2016/11/07/anonimizando-la-kali-anonym8/

Use MDK3 for Advanced Wi-Fi Jamming:
https://null-byte.wonderhowto.com/how-to/use-mdk3-for-advanced-wi-fi-jamming-0185832/

Scan, Fake & Attack Wi-Fi Networks with the ESP8266-Based WiFi Deauther:
https://null-byte.wonderhowto.com/how-to/scan-fake-attack-wi-fi-networks-with-esp8266-based-wifi-deauther-0193837/

Pentesting con Kali (recursos adicionales)

Program a $6 NodeMCU to Detect Wi-Fi Jamming Attacks in the Arduino IDE:
https://null-byte.wonderhowto.com/how-to/program-6-nodemcu-detect-wi-fi-jamming-attacks-arduino-ide-0186356

Métodos de evasión de una sandbox:
https://hacking-etico.com/2019/04/22/metodos-de-evasion-de-una-sandbox/

Convertir un payload .EXE en .PPT (Parte 1):
https://hacking-etico.com/2017/07/27/ingenieria-social-camuflando-un-payload/

Pentesting con Kali (recursos adicionales)

Convertir un payload .EXE en .PPT (Parte 2):
https://hacking-etico.com/2017/07/31/ingenieria-social-camuflando-payload-parte-2/

How to Create an Undetectable Payload, Part 1 (Bypassing Antivirus Software):
https://null-byte.wonderhowto.com/how-to/hacking-windows-10-create-undetectable-payload-part-1-bypassing-antivirus-software-0185055/

Pentesting con Kali (recursos adicionales)

How to Create an Undetectable Payload, Part 2 (Concealing the Payload):
https://null-byte.wonderhowto.com/how-to/hacking-windows-10-create-undetectable-payload-part-2-concealing-payload-0185060/

How Elliot & Fsociety Destroyed Evil Corp's Data:
https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-elliot-fsociety-destroyed-evil-corps-data-0164755/

Pentesting con Kali (recursos adicionales)

Cambiar potencia de transmisión WiFi (Ilegal): https://phoenyxacademy.com/how-to-increase-the-tx-power-of-alfa-awus036nh-adapter-in-kali-linux/

Getting Started with the Aircrack-Ng Suite of Wi-Fi Hacking Tools: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/

Pentesting con Kali (recursos adicionales)

Echar a tu vecino de su red WiFi:
https://null-byte.wonderhowto.com/how-to/hack-like-pro-get-even-with-your-annoying-neighbor-by-bumping-them-off-their-wifi-network-undetected-0147206/

Ver la relación de asociación de clientes y puntos de acceso (airgraph-ng):
https://null-byte.wonderhowto.com/how-to/spy-network-relationships-with-airgraph-ng-0193309/

Pentesting con Kali (recursos adicionales)

Use Kismet to Watch Wi-Fi User Activity Through Walls:
https://null-byte.wonderhowto.com/how-to/use-kismet-watch-wi-fi-user-activity-through-walls-0182214/

Install Kismet on Ubuntu:
https://kifarunix.com/install-kismet-on-ubuntu-18-04/

Pentesting con Kali (recursos adicionales)

Hack WPA & WPA2 Wi-Fi Passwords with a Pixie-Dust Attack Using Airgeddon: https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

Instalación de airgeddon: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Installation%20&%20Usage

Pentesting con Kali (recursos adicionales)

21 sitios para practicar las habilidades de hacking: https://noticiasseguridad.com/importantes/21-sitios-para-practicar-sus-habilidades-de-hacking-y-ciberseguridad/

sedian Seguridad Digital de Andalucía