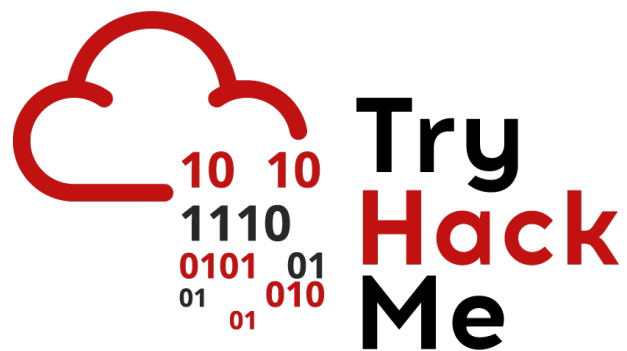


Writeup: Sala *Active Reconnaissance*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 - Introducción	2
2.2. Tarea 2 - Navegador Web	2
2.3. Tarea 3 - Ping	3
2.4. Tarea 4 - Traceroute	4
2.5. Tarea 5 - Telnet	5
2.6. Tarea 6 - NetCat	6
2.7. Tarea 7 - Poniéndolo todo junto	7
3. Conclusión sobre la Sala	7

1. Introducción

En esta sala conoceremos las técnicas fundamentales de reconocimiento activo dentro del ciclo de un pentest. Aprenderemos cómo utilizar herramientas comunes y preinstaladas como el navegador, ping, traceroute, telnet y netcat para interactuar directamente con un objetivo y recolectar información útil.

2. Sala

2.1. Tarea 1 - Introducción

En esta primera tarea diferenciamos el reconocimiento pasivo, que consiste en recopilar información sin interactuar directamente con el objetivo, del reconocimiento activo, donde se hacen conexiones directas a la víctima. También, indica que haremos uso de herramientas comunes como navegador, ping, traceroute, telnet y netcat, que son esenciales para la fase activa del reconocimiento.

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

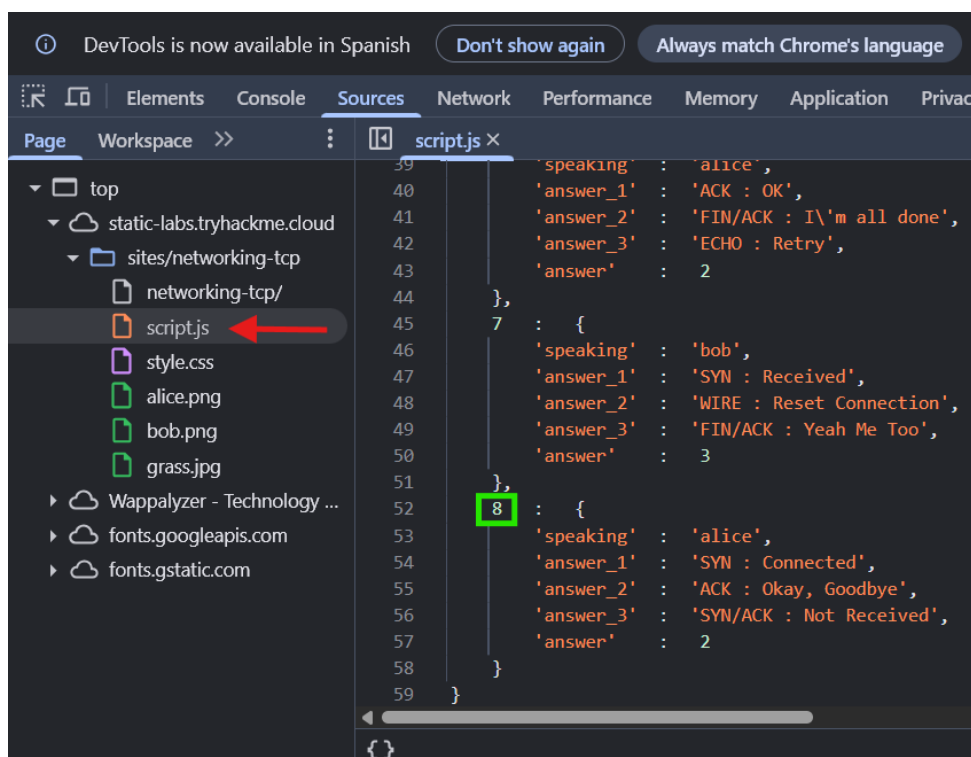
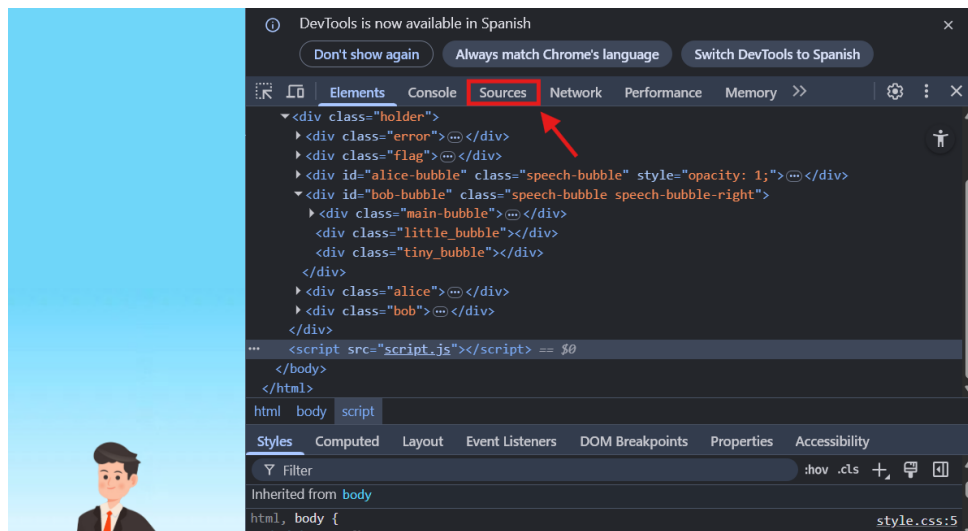
2.2. Tarea 2 - Navegador Web

En esta tarea aprenderemos cómo un navegador no solo sirve para navegar, sino también para recolectar información técnica del objetivo. También, vamos a aprender a usar la **Devtool** y de extensiones recomendadas como **FoxyProxy**, **User-Agent Switcher and Manager** y **Wappalyzer**.

Ahora, debemos visitar el **siguiente sitio web** y tener abierto la DevTool en nuestro navegador para lograr resolver la siguiente pregunta.

Pregunta: Using the Developer Tools, figure out the total number of questions.

Para encontrar la cantidad total de preguntas, debemos dirigirnos a la sección **Source** en la DevTool y haremos clic en **script.js**. Nos encontraremos con una colección de las preguntas y respuestas, bajaremos hasta el final y veremos el número de la cantidad total de preguntas.



Respuesta: 8

2.3. Tarea 3 - Ping

Aquí vamos a conocer el comando **ping** como una herramienta básica para saber si un host está en línea, a través de paquetes ICMP. Además, el uso de opciones como **-c** y **-n** para establecer recuento de paquetes.

Después de lograr comprender el **ping**, vamos a responder las siguientes preguntas.

Pregunta: Which option would you use to set the size of the data carried by the ICMP echo request?

Respuesta: -s

Pregunta: What is the size of the ICMP header in bytes?

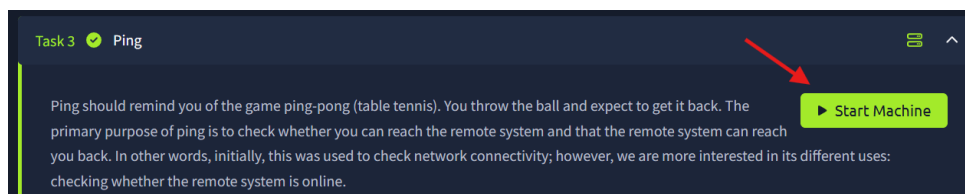
Respuesta: 8

Pregunta: Does MS Windows Firewall block ping by default? (Y/N)

Respuesta: Y

Pregunta: Deploy the VM for this task and using the AttackBox terminal, issue the command `ping -c 10 MACHINE_IP`. How many ping replies did you get back?

Para lograr responder a esta pregunta, debemos iniciar la máquina objetivo de la tarea, para ello, haremos clic en **Start Machine** en el lado superior.



Una vez iniciada, se nos proporcionará una IP objetivo a la cual debemos realizar un ping ejecutando lo siguiente en nuestra terminal:

ping -c {IP}

Al finalizar, se nos presentará la cantidad de respuestas que recibimos

```
(kali㉿kali)-[~]  
$ ping -c 10 10.10.52.90  
PING 10.10.52.90 (10.10.52.90) 56(84) bytes of data.  
  
— 10.10.52.90 ping statistics —  
10 packets transmitted, 0 received, 100% packet loss, time 9217ms
```

Respuesta: 10

2.4. Tarea 4 - Traceroute

Ahora abordaremos el aprendizaje de cómo traceroute permite trazar la ruta que recorren los paquetes hasta el objetivo, mostrando cada salto o router intermedio.

Una vez comprendido como funciona **traceroute** podemos pasar a responder las siguientes preguntas.

Pregunta: In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?

```

user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (172.67.69.208), 30 hops max, 60 byte packets
 1  ec2-3-248-240-5.eu-west-1.compute.amazonaws.com (3.248.240.5)  2.663 ms * ec2-3-248-240-13.eu-west-1.compute.amazonaws.com (3.248.240.13)  14.556 ms
 2  100.66.8.86 (100.66.8.86)  43.231 ms 100.65.21.64 (100.65.21.64)  18.886 ms 100.65.22.160 (100.65.22.160)  14.556 ms
 3  * 100.66.16.176 (100.66.16.176)  8.006 ms *
 4  100.66.11.34 (100.66.11.34)  17.401 ms 100.66.10.14 (100.66.10.14)  23.614 ms 100.66.19.236 (100.66.19.236)  17.524 ms
 5  100.66.7.35 (100.66.7.35)  12.808 ms 100.66.6.109 (100.66.6.109)  14.791 ms *
 6  100.65.14.131 (100.65.14.131)  1.026 ms 100.66.5.189 (100.66.5.189)  19.246 ms 100.66.5.243 (100.66.5.243)  19.805 ms
 7  100.65.13.143 (100.65.13.143)  14.254 ms 100.95.18.131 (100.95.18.131)  0.944 ms 100.95.18.129 (100.95.18.129)  0.778 ms
 8  100.95.2.143 (100.95.2.143)  0.680 ms 100.100.4.46 (100.100.4.46)  1.392 ms 100.95.18.143 (100.95.18.143)  0.878 ms
 9  100.100.20.76 (100.100.20.76)  7.819 ms 100.92.11.36 (100.92.11.36)  18.669 ms 100.100.20.26 (100.100.20.26)  0.842 ms
10  100.92.11.112 (100.92.11.112)  17.852 ms * 100.92.11.158 (100.92.11.158)  16.687 ms
11  100.92.211.82 (100.92.211.82)  19.713 ms 100.92.0.126 (100.92.0.126)  18.603 ms 52.93.112.182 (52.93.112.182)  17.738 ms
12  99.83.69.207 (99.83.69.207)  17.603 ms 15.827 ms 17.351 ms
13  100.92.9.83 (100.92.9.83)  17.894 ms 100.92.79.136 (100.92.79.136)  21.250 ms 100.92.9.118 (100.92.9.118)  18.166 ms
14  172.67.69.208 (172.67.69.208)  17.976 ms 16.945 ms 100.92.9.3 (100.92.9.3)  17.709 ms

```

Respuesta: 172.67.69.208

Pregunta: In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?

Respuesta: 104.26.11.229

Pregunta: In Traceroute B, how many routers are between the two systems?

Respuesta: 26

```

user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (104.26.11.229), 30 hops max, 60 byte packets
 1  ec2-79-125-1-9.eu-west-1.compute.amazonaws.com (79.125.1.9)  1.475 ms * ec2-3-248-240-31.eu-west-1.compute.amazonaws.com (3.248.240.31)  22.267 ms
 2  100.65.20.160 (100.65.20.160)  16.575 ms 100.66.8.226 (100.66.8.226)  23.241 ms 100.65.23.192 (100.65.23.192)  22.267 ms
 3  100.66.16.50 (100.66.16.50)  2.777 ms 100.66.11.34 (100.66.11.34)  22.288 ms 100.66.16.28 (100.66.16.28)  4.421 ms
 4  100.66.6.47 (100.66.6.47)  17.264 ms 100.66.7.161 (100.66.7.161)  39.562 ms 100.66.10.198 (100.66.10.198)  15.958 ms
 5  100.66.5.123 (100.66.5.123)  20.099 ms 100.66.7.239 (100.66.7.239)  19.253 ms 100.66.5.59 (100.66.5.59)  15.397 ms
 6  * 100.66.5.223 (100.66.5.223)  16.172 ms 100.65.15.135 (100.65.15.135)  0.424 ms
 7  100.65.12.135 (100.65.12.135)  0.390 ms 100.65.12.15 (100.65.12.15)  1.045 ms 100.65.14.15 (100.65.14.15)  1.036 ms
 8  100.100.4.16 (100.100.4.16)  0.482 ms 100.100.20.122 (100.100.20.122)  0.795 ms 100.95.2.143 (100.95.2.143)  0.827 ms
 9  100.100.20.86 (100.100.20.86)  0.442 ms 100.100.4.78 (100.100.4.78)  0.347 ms 100.100.20.20 (100.100.20.20)  1.388 ms
10  100.92.212.20 (100.92.212.20)  11.611 ms 100.92.11.54 (100.92.11.54)  12.675 ms 100.92.11.56 (100.92.11.56)  10.835 ms
11  100.92.6.52 (100.92.6.52)  11.427 ms 100.92.6.50 (100.92.6.50)  11.033 ms 100.92.210.50 (100.92.210.50)  10.551 ms
12  100.92.210.139 (100.92.210.139)  10.026 ms 100.92.6.13 (100.92.6.13)  14.586 ms 100.92.210.69 (100.92.210.69)  12.032 ms
13  100.92.79.12 (100.92.79.12)  12.011 ms 100.92.79.68 (100.92.79.68)  11.318 ms 100.92.80.84 (100.92.80.84)  10.496 ms
14  100.92.9.27 (100.92.9.27)  11.354 ms 100.92.80.31 (100.92.80.31)  13.000 ms 52.93.135.125 (52.93.135.125)  11.412 ms
15  150.222.241.85 (150.222.241.85)  9.660 ms 52.93.135.81 (52.93.135.81)  10.941 ms 150.222.241.87 (150.222.241.87)  16.543 ms
16  100.92.228.102 (100.92.228.102)  15.168 ms 100.92.227.41 (100.92.227.41)  10.134 ms 100.92.227.52 (100.92.227.52)  11.756 ms
17  100.92.232.111 (100.92.232.111)  10.589 ms 100.92.231.69 (100.92.231.69)  16.664 ms 100.92.232.37 (100.92.232.37)  13.089 ms
18  100.91.205.140 (100.91.205.140)  11.551 ms 100.91.201.62 (100.91.201.62)  10.246 ms 100.91.201.36 (100.91.201.36)  11.368 ms
19  100.91.205.79 (100.91.205.79)  11.112 ms 100.91.205.83 (100.91.205.83)  11.040 ms 100.91.205.33 (100.91.205.33)  10.114 ms
20  100.91.211.45 (100.91.211.45)  9.486 ms 100.91.211.79 (100.91.211.79)  13.693 ms 100.91.211.47 (100.91.211.47)  13.619 ms
21  100.100.6.81 (100.100.6.81)  11.522 ms 100.100.68.70 (100.100.68.70)  10.181 ms 100.100.6.21 (100.100.6.21)  11.687 ms
22  100.100.65.131 (100.100.65.131)  10.371 ms 100.100.92.6 (100.100.92.6)  10.939 ms 100.100.65.70 (100.100.65.70)  23.703 ms
23  100.100.2.74 (100.100.2.74)  15.317 ms 100.100.66.17 (100.100.66.17)  11.492 ms 100.100.88.67 (100.100.88.67)  35.312 ms
24  100.100.16.16 (100.100.16.16)  19.155 ms 100.100.16.28 (100.100.16.28)  19.147 ms 100.100.2.68 (100.100.2.68)  13.718 ms
25  99.83.89.19 (99.83.89.19)  28.929 ms * 21.790 ms
26  104.26.11.229 (104.26.11.229)  11.070 ms 11.058 ms 11.982 ms

```

2.5. Tarea 5 - Telnet

Conoceremos sobre el uso de **Telnet** como un método sencillo para conectarse a servicios en puertos específicos y realizar banner grabbing que al conectarse, se puede leer información que describe el servicio que corre aunque el protocolo sea inseguro. Esto permite verificar rápidamente si un puerto está activo y qué aplicación lo usa.

Después de aprender sobre Telnet, procederemos a usar nuestra máquina objetivo iniciada previamente, continuación la usaremos para responder a las siguientes preguntas.

Pregunta: Open the terminal and use the telnet client to connect to the VM on port 80. What is the name of the running server?

Para encontrar la respuesta, simplemente en nuestra terminal ejecutaremos el comando:

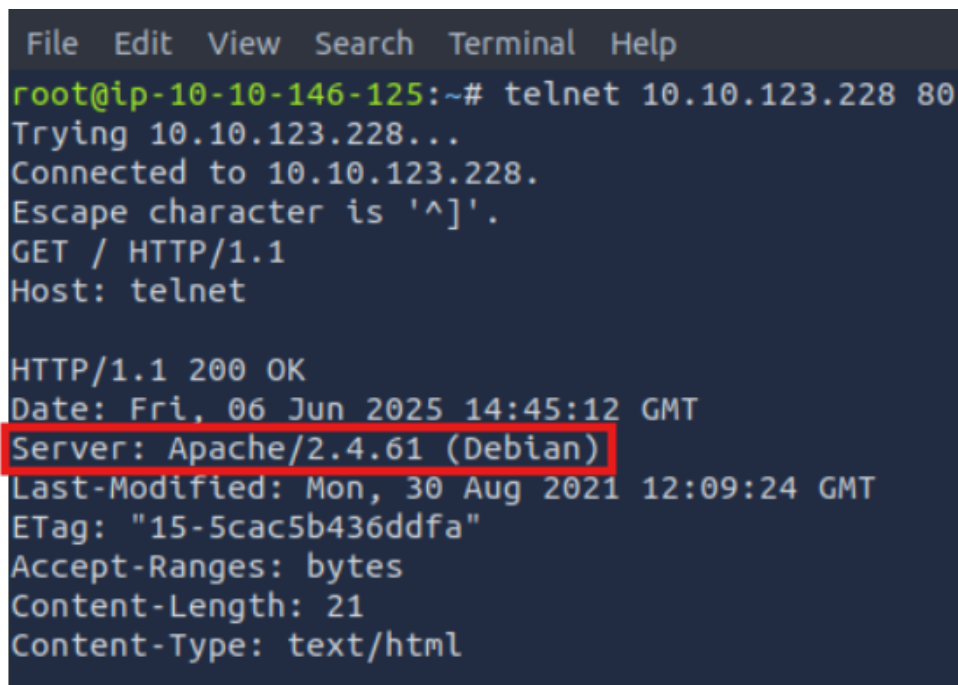
telnet {IP} 80

Una vez que logramos hacer conexión, haremos una petición ejecutando los siguientes comandos en orden:

- **GET / HTTP/1.1**

- **Host: telnet**

Posterior a eso, nos saltará la información que buscamos como respuesta.



```
File Edit View Search Terminal Help
root@ip-10-10-146-125:~# telnet 10.10.123.228 80
Trying 10.10.123.228...
Connected to 10.10.123.228.
Escape character is '^]'.
GET / HTTP/1.1
Host: telnet

HTTP/1.1 200 OK
Date: Fri, 06 Jun 2025 14:45:12 GMT
Server: Apache/2.4.61 (Debian)
Last-Modified: Mon, 30 Aug 2021 12:09:24 GMT
ETag: "15-5cac5b436ddfa"
Accept-Ranges: bytes
Content-Length: 21
Content-Type: text/html
```

Respuesta: Apache

Pregunta: What is the version of the running server (on port 80 of the VM)?

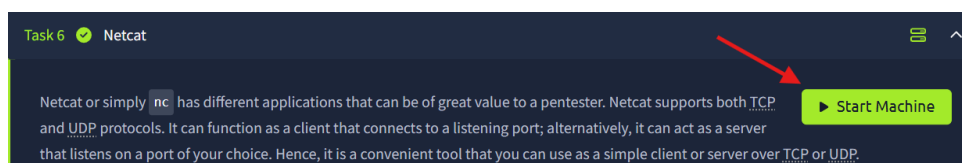
Respuesta: 2.4.61

2.6. Tarea 6 - NetCat

Aprenderemos sobre **NetCat** como una herramienta versátil para conectarse o escuchar en cualquier puerto TCP/UDP. Sirve tanto como cliente para conectarse a servicios, como servidor para recibir conexiones.

Una vez logramos aprender sobre la herramienta de **NetCat**, pasamos a iniciar una máquina objetivo para lograr responder a continuación a la siguiente pregunta.

Para iniciar la máquina, debemos hacer clic en **Start Machine** en el lado superior.



Ya iniciada podemos pasar a la parte práctica para responder a la siguiente pregunta.

Pregunta: Use Netcat to connect to the VM port 21. What is the version of the running server?

Para encontrar la versión en la cual está corriendo el servidor, debemos intentar hacer conexión al puerto 21 de la IP objetivo de la máquina. Ejecutaremos el comando:

nc {IP} 21

De esta manera, lograremos hacer una escucha y encontraremos el número de versión.

```
root@ip-10-10-152-23:~# nc 10.10.218.149 21
220 ip-10-10-218-149.eu-west-1.compute.internal FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
```

Respuesta: **0.17**

2.7. Tarea 7 - Poniéndolo todo junto

En esta tarea final, se describe cómo combinar estas herramientas en guiones o flujos manuales básicos: usar traceroute para mapear rutas, ping para verificar disponibilidad, telnet/netcat para comprobar servicios en puertos, y navegador para inspeccionar web.

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

3. Conclusión sobre la Sala

Al finalizar la sala hemos logrado aprender a cómo aplicar diversas herramientas básicas pero poderosas para realizar reconocimiento activo de forma manual.