Kali Linux

Lorenzo Elguea

Agenda

¿Qué es Kali Linux?

¿Cómo se instala?

¿Qué herramientas trae?

https://www.kali.org/docs/introduction/

Kali Linux

Kali Linux (anteriormente conocido como BackTrack Linux) es una distribución de Linux de código abierto basada en Debian destinada a pruebas de penetración avanzadas y auditorías de seguridad. Lo hace al proporcionar herramientas, configuraciones y automatizaciones comunes que permiten al usuario concentrarse en la tarea que debe completarse, no en la actividad que lo rodea.

Kali Linux contiene modificaciones específicas de la industria, así como varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense, ingeniería inversa, gestión de vulnerabilidades y pruebas de equipo rojo.

Kali Linux es una solución multiplataforma, accesible y de libre disposición para profesionales y aficionados a la seguridad de la información.

Instalación

Existen varios procesos para la instalación:

https://www.kali.org/get-kali/#kali-platforms

1. Instaladores
   https://kali.download/base-images/kali-2023.1/kali-linux-2023.1-installer-amd64.iso
2. Máquinas Virtuales
3. Dispositivos ARM
4. Dispositivos Móviles
5. En la Nube
6. Contenedores
7. USB
8. etc…

Ejercicio 1

Instalar Virtualbox y descargar Kali en formato iso

Crear y Configurar una máquina virtual

Instalar el ISO

Validarse

Herramientas

Más de 600 herramientas de prueba de penetración incluidas

Compatibilidad con una amplia variedad de dispositivos inalámbricos: un punto de conflicto habitual con las distribuciones de Linux ha sido la compatibilidad con las interfaces inalámbricas. Hemos creado Kali Linux para admitir tantos dispositivos inalámbricos como sea posible, lo que le permite ejecutarse correctamente en una amplia variedad de hardware y hacerlo compatible con numerosos dispositivos USB y otros dispositivos inalámbricos.

Soporte multilingüe: aunque las herramientas de penetración tienden a estar escritas en inglés, nos hemos asegurado de que Kali incluya un verdadero soporte multilingüe

Herramientas

01-Information Gathering

02-Vulnerability Analysis

03-Web Application Analysis

04-Database Assessment

05-Password Attacks

06-Wireless Attacks

07-Reverse Engineering

08-Exploitation Tools

09-Sniffing & Spoofing

10-Post Exploitation

11- Forensics

12-Reporting Tools

13-Social Engineering Tools

https://www.kali.org/tools/

Más Importantes

Nmap: una herramienta de escaneo de puertos que se utiliza para descubrir hosts y servicios en una red.

Metasploit Framework: una herramienta de explotación que se utiliza para probar la seguridad de los sistemas y aplicaciones.

Wireshark: una herramienta de análisis de paquetes de red que se utiliza para capturar y analizar el tráfico de red.

Aircrack-ng: una herramienta de seguridad de redes inalámbricas que se utiliza para romper la contraseña de redes WiFi.

John the Ripper: una herramienta de crackeo de contraseñas que se utiliza para probar la fortaleza de las contraseñas.

Más Importantes

Burp Suite: una herramienta de pruebas de penetración para aplicaciones web que se utiliza para encontrar vulnerabilidades en aplicaciones web.

Hydra es un cracker de inicio de sesión paralelizado que admite numerosos protocolos para atacar. Es rápido y flexible.

wpscann: Revisa un sitio en Wordpress y reporta qué plugins están instalados y si esas versiones son obsoletas y/o tienen vulnerabilidades.

Más Importantes

Sqlmap: una herramienta de pruebas de penetración que se utiliza para detectar y explotar vulnerabilidades de inyección SQL en aplicaciones web.

Maltego: una herramienta de inteligencia de amenazas que se utiliza para recopilar y analizar información sobre objetivos específicos.

OSINT Framework: una colección de herramientas de inteligencia de fuentes abiertas que se utilizan para recopilar información de fuentes públicas en línea.

01-Information Gathering

dnsenum [Options] <domain> Muestra la información DNS de un dominio

dnsenum up.edu.mx

lbd domain [port] {https} Comprueba si un dominio determinado utiliza equilibrio de carga.

lbd up.edu.mx

nmap [Scan Type(s)] [Options] {target specification} Descubrimiento de Red y auditoría de seguridad

nmap --script ssl-enum-ciphers -p 443 www.up.edu.mx

sudo nmap -sU -p 161 --script=snmp-info 172.25.232.0/23

nmap -F 172.25.0.0/16

01-Information Gathering

Netdiscover es una herramienta de reconocimiento de direcciones activo/pasivo, desarrollada principalmente para aquellas redes inalámbricas sin servidor dhcp.

Construido sobre libnet y libpcap, puede detectar hosts en línea de forma pasiva, o buscarlos, mediante el envío activo de solicitudes ARP.

sudo netdiscover -r 172.25.0.0/16 -f

01-Information Gathering

Spiderfoot

https://www.kali.org/tools/spiderfoot/

Se recomienda ejecutar en modo WEB con:

spiderfoot -l localhost:55000

Y entrar a http://localhost:55000 y en settings, poner los APIs que se puedan conseguir (excepto virustotal a menos de que sea comprado)

generic_send_tcp Spike es la herramienta de búsqueda de desbordamientos de búfer o debilidades similares para protocolos de red.

Usage: ./generic_send_tcp host port spike_script SKIPVAR SKIPSTR

generic_send_tcp 192.168.5.29 3306 /usr/share/spike/audits/MSSQL/mssql7.spk 0 0

nikto -h Nikto es un servidor web conectable y un escáner CGI escrito en Perl, que utiliza LibWhisker de rfp para realizar verificaciones rápidas de seguridad o información.

nikto -host www.up.edu.mx

02-Vulnerability Analysis

gvm

https://www.kali.org/tools/gvm/

La contraseña se cambia con:

sudo runuser -u _gvm -- gvmd --user=admin --new-password=

03-Web Application Analysis

cutycapt --help Herramienta para captura del render de una página WEB

cutycapt --url=http://www.up.edu.mx/ --out=www.png

wpscan --h Herramienta para analizar sitios de WordPress

wpscan --url upia.mx --api-token 5Pop2pznsylJ2taw0bdc88CPj5EVMBdAr7LflYRp7Ic

03-Web Application Analysis

ZAP

https://www.kali.org/tools/zaproxy/

Se recomienda actualizar todo y usar ataque automático.

04-Database Assessment

Sqlite browser

sqlmap

sqlmap --h Vulnerabilidades de inyección SQL en aplicaciones web.

sqlmap --wizard: https://educacioncontinua.up.edu.mx/programas-in-company/

05-Password Attacks

Medusa es una herramienta de fuerza bruta de inicio de sesión rápida, masivamente paralela y modular.

medusa -h 10.0.2.15 -u lalit -P /home/lalit/Desktop/Password_List.txt -M ssh -n 22

hashcat: Modos únicos de ataque para más de 300 algoritmos hash altamente optimizados, actualmente es compatible con CPU, GPU y otros aceleradores de hardware en Linux.

hashcat -m 1000 -a 3 hashesup

05-Password Attacks

John the Ripper es una herramienta diseñada para ayudar a los administradores de sistemas a encontrar contraseñas débiles (fáciles de adivinar o descifrar a través de la fuerza bruta)

john -h

a) Descomprimir wordlist (sudo, cd /usr/share/wordlists/, gzip -d rockyou.txt.gz)
b) Descargar Hashes
c) john --format=NT hashesup --wordlist=/usr/share/wordlists/rockyou.txt
d) john --format=NT hashesup --incremental --length=7
e) ó john --wordlist=/usr/share/wordlists/rockyou.txt --rules hashesup
f) john --format=Raw-md5 Lorenzo.txt --mask='?u[A-Z][a-z][a-z][a-z][0-9][0-9]'
g) john --format=Raw-md5 hash2 --incremental

05-Password Attacks

Hydra: una herramienta de fuerza bruta que se utiliza para descifrar contraseñas mediante el uso de un ataque de fuerza bruta.

Es un cracker de inicio de sesión paralelizado que admite numerosos protocolos para atacar. Es rápido y flexible.

hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh://192.168.1.123

hydra -L /home/lelguea/Desktop/ataque/usernames.txt -P /usr/share/wordlists/rockyou.txt -u 192.168.5.9 -s 8080 http-post-form -m '/Hydra/login:username=^USER^&password=^PASS^&Login=login:F=Usuario incorrecto'

hydra -l admin -P /usr/share/wordlists/rockyou.txt -u 192.168.5.9 -s 8080 http-post-form -m '/Hydra/login:username=^USER^&password=^PASS^&Login=login:F=Usuario incorrecto'

hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt -u 192.168.5.9 -s 8080 http-post-form -m '/Hydra/login:username=^USER^&password=^PASS^&Login=login:F=Usuario incorrecto'

06-Wireless Attacks

Aircrack-ng es un paquete de software de red que consta de un detector, un rastreador de paquetes, un cracker WEP y WPA/WPA2-PSK y una herramienta de análisis para LAN inalámbricas 802.11.

Pasos:

1. Detectar paquetes y recopilar vectores de inicialización débiles

2. Impulsar el tráfico a los vectores de inicialización débiles

3. Descifrar la clave WEP

https://techofide.com/blogs/how-to-use-aircrack-ng-aircrack-ng-tutorial-practical-demonstration/

https://www.aircrack-ng.org/doku.php?id=cracking_wpa

07-Reverse Engineering

NASAM: Ensamblador y desensamblador de archivos binarios de formato plano, a.out, archivos de objetos COFF y ELF Unix, y archivos de objetos Win32 y DOS de 16 bits de Microsoft. También se incluye NDISASM, un prototipo de desensamblador de archivos binarios x86 que utiliza la misma tabla de instrucciones que NASM.

Radare2: Cadena de herramientas completa, portátil, de múltiples arquitecturas y similar a Unix para la ingeniería inversa.

https://youtu.be/C06r6DfCxpA?si=cEp2gcDzbacCvrsI

08-Exploitation Tools

Metasploid Framework (/usr/share/metasploit-framework/modules y https://www.infosecmatter.com/metasploit-module-library/)

1. use auxiliary/scanner/portscan/tcp
2. info
3. set rhosts 192.168.5.29 ó set rhosts 192.168.5.0/24
4. set threads 4
5. set ports 2-600
6. run
7. hosts
8. use scanner/discovery/udp_probe
9. info
10. set rhosts 192.168.5.0/24
11. set threads 4
12. hosts
13. services

08-Exploitation Tools

Metasploid Framework

1. use auxiliary/scanner/discovery/ipv6_neighbor
2. info
3. set rhosts 192.168.5.1
4. set threads 4
5. set timeout 60
6. set interface eth0
7. run

mitmproxy: Proxy intermediario interactivo para HTTP y HTTPS. Proporciona una interfaz de consola que permite inspeccionar y editar los flujos de tráfico sobre la marcha.

wireshark: Herramienta para disección de paquetes de red y análisis de protocolos.

Es útil combinar varias herramientas, por ejemplo Wireshark y nmap:

nmap -sU -p 161 --script=snmp-info 172.25.232.0/2

Adicionales:

10-Post Exploitation

11- Forensics

12-Reporting Tools

13-Social Engineering Tools

Adicionales:

DVWA:

https://github.com/digininja/DVWA/blob/master/README.es.md

a) Crear Usuarios
b) Crear Contraseñas
c) Instalar DVWA
    i) git clone https://github.com/digininja/DVWA.git
    ii) sudo vm DVWA /var/www/html/
    iii) sudo service apache2 start
    iv) cp config.inc.php.dist config.inc.php
    v) http://localhost/DVWA/setup.php