Lame

22nd July 2024 / Document No D24.100.293

Prepared By: Arrexel & C4rm3l0

Machine Author: ch4p

Difficulty: Easy

Classification: Official

Maquina: LAME, SO: Linux

IP: 10.10.10.3

Lame es una maquina Linux publicada en Hack The Box, solía ser la primera maquina para los nuevos usuarios, solo requiere un exploit para obtener acceso como root.

Lo que veremos será una guía de paso a paso la solución para acceder como root y capturar las flags de la máquina, detallaremos algunos parámetros para explicarlos y que me ayudo a entender.

Habilidades Requeridas

- Conocimientos básicos de Linux
- Enumeración de puertos y servicios

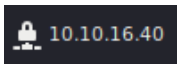
Habilidades Adquiridas

- Identificación de servicios vulnerables
- Explotación de **Samba**

El primer paso que haremos será conectarnos a una VPN de HackTheBox, podremos descargar el archivo desde la propia plataforma, nos descargará un archivo. ovpn que tendremos que ejecutar utilizando Openvpn que se usa para iniciar y gestionar conexiones VPN, nos permite conectarnos de forma segura a una red privada a través de internet.

para poder conectarnos lo que haremos será escribir el siguiente comando.

```
┌──(caan31㉿vbox)-[/media/sf_vm]
└─$ sudo openvpn lab_Aragon3105.ovpn
```



Una vez ejecutado el comando, podremos ver que nuestra ip ha cambiado, si no estas seguro puedes ejecutar el comando ifconfig y veras como aparece una nueva interfaz de red:

tun0 → si es una conexión TUN (más común)

tap0 → si es una conexión TAP (menos común, capa 2)

Vamos a comprobar que tenemos conectividad entre nuestro equipo y la maquina atacada.

El parámetro -c 1 le dice a ping que solo envié 1 paquete ya que por defecto manda infinitos hasta cancelarlo.

```
┌──(caan31㉿vbox)-[~]
└─$ 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=33.6 ms

── 10.10.10.3 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 33.564/33.564/33.564/0.000 ms
```

Una cosa que podemos fijarnos si en algún caso no sabemos con que maquina nos encontramos es en el parámetro **TTL**

Sistema operativo	TTL inicial común
Windows	128
Linux/Unix/macOS	64
Routers/Cisco	255

Así que, si ves un TTL de 64, 128 o 255 en la respuesta, puedes adivinar desde qué sistema te están respondiendo

El primer paso que haremos es escanear los puertos que tenga abierta la maquina con el comando **nmap**, el apartado que utilizamos **-Pn** sirve para desactivar la detección de host, es decir **nmap** no envia paquetes ICMP (ping), asume que el host esta activo y procede directamente al escaneo de puertos.

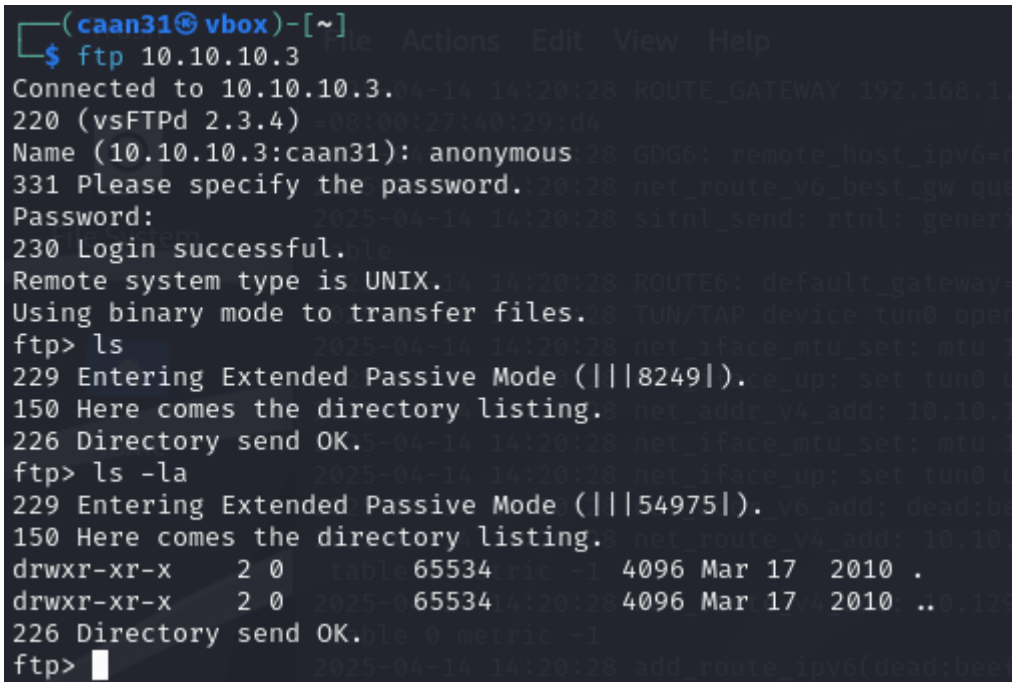
```
┌──(caan31㉿vbox)-[~]
└─$ nmap -Pn 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 14:22 CEST
Nmap scan report for 10.10.10.3
Host is up (0.056s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds
```

Podemos comprobar que tenemos varios puertos abiertos, ahora ejecutaremos **nmap** especificando cada puerto que hemos encontrado con el apartado **-p**, con el apartado **-sCV** combina dos herramientas, para obtener más información del servicio como versiones, usuarios anónimos en FTP, vulnerabilidades básicas, intentar identificar la versión exacta

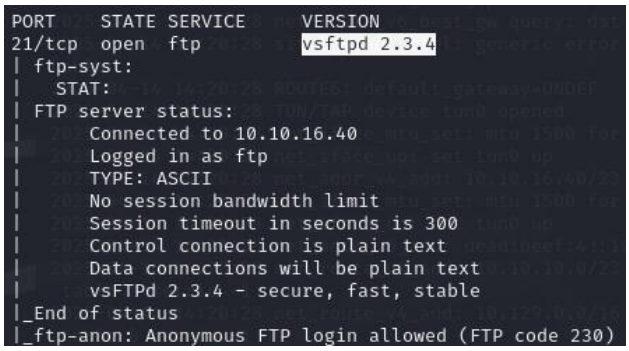
```
┌──(caan31㉿vbox)-[~]
└─$ nmap -p21,22,139,445 -sCV -Pn 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 14:23 CEST
Nmap scan report for 10.10.10.3
Host is up (0.075s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.40
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| 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: 2025-04-14T08:25:13-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h01m39s, deviation: 2h49m45s, median: 1m36s

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.75 seconds
```

Como vimos al ejecutar podemos intentar ingresar al servicio FTP con el usuario Anonymous que por defecto no se necesita ninguna contraseña.

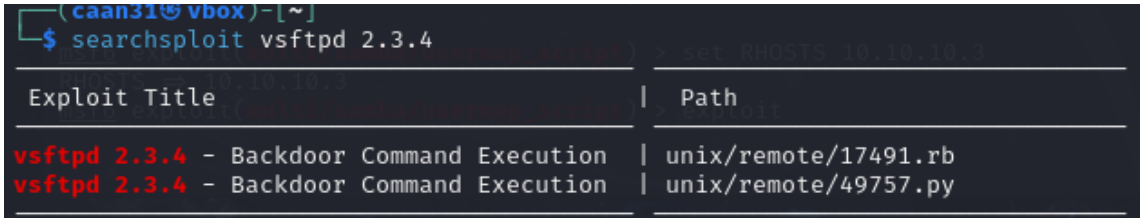
Ejecutamos el comando **ls** para listar los contenidos y **ls -la** para los contenidos incluidos los ocultos, al ver que no tenemos nada que nos pueda ayudar a acceder a la flag vamos a intentarlo con otro método.



Vamos a intentar buscar un exploit con searchploit que forma parte de una base de datos que permite buscar exploits conocidos. Al escanear los puertos abiertos podemos ver la versión que nos encontramos de ftp.



Aquí podemos ver que cuenta con una vulnerabilidad de puerta trasera.



Para poder explotar la vulnerabilidad, utilizaremos la herramienta de metasploit, para ejecutar deberemos ejecutar el siguiente comando.

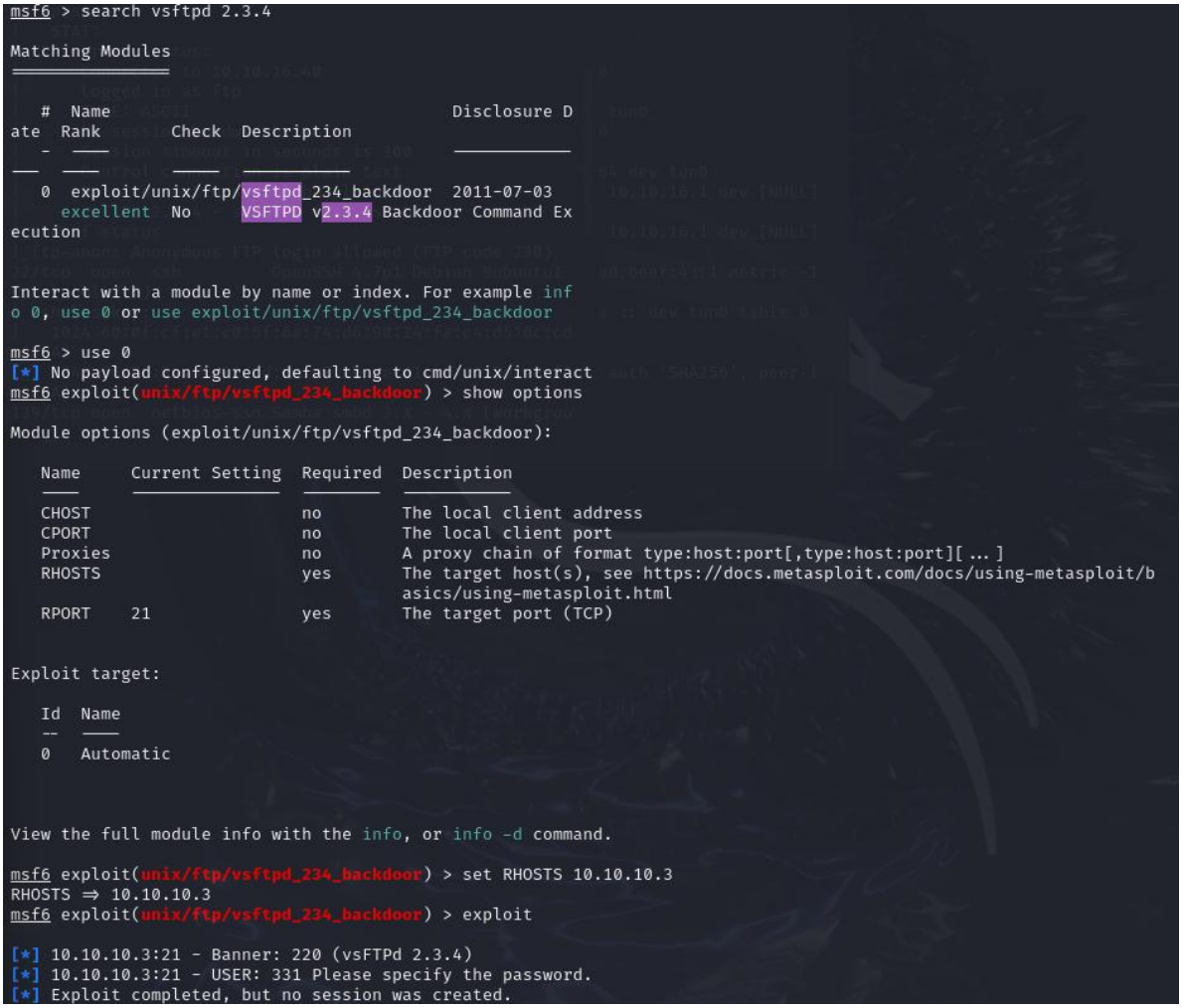
```
┌──(caan31㉿vbox)-[~]
└─$ msfconsole
```

Una vez ejecutado podemos buscar el exploit que necesitemos con lo que encontramos anteriormente.

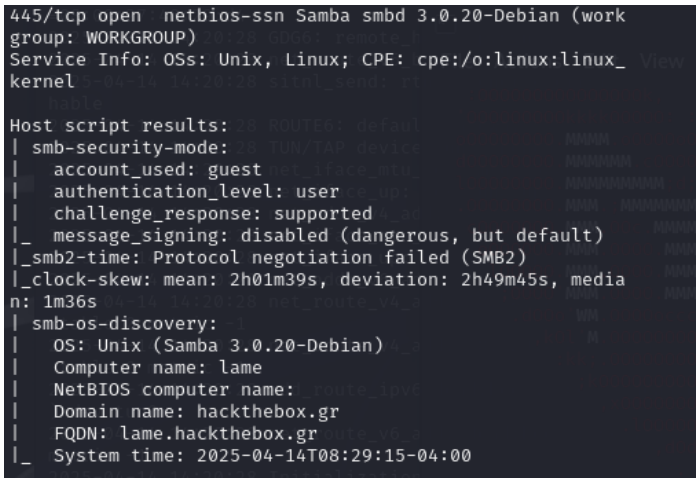
Con el comando **use** podremos abrir el panel para ejecutar el exploit, para poder ver lo que nos pide para poder realizar el exploit utilizaremos el comando **show options**, la mayoría de las veces nos pedirá el **RHOSTS** que es la **IP** de la maquina atacada.

Con el comando **set RHOSTS "IP"** le daremos valor de la ip para poder ejecutar el exploit.

Al ver que no nos permite acceder podemos llegar a la conclusión que esta versión no nos permite ejecutar el **exploit** de la puerta trasera.

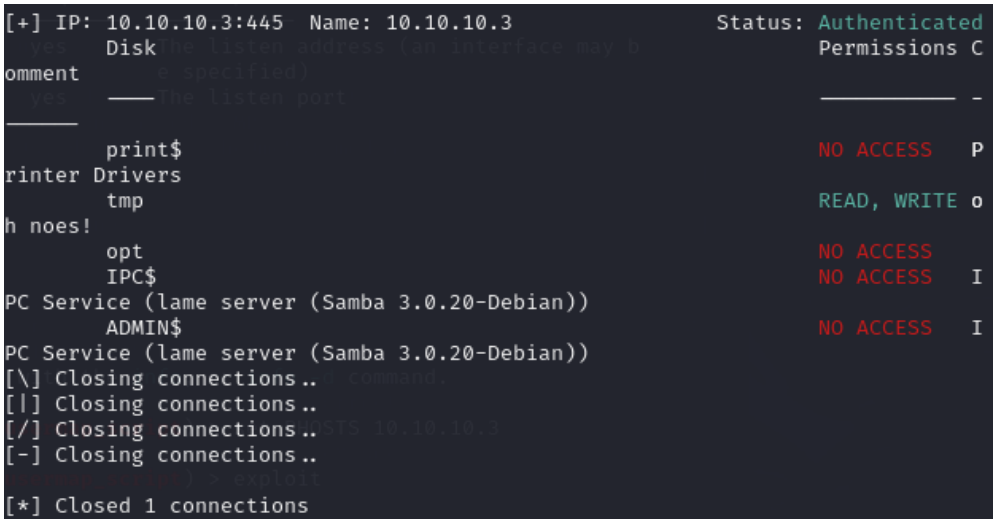


La siguiente opción que tenemos es con otro puerto que este abierto que es el servicio de SAMBA, podremos ver la versión con la que nos encontramos en el escaneo de puertos que ejecutamos anteriormente.

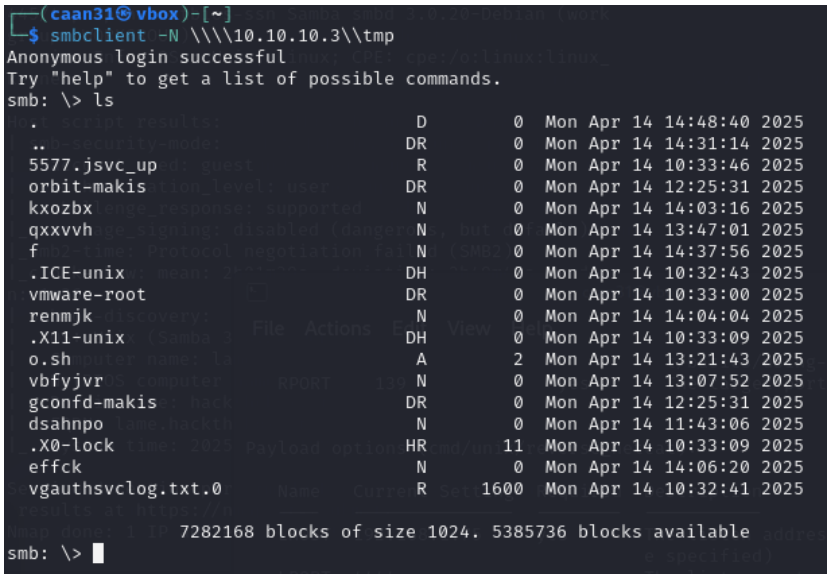


Con el comando smbmap nos permitirá enumerar recursos compartidos y ver que permisos tiene el usuario sobre esos recueros, con el parámetro -H nos permitirá mostrar la ayuda de la herramienta

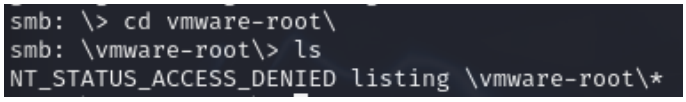
Podemos ver que tmp tiene permisos de lectura y escritura, así que intentaremos conectarnos directamente



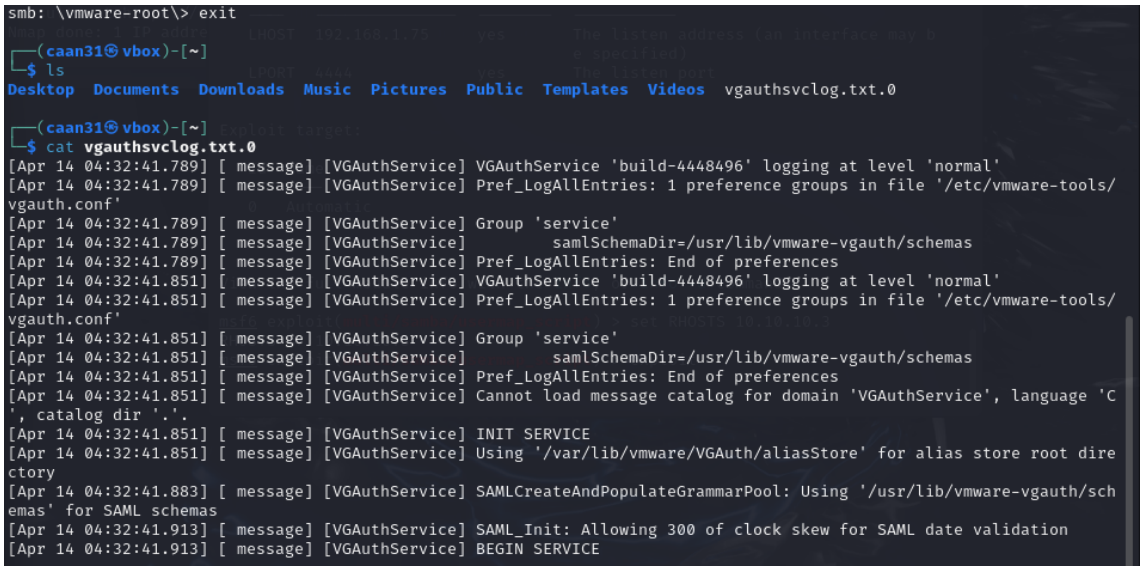
Con el comando smbclient es como usar FTP pero para SMB, que nos permite conectarnos manualmente a recursos compartidos, con el parámetro -N nos dice que a smbclient que no use credenciales, de igual manera que ftp que entre con el usuario Anonymous



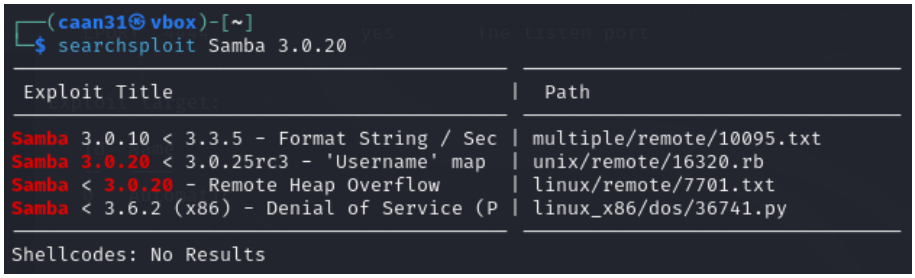
Podemos ver que podemos ingresar al servicio smb, ejecutamos un listado de los contenidos, vemos dos cosas que nos pueden interesar, una carpeta con el nombre root y un archivo txt, intentamos ingresar primero a la carpeta y podemos ver que no contamos con permisos.



Vamos a leer el archivo txt, lo vamos a llevar a nuestra maquina con el comando get y luego lo leeremos a ver si encontramos algo que nos sirva.

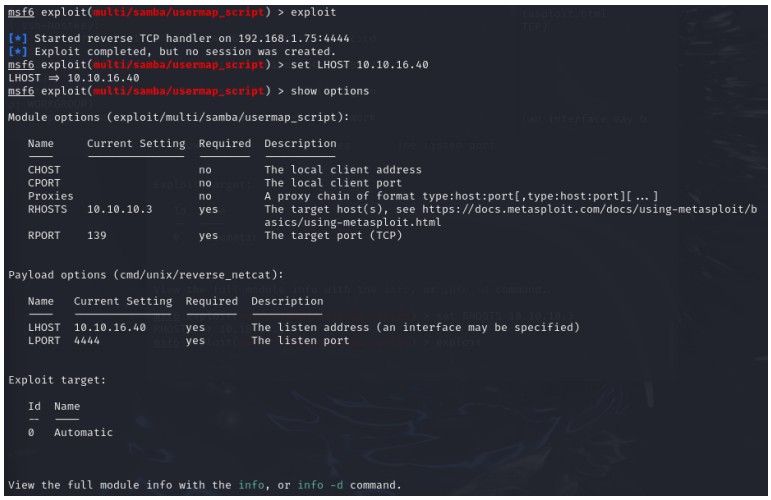


Como podemos ver, no contiene nada interesante, así que pasaremos al paso de antes, buscar un exploit de la versión de SAMBA.



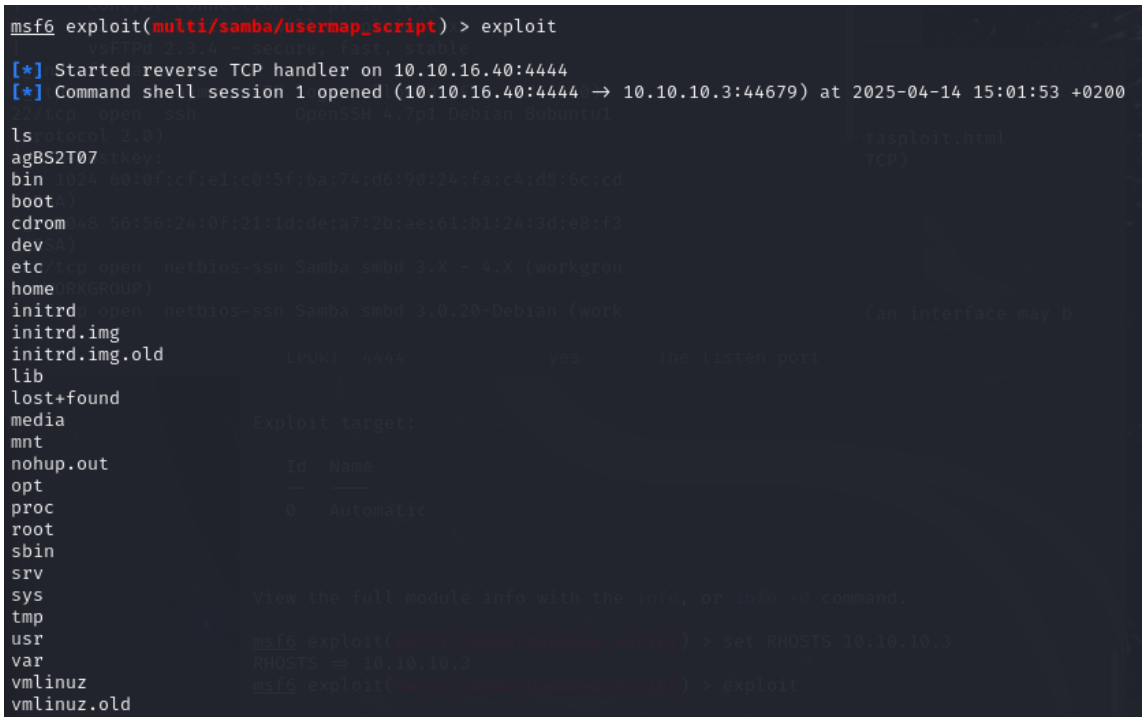
De igual manera lo ejecutaremos y vemos que nos pide la ip de la maquina atacante, repetimos los pasos que hicimos anteriormente.

Al ejecutarlo me di cuenta de LHOST tenia otra IP que no era la mía, así que hay que revisar bien que todos los parámetros que nos pide requeridos son correctos, se soluciona simplemente colocando con set LHOST “IP”.



Al ejecutarlo podemos ver que estamos dentro con el comando **ls**.

No es la interfaz más gráfica, ni bonita, pero se llega a entender.



Haremos un cd a la carpeta de root y podremos encontrar un txt, si ejecutamos un cat para leer el fichero podremos encontrar la flag.

```
cd root
ls
3TfG2Cmq
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
e26e43628249757b39bc83809bade60e
```

Ahora para la flag del usuario de igual manera nos dirigiremos al directorio donde se encuentran los usuarios. /home y podemos ver los usuarios con los que cuentan, nos movemos a la carpeta del usuario **makis** y con un **ls** podremos encontrar de igual manera un **txt** donde esta la flag.

```
cd /home
ls
ftp
makis
service
user
cd makis
ls
HNxZ3lrO
malicious_file.exe
user.txt
cat user.txt
bb25491382905243bfb8f463943b9ba4
```

Esto más que una guía, es una inspiración a futuro para ver mi evolución.