Guía de Comandos en Kali Linux

1. Iniciar sesión

Usuario y contraseña predeterminados:

- Usuario: `kali`

- Contraseña: `kali`

2. Actualizar Repositorios de Kali Linux

Es importante mantener el sistema actualizado para obtener las últimas mejoras y parches de seguridad.

┌──(kali㉿kali)-[~]

└─$ sudo apt update && sudo apt upgrade -y

3. Recomendación: Ser Usuario Root

Para tener privilegios administrativos, es recomendable cambiar al usuario root.

┌──(kali㉿kali)-[~]

└─$ sudo su

- Contraseña: `kali`

Aquí ya seriamos usuarios root.

┌──(root㉿kali)-[/home/kali]

└─#

Aquí nos encontramos en la carpeta raiz

┌──(kali㉿kali)-[~]

└─$

Para navegar entre carpetas utilizamos

Para ubicarnos en el escritorio.

┌──(kali㉿kali)-[~]

└─$ cd Desktop

Aquí ya estamos ubicados en el escritorio

──(kali㉿kali)-[~/Desktop]

└─$

Ahora para regresar.

──(kali㉿kali)-[~/Desktop]

└─$ cd ..

4. Limpiar Consola

Para limpiar la consola y tener una vista despejada:

┌──(kali㉿kali)-[~]

└─$ clear

5. Instalación de Paquetes

Para instalar un paquete, utiliza el siguiente comando:

┌──(root㉿kali)-[/home/kali]

└─# sudo apt install <nombre\_paquete>

Ejemplo para instalar `neofetch`, un paquete que muestra las especificaciones del equipo:

┌──(root㉿kali)-[/home/kali]

└─# sudo apt install neofetch

6. Ejecutar `neofetch`

Después de instalar `neofetch`, se puede ejecutar con:

┌──(root㉿kali)-[/home/kali]

└─# neofetch

7. Desinstalación de Paquetes

Para desinstalar un paquete, usa:

┌──(root㉿kali)-[/home/kali]

└─# sudo apt remove <nombre\_paquete>

Ejemplo para desinstalar `neofetch`:

┌──(root㉿kali)-[/home/kali]

└─# sudo apt remove neofetch

8. Remover Dependencias Residuales

Para eliminar todas las dependencias que ya no se necesitan:

┌──(root㉿kali)-[/home/kali]

└─# sudo apt autoremove

9. Comandos Básicos de Navegación y Gestión de Archivos

- Listar elementos de un directorio:\*\*

┌──(root㉿kali)-[/home/kali]

└─# ls

- Mostrar la ruta actual:

┌──(root㉿kali)-[/home/kali]

└─# pwd

- Volver al directorio anterior:

┌──(root㉿kali)-[/home/kali]

└─# cd ..

- Eliminar un archivo:

┌──(root㉿kali)-[/home/kali]

└─# rm <nombre\_archivo>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# rm prueba.txt

- Crear un archivo:

┌──(root㉿kali)-[/home/kali]

└─# touch <nombre\_archivo>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# touch prueba.txt

- Modificar un archivo:

┌──(root㉿kali)-[/home/kali]

└─# nano <nombre\_archivo>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# nano prueba.txt

- Mostrar el contenido de un archivo:

┌──(root㉿kali)-[/home/kali]

└─# cat <nombre\_archivo>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# cat prueba.txt

- Guardar texto en un archivo directamente:

┌──(root㉿kali)-[/home/kali]

└─# echo 'texto' > <nombre\_archivo>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# echo 'esto es una prueba' > prueba.txt

- Crear una carpeta:

┌──(root㉿kali)-[/home/kali]

└─# mkdir <nombre\_carpeta>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# mkdir nueva\_carpeta

- Borrar un directorio o carpeta

┌──(root㉿kali)-[/home/kali]

└─# rm -r <nombre\_carpeta>

Ejemplo:

┌──(root㉿kali)-[/home/kali]

└─# rm -r experimento

-Borrar un archivo

┌──(root㉿kali)-[/home/kali]

└─# rm <nombre\_archivo>

10. Obtener la Dirección IP

Para conocer la dirección IP del equipo:

┌──(root㉿kali)-[/home/kali]

└─# ip a

┌──(root㉿kali)-[/home/kali]

└─# ifconfig

Nota: En algunos sistemas `ipconfig` puede no estar disponible o no mostrar la información esperada. En su lugar, usa `ip a`.

Esta guía proporciona una lista de comandos esenciales y buenas prácticas para manejar Kali Linux de manera efectiva.

nmap: Es el comando para ejecutar Nmap, una herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red informática.

-O: Habilita la detección de sistema operativo (OS detection). Nmap intenta determinar el sistema operativo de cada host en la red objetivo, utilizando una serie de técnicas de huella digital para identificar la pila TCP/IP del sistema.

192.168.1.0/24: Especifica el rango de direcciones IP que se deben escanear. En este caso, 192.168.1.0/24 abarca todas las direcciones IP desde 192.168.1.0 hasta 192.168.1.255, lo que incluye todos los hosts en la subred 192.168.1.x.

En resumen:

El comando completo nmap -O 192.168.1.0/24 realiza las siguientes acciones:

┌──(root㉿kali)-[/home/kali]

└─# nmap -O 192.168.1.0/24

Escanea la subred: 192.168.1.0/24, que incluye todas las direcciones IP desde 192.168.1.0 hasta 192.168.1.255.

Detecta el sistema operativo: Intenta identificar el sistema operativo de cada host activo en esa subred utilizando técnicas de huella digital de la pila TCP/IP.

Uso práctico:

Este tipo de escaneo es útil para:

Auditorías de seguridad: Ayuda a identificar sistemas operativos en la red, lo que es crucial para la gestión de vulnerabilidades.

Inventario de red: Facilita la creación de un inventario de los dispositivos y sus sistemas operativos en una red.

Reconocimiento: En pruebas de penetración, permite conocer más detalles sobre los sistemas de la red objetivo.

Consideraciones:

Permisos: Realizar escaneos de red sin autorización puede ser ilegal y está prohibido por políticas de uso aceptable de muchas redes.

Impacto: Un escaneo detallado como este puede generar tráfico adicional en la red y potencialmente afectar el rendimiento de la misma.

-cuando ya tenemos una ip definida necesitamos conocer mas informacion de la maquina victima

┌──(root㉿kali)-[/home/kali]

└─# nmap -p- -sVC -sC --open -sS -vvv -n -Pn 192.168.1.10 -oN escaneo

nmap: Es el comando para ejecutar Nmap, una herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red informática.

-p-: Indica que se deben escanear todos los puertos (0-65535) en el host objetivo.

-sV: Realiza detección de versiones. Trata de determinar el software y la versión de los servicios que se están ejecutando en los puertos abiertos.

-sC: Utiliza scripts de Nmap Scripting Engine (NSE) con el conjunto de scripts predeterminados. Estos scripts realizan diversas tareas adicionales, como la detección de vulnerabilidades y la obtención de información adicional.

--open: Muestra solo los puertos que están abiertos. No se mostrarán los puertos cerrados o filtrados.

-sS: Realiza un escaneo SYN (o escaneo semiabierto). Este tipo de escaneo es más sigiloso y rápido porque no establece una conexión completa con el host objetivo.

-vvv: Aumenta la verbosidad. Proporciona mucha más información sobre el progreso del escaneo y los resultados intermedios.

-n: No resuelve nombres de host. Solo usa direcciones IP en los resultados, lo que puede acelerar el escaneo.

-Pn: Desactiva la detección de host. Supone que el host está activo, evitando la fase de ping.

10.0.2.2: Es la dirección IP del objetivo a escanear.

-oN escaneo: Guarda los resultados del escaneo en un archivo llamado escaneo en formato de salida normal de Nmap.

En resumen:

Este comando de Nmap realiza un escaneo muy detallado de todos los puertos (0-65535) en el host 10.0.2.2. Utiliza un escaneo SYN para detectar servicios y versiones de software en esos puertos abiertos. Además, ejecuta scripts NSE predeterminados para recopilar información adicional y vulnerabilidades potenciales. El escaneo es muy verboso (-vvv) y los resultados se guardan en un archivo llamado escaneo.

Instalar Entorno Vulnerable METASPLOITABLE en Virtualbox y VMware

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Metasploitable es una máquina virtual intencionalmente vulnerable diseñada para ayudar a los profesionales de seguridad a aprender y practicar habilidades de explotación y penetración. Desarrollada por Rapid7, la misma compañía que mantiene Metasploit Framework, Metasploitable se usa comúnmente en entornos de laboratorio para realizar pruebas de seguridad y aprender sobre vulnerabilidades comunes.

Características y Propósitos de Metasploitable:

1. Entorno de Práctica:

- Proporciona un entorno seguro para que los profesionales y estudiantes de seguridad practiquen y desarrollen habilidades de hacking ético.

2. Vulnerabilidades Intencionales:

- Contiene múltiples vulnerabilidades intencionales que se encuentran en software y servicios populares, ofreciendo una variedad de desafíos.

3. Aprendizaje de Herramientas de Explotación:

- Permite a los usuarios practicar con herramientas como Metasploit Framework, Nmap, y otras herramientas de seguridad.

4. Diversidad de Explotaciones:

- Las vulnerabilidades cubren un amplio espectro, incluyendo SQL Injection, vulnerabilidades en servidores web, servicios inseguros, y más.

Uso de Metasploitable:

Para usar Metasploitable, generalmente se sigue el siguiente proceso:

1. Descargar y Configurar la Máquina Virtual:

- Metasploitable se puede descargar como una imagen de máquina virtual (VM) y se puede ejecutar en software de virtualización como VirtualBox o VMware.

2. Exploración de la Red:

- Usar herramientas como Nmap para escanear y mapear los puertos abiertos y servicios en la máquina Metasploitable.

3. Identificación de Vulnerabilidades:

- Utilizar escáneres de vulnerabilidades para identificar puntos débiles en la seguridad del sistema.

4. Explotación de Vulnerabilidades:

- Emplear Metasploit Framework y otras herramientas para explotar las vulnerabilidades identificadas, aprender a usar diferentes exploits y payloads.

Ejemplo de Escenario de Uso:

1. Configuración Inicial:

- Descarga Metasploitable desde el sitio oficial o una fuente confiable.

- Importa la máquina virtual en tu software de virtualización (por ejemplo, VirtualBox).

2. Exploración con Nmap:

- Abre una terminal en tu máquina host y ejecuta un escaneo de puertos contra Metasploitable:

```bash

nmap -A 192.168.x.x

```

- Esto proporcionará información sobre los puertos abiertos y los servicios que se ejecutan en esos puertos.

3. Identificación de Vulnerabilidades:

- Usa una herramienta como Nessus o OpenVAS para realizar un escaneo de vulnerabilidades y generar un reporte.

4. Explotación con Metasploit:

- Inicia Metasploit Framework en tu terminal:

```bash

msfconsole

```

- Busca y selecciona un exploit:

```bash

use exploit/unix/ftp/vsftpd\_234\_backdoor

```

- Configura las opciones necesarias, como la dirección IP de la máquina Metasploitable:

```bash

set RHOST 192.168.x.x

```

- Ejecuta el exploit:

```bash

run

```

Advertencia:

Es importante usar Metasploitable en un entorno controlado y con fines educativos. Nunca debe ser usado en redes o sistemas no autorizados, ya que esto sería ilegal y poco ético.

Recursos Adicionales:

- Metasploit Unleashed: Un curso gratuito ofrecido por Offensive Security que cubre el uso de Metasploit.

- OWASP (Open Web Application Security Project): Ofrece recursos y herramientas para aprender sobre seguridad web.

- Hack The Box: Una plataforma en línea que ofrece máquinas vulnerables para practicar hacking ético en un entorno seguro.

**Cómo Explotar Vulnerabilidades de Forma Manual**