Writeup: Sala *FurtherNmap*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025

Índice

1. Introducción

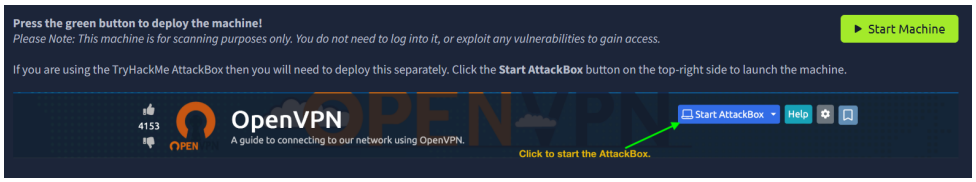
La sala Further Nmap de TryHackMe profundiza en técnicas avanzadas de escaneo y evasión con Nmap, ofreciendo un entorno práctico para fortalecer tus habilidades de reconocimiento en redes. Mediante una serie de retos guiados en una máquina virtual controlada, experimentarás escenarios reales que te obligarán a adaptar tus métodos y afinar tu enfoque en cada fase del escaneo.

Además, explorarás el motor de scripting de Nmap y aprenderás a gestionar y exportar los resultados de manera profesional, consolidando herramientas clave para pruebas de penetración discretas y eficientes

2. Sala

2.1. Tarea 1 - Deploy

La sala se compone de 15 tareas y para comenzar debemos iniciar nuestra maquina virtual como primera tarea.



Una vez inicializada podemos proceder a darle enviar (**Submit**) a la tarea directamente ya que cumplimos nuestro primer objetivo que es darle inicio a la maquina.

2.2. Tarea 2 - Introducción

En esta etapa se sientan las bases para comprender por qué Nmap es una herramienta fundamental en el reconocimiento durante una auditoría de seguridad. Permite identificar qué puertos están abiertos en un sistema, lo cual es esencial para descubrir servicios expuestos que puedan ser vulnerables. Cada máquina cuenta con un rango de 65.535 puertos TCP y UDP, y conocer qué puertos están accesibles puede darnos información crítica sobre los servicios que se ejecutan detrás (por ejemplo, HTTP en el puerto 80 o SSH en el 22).

También, se introduce el concepto de estados de puertos: abiertos, cerrados y filtrados, que permiten interpretar cómo responde un sistema ante nuestras sondas.

Según lo leído en esta segunda tarea podemos responder las siguientes preguntas

Pregunta: What networking constructs are used to direct traffic to the right application on a server?

Respuesta: **Ports**

Pregunta: How many of these are available on any network-enabled computer?

Respuesta: **65535**

Pregunta: How many of these are considered well-known? (These are the standard numbers mentioned in the task)

Respuesta: **1024**

2.3. Tarea 3 - Nmap Switches

En esta tarea nos introducimos en el concepto de switches o conmutadores en Nmap, los cuales permiten personalizar y optimizar los escaneos según las necesidades específicas. Se destaca la importancia de familiarizarse con estos switches para realizar escaneos más efectivos y adaptados a diferentes escenarios.

A través del uso del comando **nmap -h** o usando la página del manual de **Nmap** podemos explorar y comprender los distintos switches disponibles, dominar estos parámetros es esencial para aprovechar al máximo las capacidades de Nmap en tareas de reconocimiento y análisis de redes.

```
┌──(kali㉿kali)-[~]
└─$ nmap -h
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
```

Una vez comprendido esta tarea podemos pasar a responder las siguientes preguntas

Pregunta: What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?
Respuesta: **-sS**

Pregunta: Which switch would you use for a UDP scan?
Respuesta: **-sU**

Pregunta: If you wanted to detect which operating system the target is running on, which switch would you use?
Respuesta: **-O**

Pregunta: Nmap provides a switch to detect the version of the services running on the target. What is this switch?
Respuesta: **-sV**

Pregunta: The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?
Respuesta: **-v**

Pregunta: Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?
Respuesta: **-vv**

Pregunta: What switch would you use to save the nmap results in three major formats?
Respuesta: **-oA**

Pregunta: What switch would you use to save the nmap results in a normal format?
Respuesta: **-oN**

Pregunta: A very useful output format: how would you save results in a grepable format?
Respuesta: **-oG**

Pregunta: Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable .ªggressive"mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

How would you activate this setting?
Respuesta: -A

Pregunta: How would you set the timing template to level 5?
Respuesta: -T5

Pregunta: How would you tell nmap to only scan port 80?
Respuesta: -p 80

Pregunta: How would you tell nmap to scan ports 1000-1500?
Respuesta: -p 1000-1500

Pregunta: How would you tell nmap to scan all ports?
Respuesta: -p-

Pregunta: How would you activate a script from the nmap scripting library (lots more on this later!)?
Respuesta: –script

Pregunta: How would you activate all of the scripts in the "vulnçategory?
Respuesta: –script=vuln

2.4. Tarea 4 - Descripción general de Tipos de Escaneos

En esta tarea aprenderemos los diversos métodos de escaneo que Nmap ofrece para identificar puertos abiertos en un sistema objetivo. Cada tipo de escaneo tiene sus propias características, ventajas y desventajas, y su elección depende del contexto del análisis de seguridad.

Los diferentes tipos de escaneos que se presentan son:

- Escaneo TCP Connect (-sT)
- Escaneo SYN (-sS)
- Escaneo UDP (-sU)
- Escaneos NULL, FIN y Xmas (-sN, -sF, -sX)

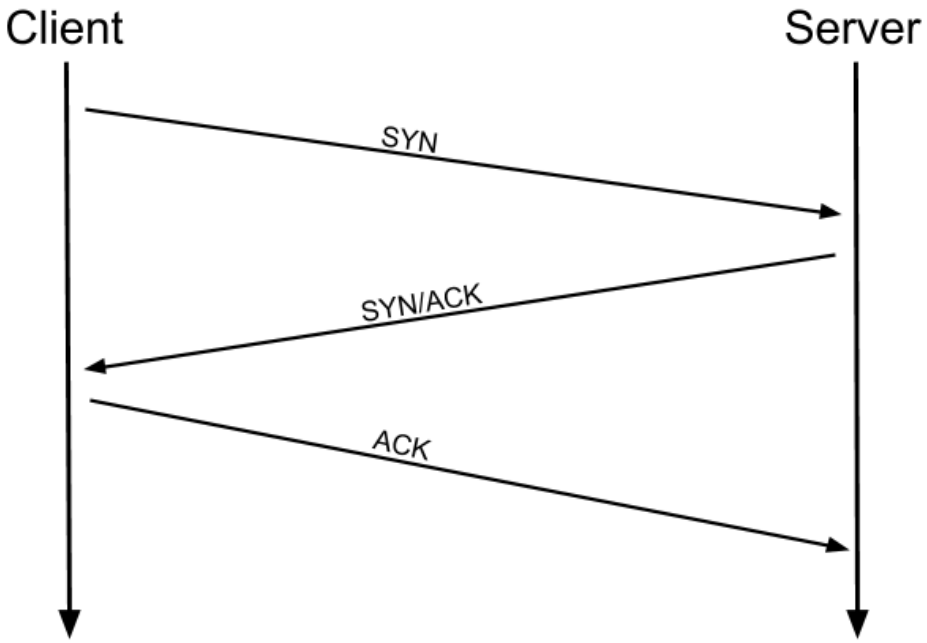
También se menciona el uso de escaneos ICMP (ping) para descubrir hosts activos en la red.

La tarea enfatiza la importancia de comprender cómo y cuándo utilizar cada tipo de escaneo para obtener resultados efectivos y evitar detecciones innecesarias.

Esta tarea no requiere una respuesta, por ende, una vez comprendida podemos simplemente darle a enviar (**Submit**).

2.5. Tarea 5 - Escaneos de conexión TCP

La tarea se profundiza en el método de escaneo TCP Connect (**-sT**) de Nmap, que es el más básico. Este tipo de escaneo se basa en el handshake de tres vías del protocolo TCP:



Si el puerto está cerrado, el servidor responde con un paquete RST (Reset), indicando que no hay servicio escuchando en ese puerto.

Este escaneo es útil cuando no se tienen privilegios elevados, ya que no requiere acceso a funciones de bajo nivel del sistema operativo. Sin embargo, es más fácil de detectar por sistemas de seguridad, ya que establece conexiones completas con los puertos objetivo.

Una vez que entendemos como funciona el protocolo de conexión TCP podemos responder las siguientes preguntas:

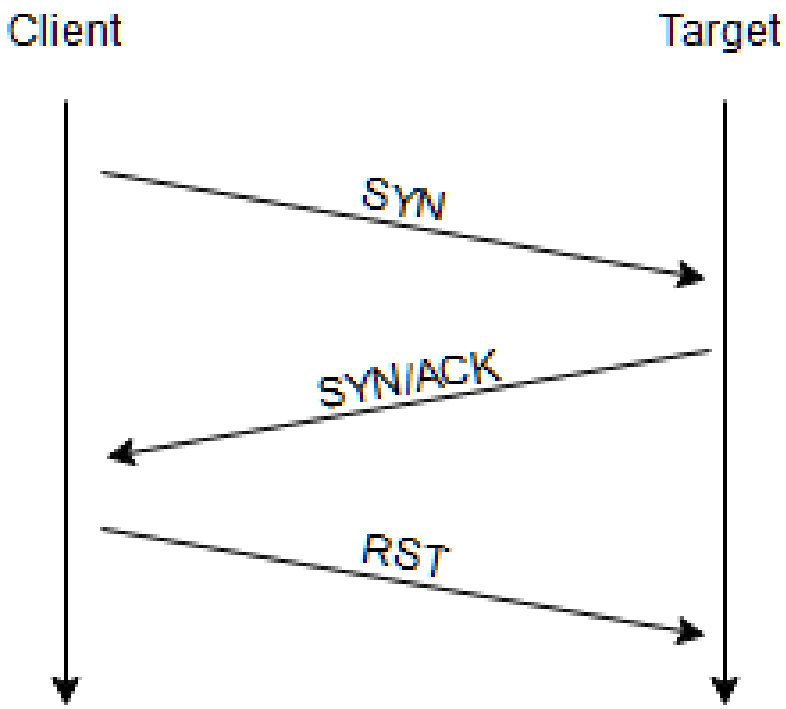
Pregunta: Which RFC defines the appropriate behaviour for the TCP protocol?
Respuesta: **RFC 9293**

Pregunta: If a port is closed, which flag should the server send back to indicate this?
Respuesta: **RST**

2.6. Tarea 6 - Escaneos SYN

En esta tarea, se explora el escaneo SYN (-sS) de Nmap, también conocido como "Half-Open.º "Stealth"scan. Este método envía un paquete SYN al puerto objetivo y,

si recibe un SYN-ACK como respuesta, no completa la conexión, sino que envía un RST para abortarla. Esto permite identificar puertos abiertos sin establecer conexiones completas, lo que lo hace más sigiloso y rápido que el escaneo TCP Connect.



Este tipo de escaneo es útil para evadir ciertos sistemas de detección de intrusos y minimizar el registro en los servicios objetivo, ya que no completa el protocolo de enlace TCP de tres vías. Sin embargo, algunos sistemas modernos pueden detectar este tipo de actividad.

Entendiendo como funciona el escaneo SYN podemos pasar a responder las preguntas de la tarea actual:

Pregunta: There are two other names for a SYN scan, what are they?
Respuesta: **Half-Open, Stealth**

Pregunta: Can Nmap use a SYN scan without Sudo permissions (Y/N)?
Respuesta: **N**

2.7. Tarea 7 - Escaneos UDP

Este tipo de escaneo a diferencia de TCP, UDP es un protocolo sin conexión, lo que significa que no establece una sesión previa antes de enviar datos. Esto complica

la detección de puertos abiertos, ya que, en muchos casos, no se recibe respuesta alguna, dificultando la interpretación de los resultados.

Cuando se envía un paquete UDP a un puerto:

- Si el puerto está **cerrado**, el sistema objetivo suele responder con un mensaje ICMP indicando que el puerto es inalcanzable.
- Si el puerto está **abierto**, es común no recibir respuesta, lo que lleva a Nmap a marcar el puerto como open|filtered, ya que no puede determinar con certeza si está abierto o si un firewall está bloqueando la comunicación.

Debido a la falta de respuestas claras y a la necesidad de esperar tiempos de espera prolongados, los escaneos UDP suelen ser más lentos que los TCP.

En resumen, el escaneo UDP es esencial para una evaluación completa de la superficie de ataque, pero requiere paciencia y una interpretación cuidadosa de los resultados debido a la naturaleza del protocolo.

Al haber aprendido sobre este tipo de escaneo pasamos a responder las siguientes preguntas:

Pregunta: If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

Respuesta: Respuesta: open|filtered

Pregunta: When a UDP port is closed, by convention the target should send back a port unreachable message. Which protocol would it use to do so?

Respuesta: Respuesta: ICMP

2.8. Tarea 8 - NULL, FIN Y Xmas

En esta tarea se presentan tres tipos de escaneo menos convencionales: **NULL**, **FIN** y **Xmas**. Estos métodos envían paquetes TCP con combinaciones inusuales de flags para identificar puertos abiertos sin utilizar el flag SYN, lo que puede ayudar a evadir ciertos firewalls que bloquean conexiones estándar. Sin embargo, su efectividad depende del sistema operativo del objetivo. Por ejemplo, sistemas como Microsoft Windows tienden a responder con paquetes RST a cualquier paquete malformado, independientemente del estado del puerto, lo que puede llevar a resultados inexactos.

En resumen, estos escaneos ofrecen una alternativa más sigilosa para la detección de puertos, pero su fiabilidad varía según la configuración del sistema objetivo.

Después de estudiar estos tipos de escaneos podemos responder las siguientes preguntas:

Pregunta: Which of the three shown scan types uses the URG flag?
Respuesta: Respuesta: Xmas

Pregunta: Why are NULL, FIN and Xmas scans generally used?
Respuesta: Respuesta: Firewall Evasion

Pregunta: Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?
Respuesta: Respuesta: Microsoft Windows

2.9. Tarea 9 - Escaneo de red ICMP

En esta tarea estudiaremos el escaneo de red mediante ICMP, comúnmente conocido como "ping sweep". Este método permite identificar hosts activos en una red enviando paquetes ICMP a un rango de direcciones IP especificado.

Es importante tener en cuenta que algunos sistemas pueden estar configurados para no responder a solicitudes ICMP, lo que podría llevar a falsos negativos. Por lo tanto, aunque el escaneo ICMP es una herramienta valiosa para la detección de hosts, sus resultados deben interpretarse con precaución y, si es necesario, complementarse con otros métodos de escaneo.

Este enfoque proporciona una base sólida para la enumeración inicial en evaluaciones de seguridad y pruebas de penetración.

Después de que logramos entender como funciona el escaneo de red ICMP podemos responder la siguiente pregunta:

Pregunta: How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)
Respuesta: nmap -sn 172.16.0.0/16

2.10. Tarea 10 - Descripción general de NSE Scripts

En esta tarea conoceremos a **Nmap Scripting Engine (NSE)**, una potente funcionalidad que amplía las capacidades de Nmap mediante scripts escritos en el lenguaje de programación Lua. Estos scripts permiten automatizar diversas tareas, como la detección de vulnerabilidades, la recopilación de información y la ejecución de pruebas de penetración, además, los scripts NSE se encuentran organizados en diferentes categorías.

NSE convierte a Nmap en una herramienta más versátil y poderosa para evaluaciones de seguridad, permitiendo realizar análisis más profundos y automatizados.

Después de entender que es NSE podemos pasar a responder las siguientes preguntas:

Pregunta: What language are NSE scripts written in?
Respuesta: **Lua**

Pregunta: Which category of scripts would be a very bad idea to run in a production environment?
Respuesta: Respuesta: **intrusive**

2.11. Tarea 11 - Trabajando con el NSE

Profundizaremos en el uso práctico de la **Nmap Scripting Engine (NSE)**. Se explica cómo ejecutar scripts específicos utilizando el parámetro **–script**, permitiendo así personalizar los escaneos según las necesidades del análisis.

Además, se introduce el uso de **–script-args** para proporcionar argumentos opcionales a los scripts. Por ejemplo, el **script ftp-anon.nse**, que verifica el acceso anónimo en servidores FTP, acepta el argumento **maxlist** para limitar la cantidad de archivos listados durante el escaneo.

Luego de poner en prácica y entender el uso de NSE pasaremos a contestar la siguiente pregunta:

Pregunta: What optional argument can the **ftp-anon.nse** script take?
Respuesta: **maxlist**

2.12. Tarea 12 - Busqueda de Scripts

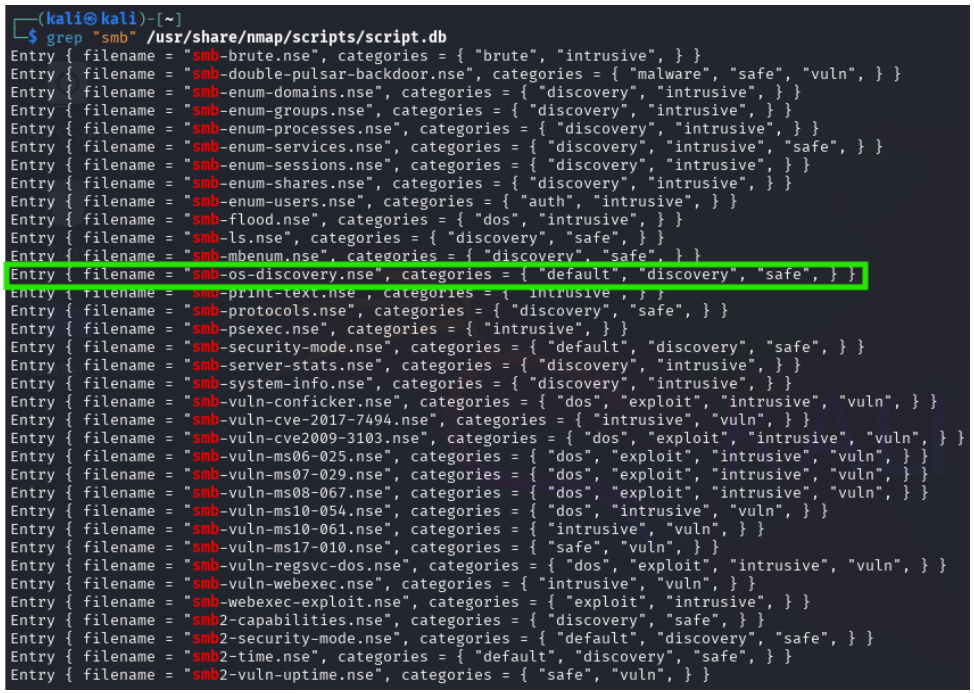
Esta tarea se centra en cómo buscar y gestionar scripts de la **Nmap Scripting Engine (NSE)**. Se presentan métodos para localizar scripts específicos, como utilizar el archivo **script.db** o realizar búsquedas directas en el directorio de scripts.

Además, se explica cómo identificar dependencias entre scripts, lo cual es crucial para ejecutar escaneos efectivos y personalizados.

Una vez que aprendemos a como buscar los scripts pondremos esto en práctica para responder las siguientes preguntas:

Pregunta: Search for **smb** scripts in the /**usr**/**share**/**nmap**/**scripts**/ directory using either of the demonstrated methods. What is the filename of the script which determines the underlying OS of the SMB server?

Para responder a esta pregunta debemos dirigirnos a nuestra terminal y ejecutar lo siguiente para realizar la busqueda **grep 'smb' /usr/share/nmap/scripts/script.db**. Una vez ejecutado procederemos a buscar el nombre del script.



Respuesta: **smb-os-discovery.nse**

Pregunta: Read through this script. What does it depend on?
Respuesta: **smb-brute**

2.13. Tarea 13 - Evasión de Firewall

La tarea aborda técnicas para evadir firewalls y sistemas de detección durante escaneos de red. Se destacan opciones como **-Pn** para omitir la detección de hosts activos, útil cuando los pings están bloqueados, y **–data-length** para añadir datos aleatorios a los paquetes, dificultando su identificación por sistemas de seguridad. Estas estrategias permiten realizar escaneos más discretos en entornos protegidos.

Después de estudiar como funcionan las evasiones a firewall pasamos a responder las siguientes preguntas:

Pregunta: Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the **-Pn** switch?
Respuesta: **ICMP**

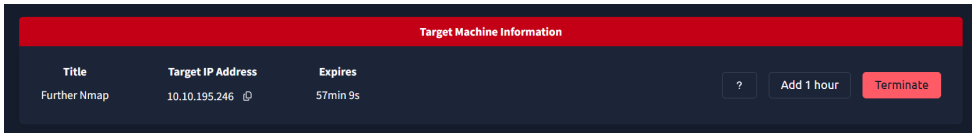
Pregunta: Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

Respuesta: –data-length

2.14. Tarea 14 - Práctica

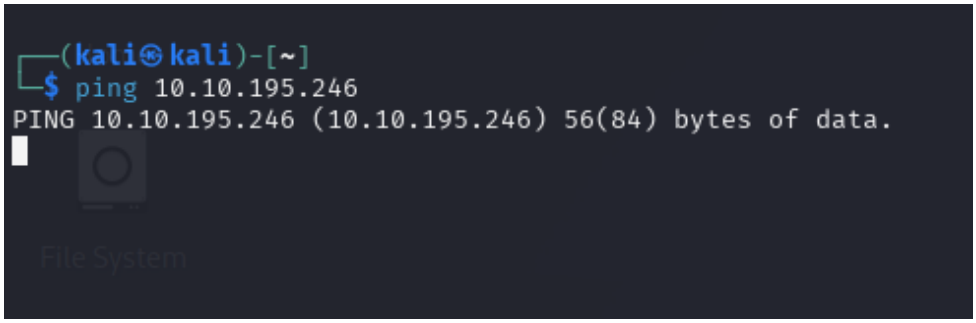
Aquí pondremos en práctica todo lo aprendido en la sala con la IP objetivo de la maquina que nos proporciona **TryHackMe**.

Para iniciar lo primero que haremos es copiar la IP objetivo.



Después vamos a comenzar a responder las siguientes preguntas:

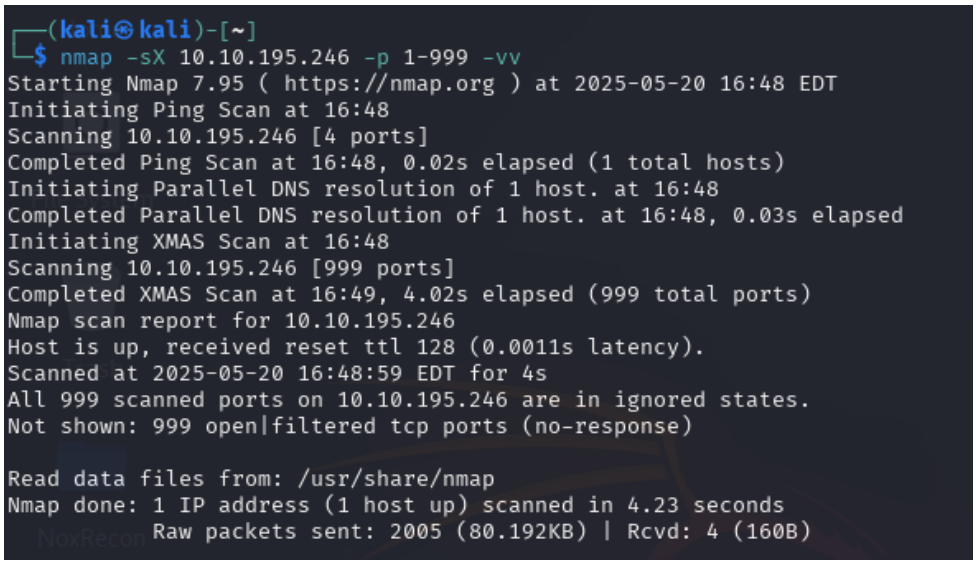
Pregunta: Does the target ip respond to ICMP echo (ping) requests (Y/N)?
Para responder a esta pregunta debemos ejecutar en nuestra terminal lo siguiente:



Respuesta: N

Pregunta: Perform an Xmas scan on the first 999 ports of the target – how many ports are shown to be open or filtered?

Ahora nos toca hacer un escaneo para saber la cantidad de puertos que se encuentran abiertos o filtrados, para ello, vamos a ejecutar lo siguiente en la terminal:



Respuesta: 999

Pregunta: There is a reason given for this – what is it?

Note: The answer will be in your scan results. Think carefully about which switches to use – and read the hint before asking for help!

Respuesta: No Response

Pregunta: Perform a TCP SYN scan on the first 5000 ports of the target – how many ports are shown to be open?

Respuesta: 5

Pregunta: Deploy the **ftp-anon script** against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Respuesta: Y

3. Conclusión

En esta sala logramos adquirir los conocimientos sobre el uso avanzado de Nmap donde se destacaron las diferentes técnicas de escaneo, como **TCP Connect**, **SYN**, **UDP**, **NULL**, **FIN**, **Xmas** e **ICMP**, así como el uso del motor de **scripting NSE** para automatizar tareas y detectar vulnerabilidades. También se abordaron estrategias para evadir firewalls y sistemas de detección.

Esto nos deja a entender la importancia de practicar y consultar la documentación oficial de Nmap para profundizar aún más en el dominio de esta herramienta.