🧠 Lame - Hack The Box (HTB)

Análisis técnico, didáctico y documentado por **r4ms4nt**.

Primera máquina publicada en Hack The Box. Diseñada como puerta de entrada para nuevos usuarios. Ideal para aprender enumeración, detección de vulnerabilidades clásicas y explotación básica con Metasploit.

🗓️ **Fecha:** Mayo 2025

🎯 **Objetivo:** Reproducir y documentar la resolución de la máquina *Lame*, la primera máquina publicada por Hack The Box.

🎯 Objetivos del proyecto

- Desarrollar una metodología práctica de hacking ético.
- Aplicar técnicas reales de reconocimiento, enumeración y explotación.
- Practicar documentación profesional para entornos de certificación (OSCP, eJPT...).

🔍 Task 1: How many of the nmap top 1000 TCP ports are open?

🎯 **Objetivo:** Identificar puertos TCP abiertos más comunes.

✅ **Comandos ejecutados:**

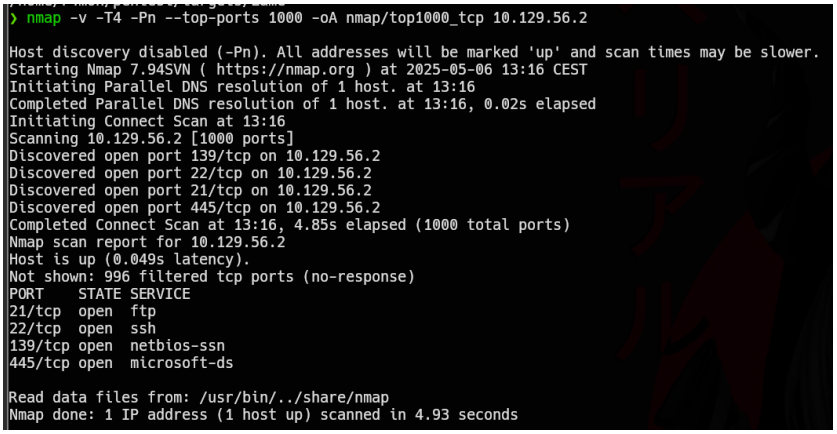
```
nmap -v -T4 -Pn --top-ports 1000 -oA nmap/top1000_tcp 10.129.56.2
grep open nmap/top1000_tcp.nmap
```

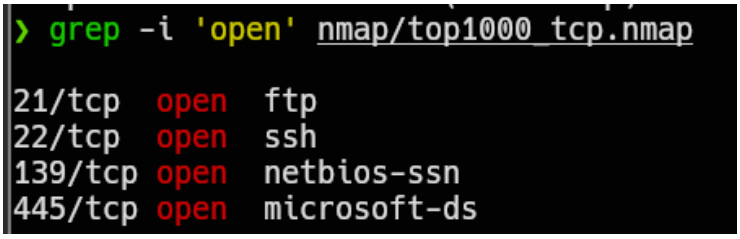
Explicación:

-v: modo verbose.
-T4: velocidad razonablemente rápida.
-Pn: omite el ping inicial, asume que el host está activo.
--top-ports 1000: escanea los 1000 puertos TCP más comunes.
-oA nmap/top1000_tcp: guarda la salida en 3 formatos (normal, grepeable y XML) en el subdirectorio nmap/.
grep open: filtra la salida para mostrar solo los puertos abiertos.

🔎 **Resultado:**

- Puertos abiertos: 21, 22, 139, 445
- Total: **4**





🔍 Task 2: What version of VSFTPd is running on Lame?

🎯 **Objetivo:** Determinar la versión del servicio FTP en el puerto 21.

✅ **Comandos ejecutados:**

```
nmap -sV -p21 -oA nmap/ftp_version 10.129.56.2
```

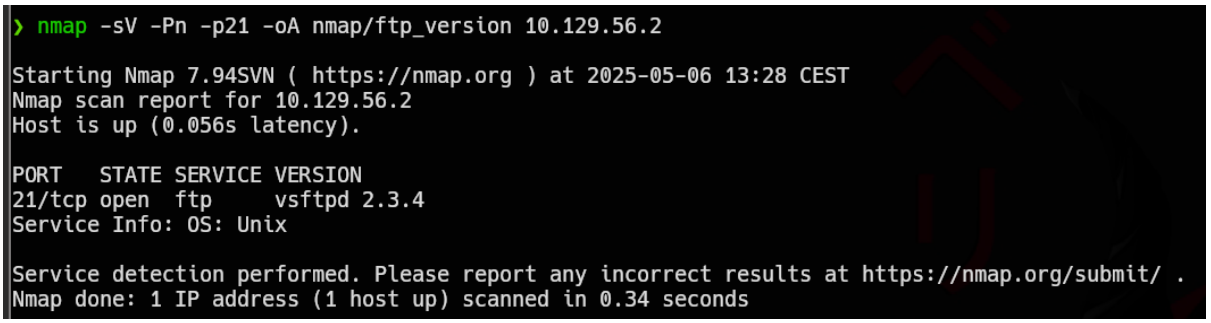
Explicación:

-sV: Detecta versiones de servicios.
-p21: Solo el puerto FTP.
-oA nmap/ftp_version: Guarda en el subdirectorio nmap/.

🔎 **Resultado:**

- Servicio: **vsFTPd 2.3.4**

📸



🔍 Task 3: ¿Funciona el famoso exploit de VSFTPd 2.3.4?

🎯 **Objetivo:** Verificar si la vulnerabilidad conocida de backdoor está activa.

✅ **Comandos ejecutados (en Metasploit):**

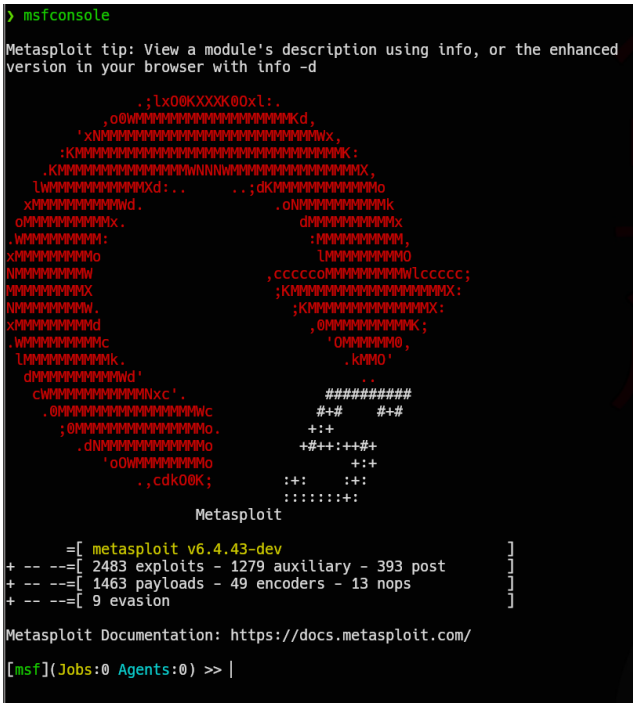
```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 10.129.56.2
run
```

Explicación:
use: carga el módulo de exploit.
set RHOSTS: establece la dirección IP del objetivo.
run: ejecuta el exploit.

🔎 **Resultado:**

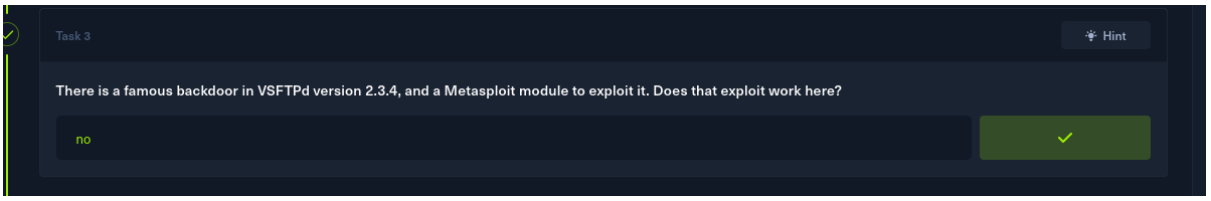
- El exploit se ejecuta pero **no devuelve sesión**.

📸



```
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 10.129.56.2
RHOSTS => 10.129.56.2
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> run
[*] 10.129.56.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.129.56.2:21 - USER: 331 Please specify the password.
```



🔍 Task 4: ¿Qué versión de Samba corre en Lame?

🎯 **Objetivo:** Enumerar la versión del servicio Samba en los puertos 139 y 445.

✅ **Comandos ejecutados:**

```
nmap -sV -Pn -p139,445 --script=smb-protocols,smb-os-discovery,smb2-security-mode,smb2-time -oA nmap/smb_version 10.129.56.2
```

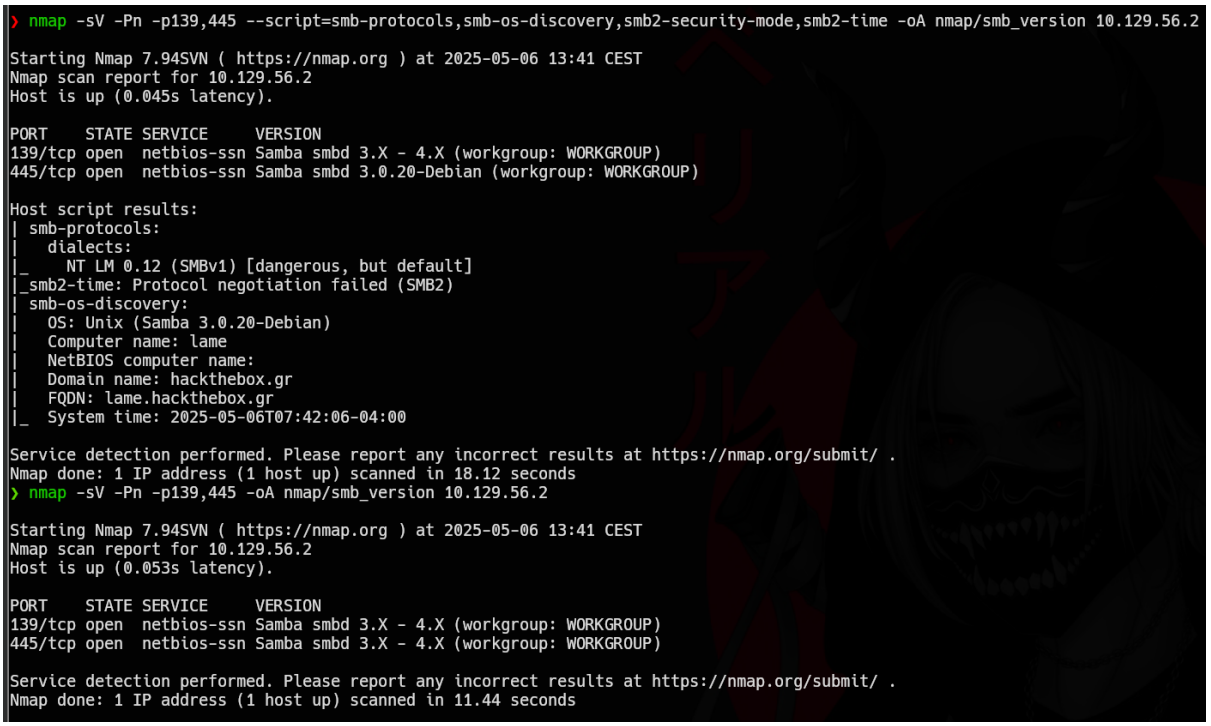
Explicación:

-sV: Detecta versiones de servicios.
-Pn: Omite el ping inicial.
-p139,445: Escanea los puertos 139 y 445.
--script: ejecuta scripts de Nmap para obtener información adicional sobre Samba.
-oA nmap/smb_version: guarda la salida en el subdirectorio nmap/.

Resultado:

- Versión detectada: **Samba 3.0.20**

📸



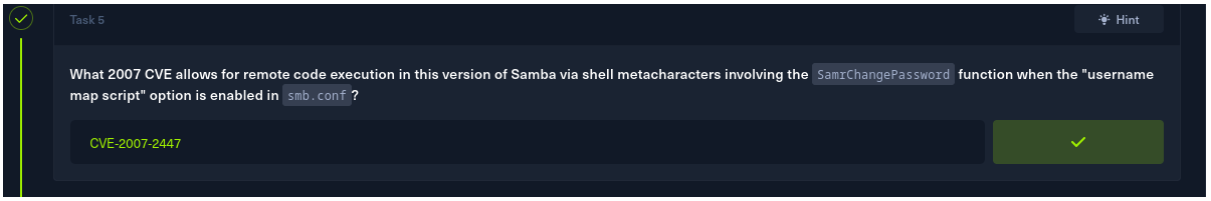
🔍 Task 5: ¿Qué CVE del 2007 permite RCE en esta versión de Samba?

🎯 **Objetivo:** Identificar una vulnerabilidad histórica en la versión de Samba.

✅ **Referencia:**

- CVE-2007-2447
- Condición: uso de username map script en smb.conf

📸



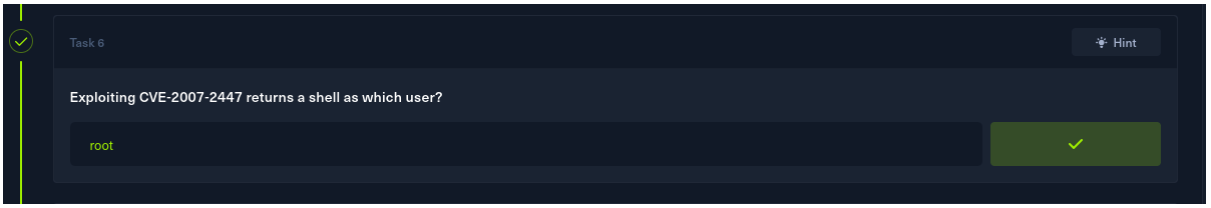
🔍 Task 6: ¿Qué usuario obtiene shell al explotar CVE-2007-2447?

🎯 **Objetivo:** Determinar el contexto del shell recibido tras la explotación.

✅ **Resultado:**

- Usuario: **root**

📸



🔍 Task 7: Obtener la flag del usuario makis

🎯 **Objetivo:** Localizar y leer el archivo user.txt.

✅ **Comandos ejecutados:**

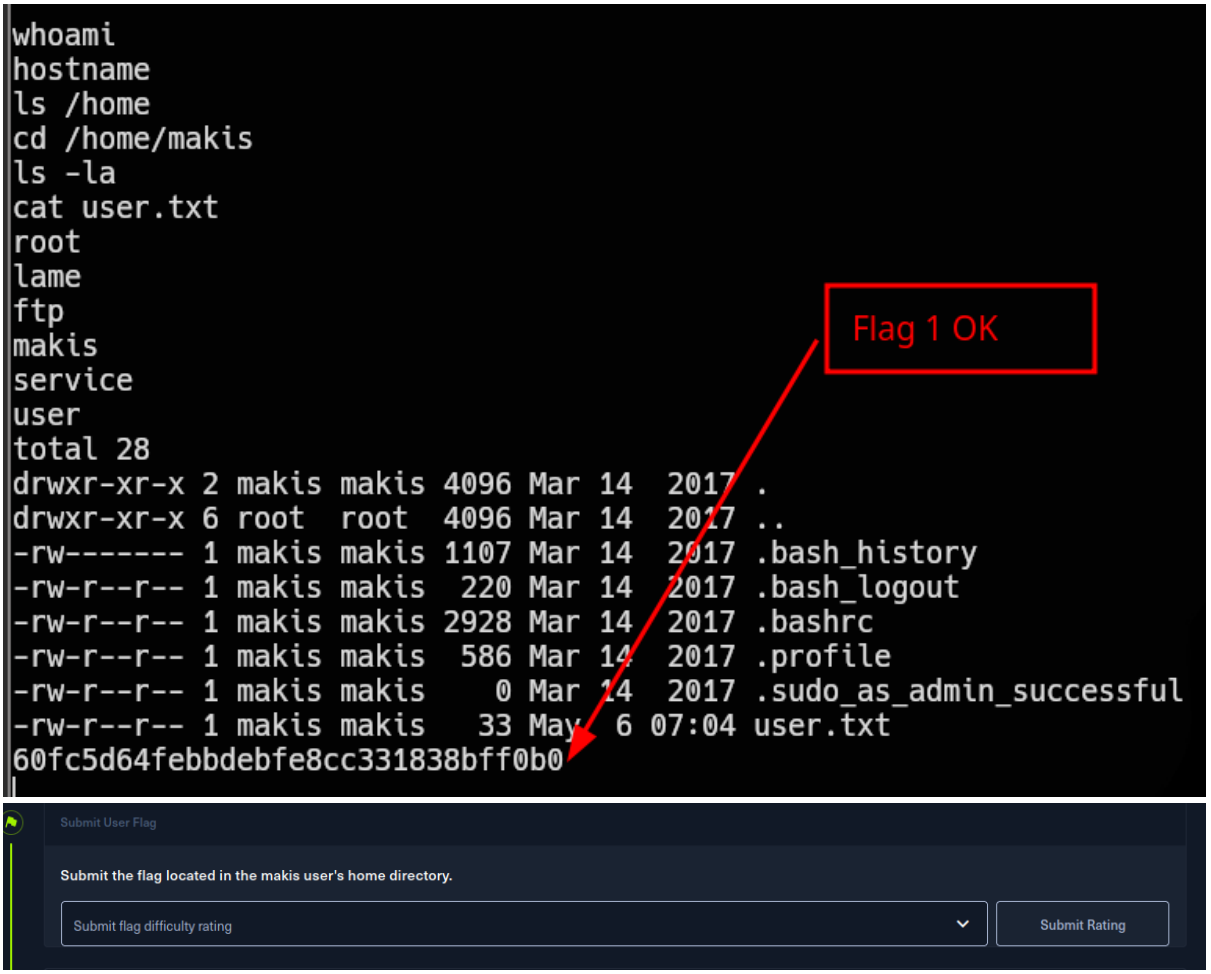
```
cd /home/makis
ls -la
cat user.txt
```

Explicación:

cd: cambia al directorio del usuario.
ls -la: lista archivos y permisos.
cat user.txt: muestra el contenido del archivo.

🔎 **Resultado:**

📸



🔍 Task 8: Obtener la flag del usuario root

🎯 **Objetivo:** Escalar privilegios y leer /root/root.txt

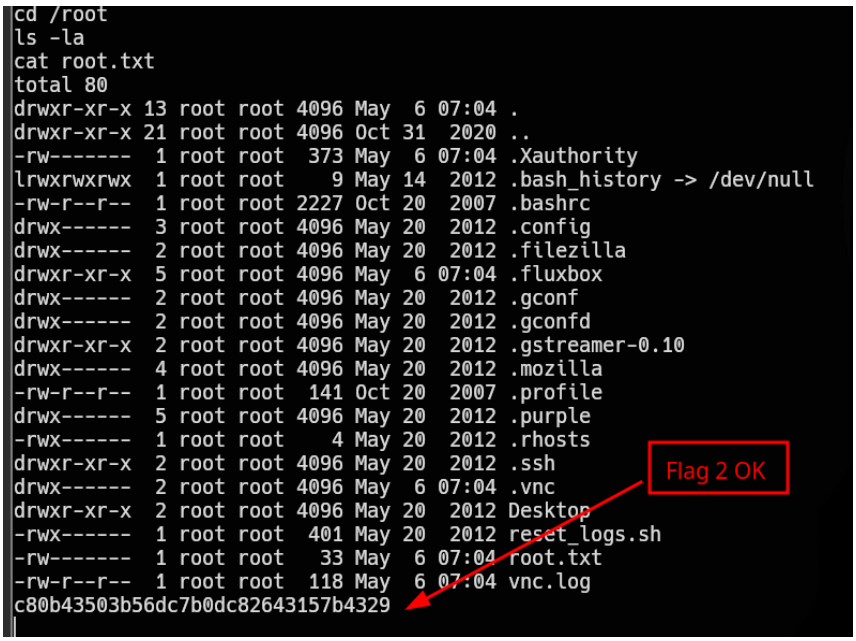
✅ **Comandos ejecutados**

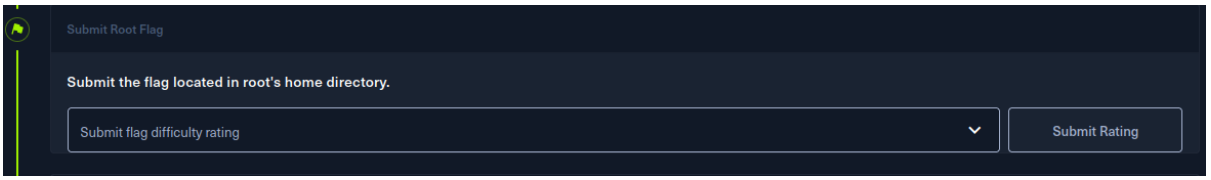
```
cd /root
ls -la
cat root.txt
```

Explicación:

cd: cambia al directorio root.
ls -la: lista archivos y permisos.
cat root.txt: muestra el contenido del archivo.

🔎 **Resultado:** 📸





🔍 Task 9: ¿Qué impide la conexión a ciertos puertos visibles con netstat?

🎯 **Objetivo:** Explicar por qué no todos los puertos escuchando son accesibles desde fuera.

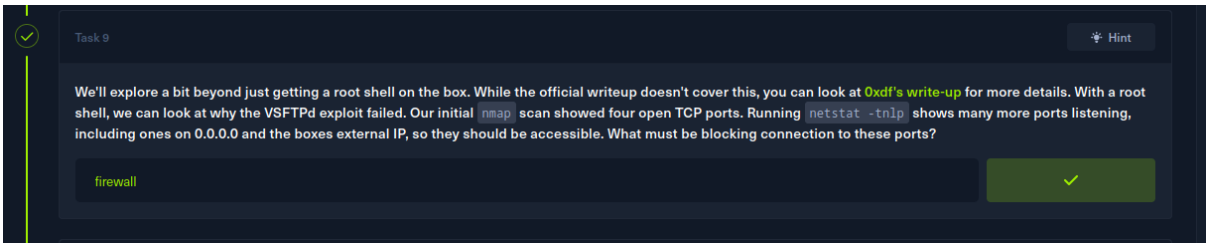
✅ **Comandos ejecutados:**

```
netstat -tnlp
```

Explicación:
netstat -tnlp: muestra conexiones TCP activas y puertos escuchando.
-t: TCP
-n: muestra direcciones y puertos en formato numérico.
-l: muestra solo puertos escuchando.
-p: muestra el PID y nombre del programa.

🔎 **Resultado:**

- Causa: **firewall**



🔍 Task 10: ¿Qué puerto escucha cuando se activa el backdoor de VSFTPd?

🎯 **Objetivo:** Confirmar el comportamiento del backdoor.

✅ **Resultado:**

- Puerto: **6200**

🔍 Task 11: ¿El puerto 6200 escucha realmente en Lame?

🎯 **Objetivo:** Verificar con netstat si efectivamente se activa el puerto.

✅ **Comandos ejecutados:**

```
ss -tnlp | grep 6200
```

Explicación:
ss: herramienta para investigar sockets.
-t: muestra conexiones TCP.
-n: muestra direcciones y puertos en formato numérico.
-l: muestra solo puertos escuchando.
-p: muestra el PID y nombre del programa.
grep 6200: filtra la salida para mostrar solo el puerto 6200.

🎾 **Resultado:**

- Sí, escucha.