Descripción

Esta máquina es bastante básica y a mi parecer está muy bien para la preparación del examen de la certificación **eJPTv2** ya que cubre una enumeración y explotación bastante básica

Herramientas empleadas en está máquina

- NMAP
- METASPLOIT
- SEARCHSPLOIT

Enumeración

Empezamos la enumeración con un escaneo de puertos

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.3 -oN lame
```

Obtenemos esta información del escaneo

```
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 10.10.16.16
|      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:
|_clock-skew: mean: 2h30m21s, deviation: 3h32m09s, median: 20s
| 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: 2025-01-31T17:44:12-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

En los resultados del escaneo podemos encontrar los puertos **21**, **22**, **139**, **445** y **3632**

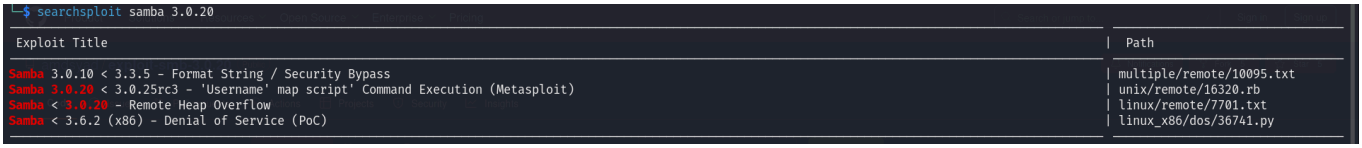
Si nos fijamos en el puerto **445** (smb) podremos ver la versión de **samba**

```
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

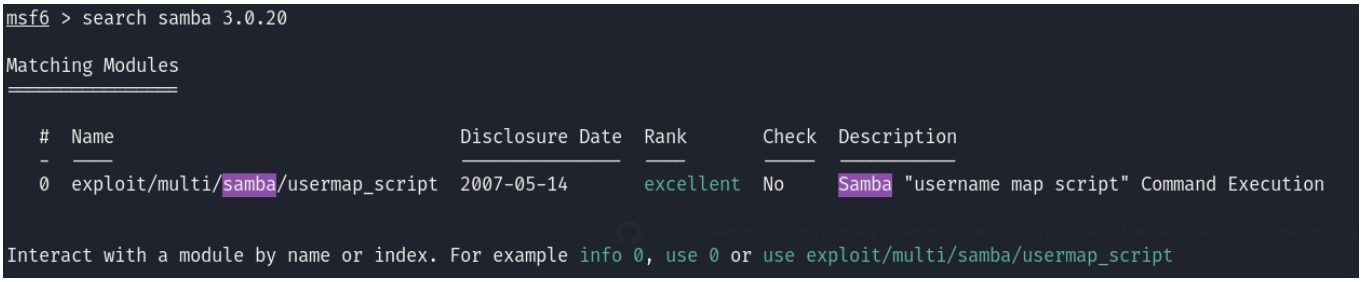
Versión 3.0.20

Explotación

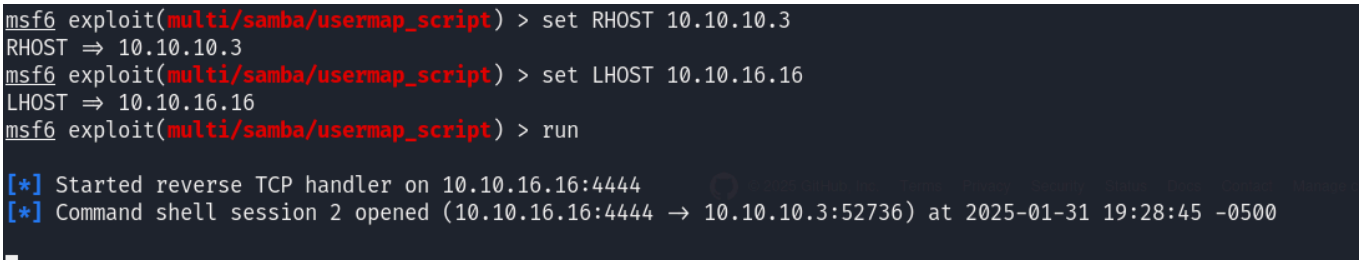
Vamos a usar la herramienta **searchsploit** para buscar exploits para la versión de samba que tenemos



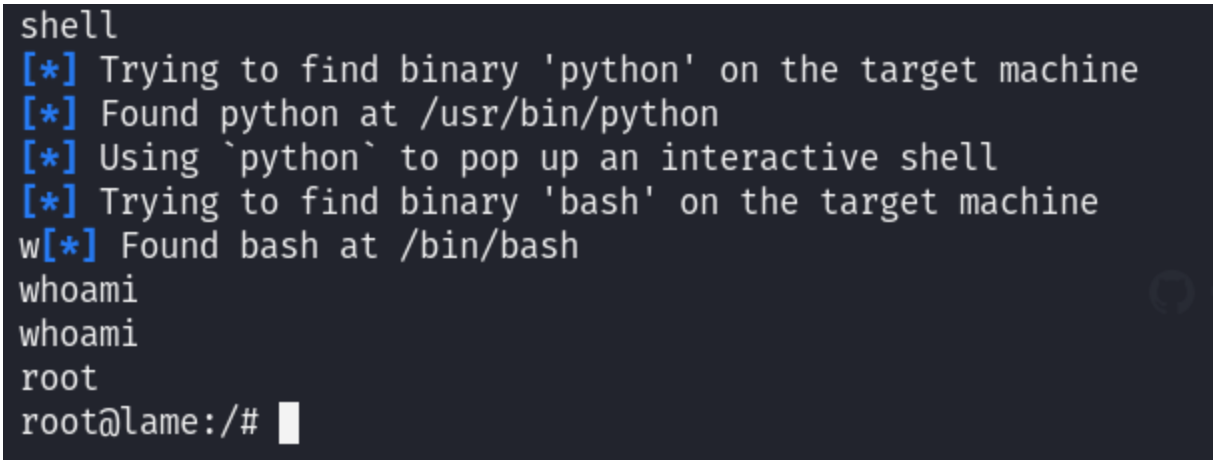
Por lo que podemos ver tenemos un módulo de **Metasploit** para la versión exacta de **SAMBA**, abriremos **Metasploit** y buscaremos el módulo



Usamos el módulo, lo configuramos y lanzamos el exploit



Ahora tendremos una sesión shell con privilegios



Ahora simplemente tendremos que buscar la rootflag y la userflag