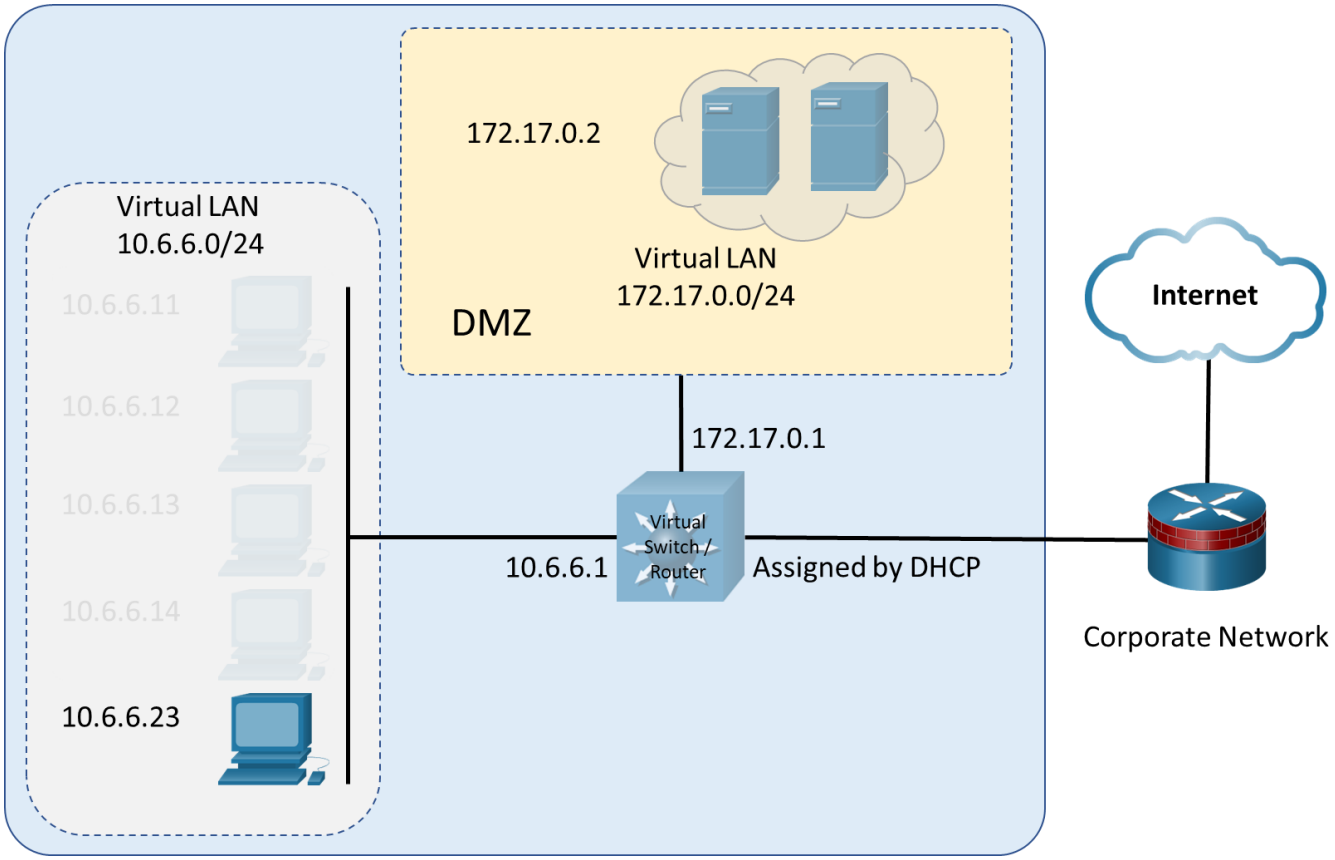
Práctica de laboratorio: Enumeración con Nmap

Topología



Objetivos

Nmap es una potente herramienta de código abierto para la asignación y el descubrimiento de redes. En esta práctica de laboratorio, utilizará Nmap como parte de su estrategia de reconocimiento activa.

- Investigar Nmap
- Realizar escaneos básicos de Nmap

Aspectos básicos/Situación

Una captura de Wireshark muestra una actividad inusual en una máquina en la red DMZ 10.6.6.0. Se le ha pedido que realice un reconocimiento activo en la máquina para determinar qué servicios puede ofrecer y si hay aplicaciones vulnerables que podrían presentar problemas de seguridad. La dirección IP de la computadora sospechosa es 10.6.6.23. Tiene acceso a un sistema Kali Linux en la red 10.6.6.0.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker

Instrucciones

Parte 1: Investigar Nmap

Paso 1: Inicie sesión en Kali Linux y verifique el entorno.

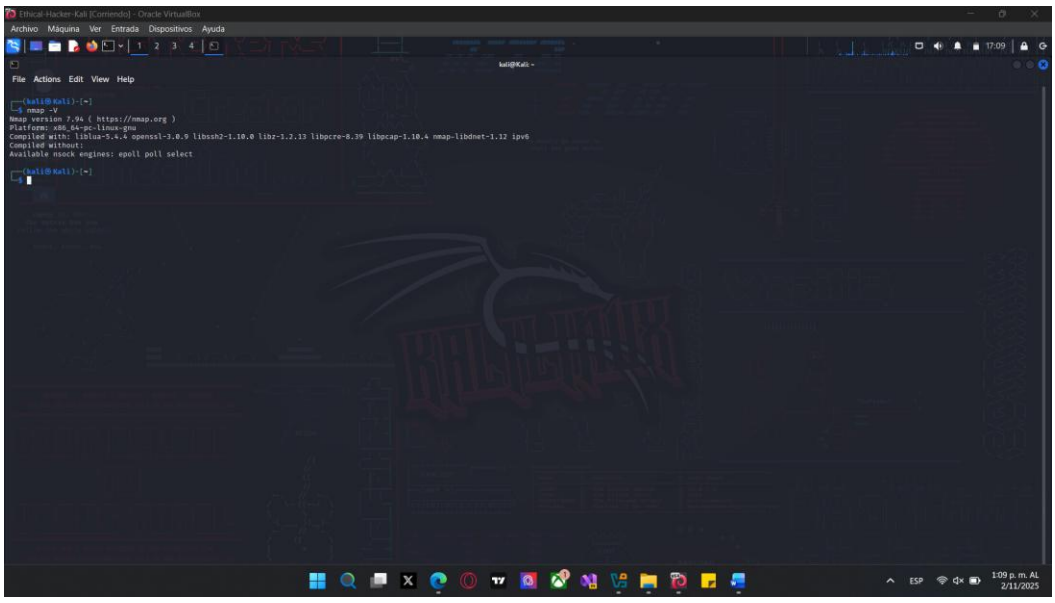
a. Inicie sesión en el sistema Kali con el nombre de usuario **kali** y la contraseña **kali**. Se le presenta el escritorio Kali.

b. Abran una ventana del terminal.

c. Verifique que Kali tenga una interfaz en la red 10.6.6.0/24 mediante el comando **ifconfig**.

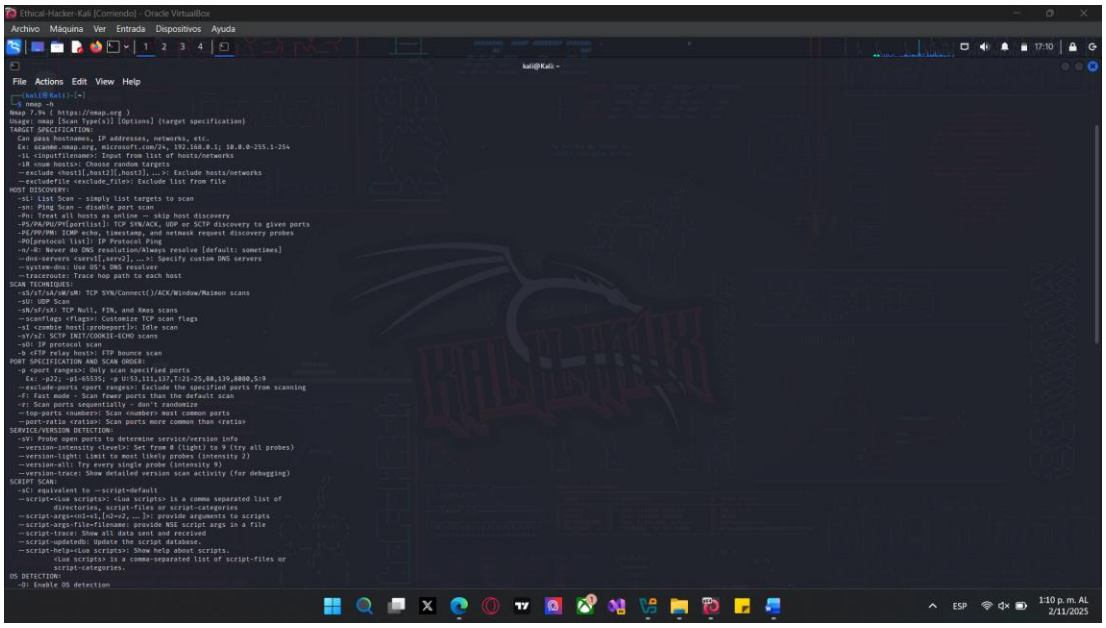
d. Utilice el comando **nmap -V** para verificar que Nmap esté instalado y para mostrar la versión de Nmap. Debería obtener una salida similar a la que se muestra a continuación.

```
┌──(kali㉿Kali)-[~]
└─$ nmap -V
Nmap version 7.93 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.7 libssh2-1.10.0 libz-1.2.11 libpcre-8.39
nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

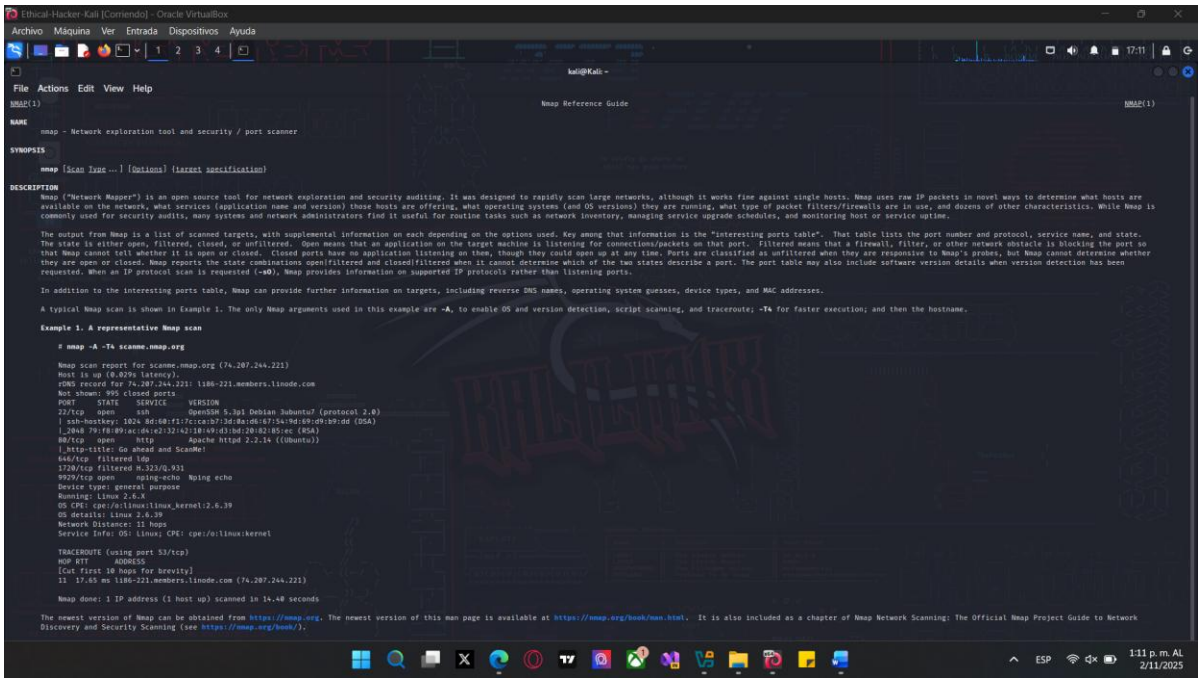


Paso 2: Investigue las opciones y las funciones de Nmap

a. El uso del comando **nmap** sin especificar ninguna opción ni destino devuelve una lista de las opciones de Nmap más utilizadas. Para acceder al sistema de ayuda de Nmap, utilice el comando **nmap -h**. La salida de ayuda se divide en secciones según el tipo de detección que admite la opción.



b. La página del manual de Nmap proporciona información adicional. Para acceder a la página del manual, introduzca el comando **man nmap**. Para salir de las páginas del manual, presione **q** para salir y volver al indicador del terminal.



Utilice la página del manual de Nmap para completar la tabla.

Opciones comunes de Nmap

Opción	Descripción
-A	**Escaneo agresivo que permite la detección del sistema operativo, detección de versiones, escaneo de scripts (guiones) y traceroute (rastreo de rutas)**
-O	**Permite la detección de SO**

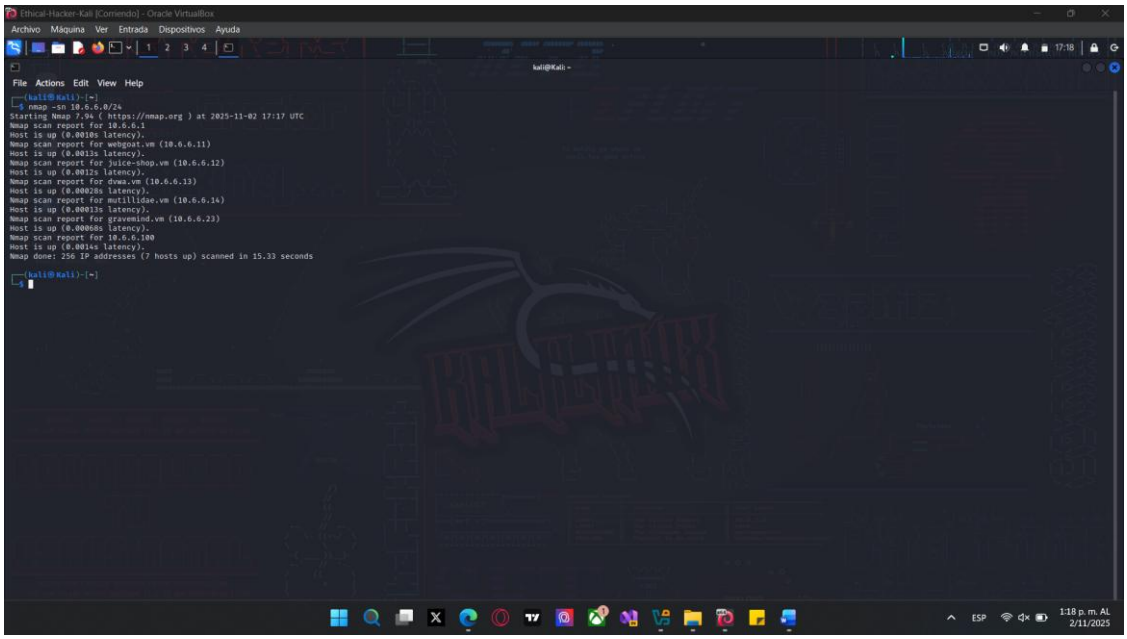
Opción	Descripción
-p <port ranges>	Permite escanear puertos o rangos de puertos específicos
-sF	Realiza un escaneo TCP FIN
-sn	Realiza un escaneo de detección de host
-sS	Realiza escaneo TCP SYN
-sT	Realiza un escaneo de TCP Connect
-sV	Sondeos de puertos abiertos para determinar información de servicio / versión
-T <0-5>	Establece la duración del escaneo. Los números más altos producen resultados más rápidamente. Los escaneos más lentos eluden mejor la detección.
-v	Aumenta el nivel de detalle de la salida.
--open	Solo reporta puertos abiertos (o posiblemente abiertos)

Parte 2: Realizar escaneos básicos de Nmap

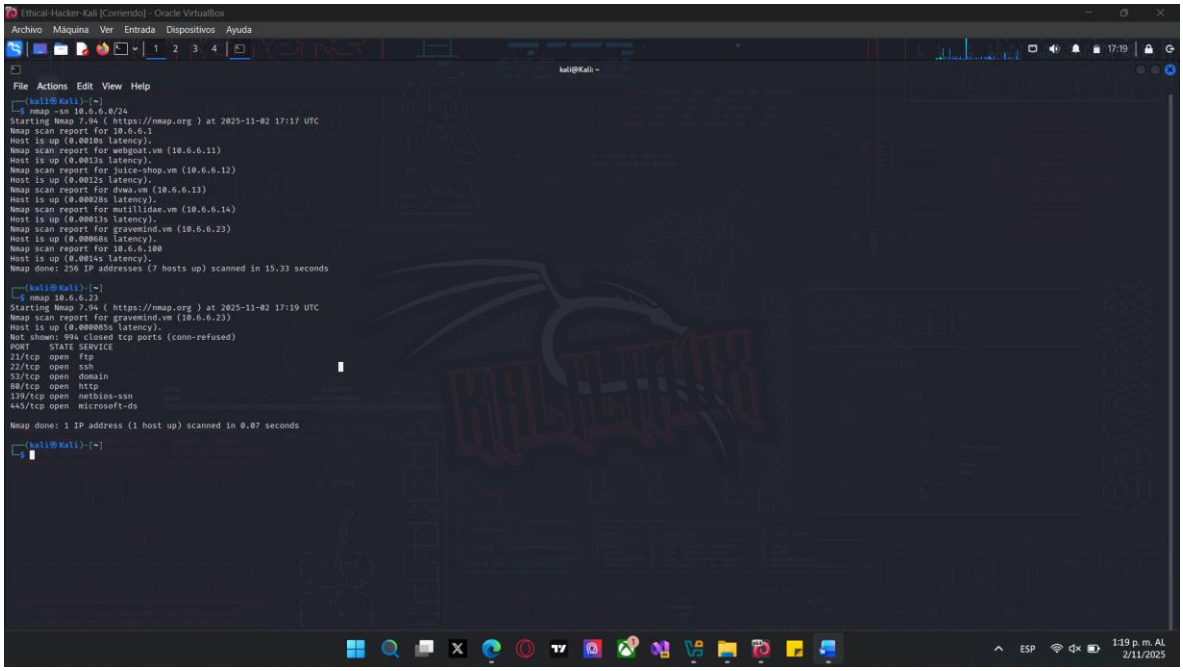
Paso 1: Inicie un escaneo básico de Nmap del equipo de destino.

a. Para escanear rápidamente la DMZ en busca de hosts activos, puede realizar un escaneo de detección. En un escaneo de detección, el host de escaneo envía una solicitud de eco (ping) de ICMP, un TCP SYN al puerto 443, un TCP ACK al puerto 80 y una solicitud de marca de tiempo de ICMP. Una respuesta a cualquiera de las solicitudes indica que el host está activo y la pila de protocolos IP en el host. Ingrese el siguiente comando para escanear la red DMZ:

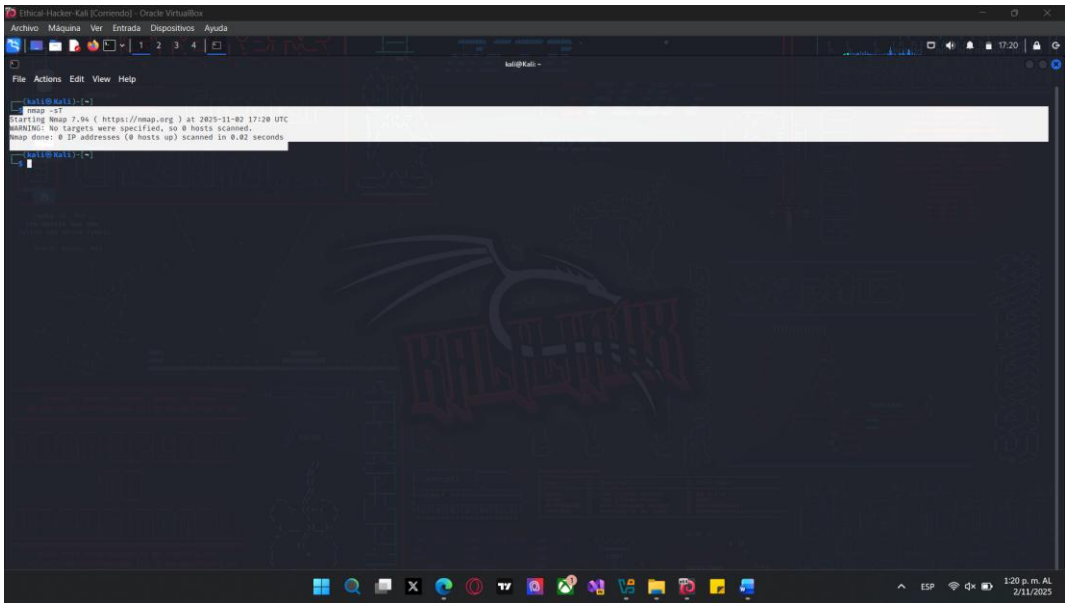
```
┌──(kali㉿Kali)-[~]
└─$ nmap -sn 10.6.6.0/24
```




```
┌──(kali㉿Kali)-[~]
└─$ nmap 10.6.6.23
```



De manera predeterminada, Nmap realiza un escaneo de conexión de los 1000 puertos TCP más comunes. Esto utiliza el software de red del sistema operativo para establecer una conexión TCP completa. Este tipo de escaneo crea una gran cantidad de tráfico de red y aumenta la probabilidad de detección por parte de los servicios de detección de intrusiones. También puede especificar un escaneo de conexión TCP mediante la opción de comando **nmap -sT**.

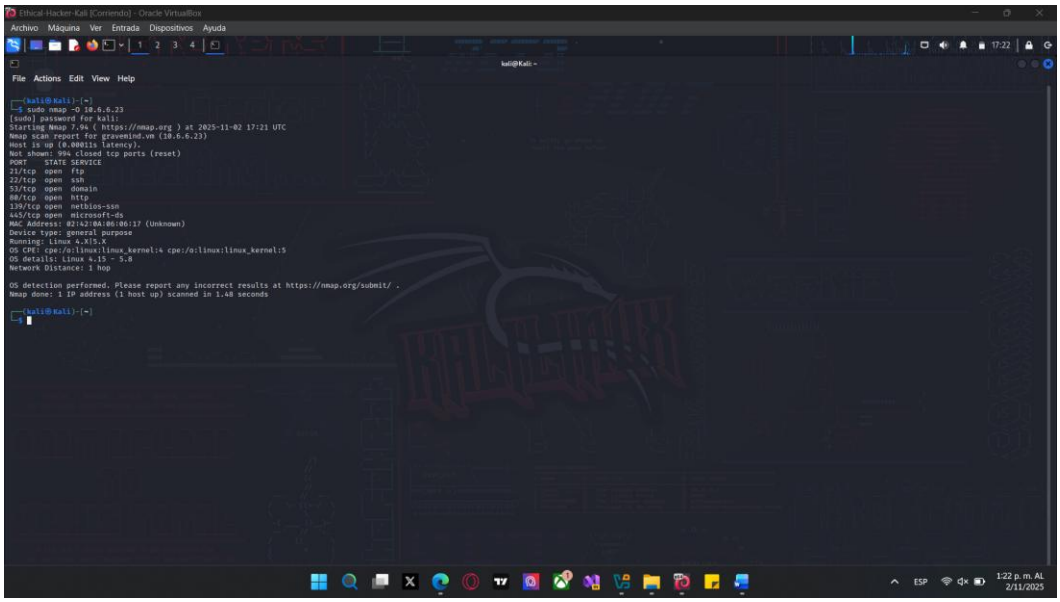


La salida del escaneo de conexión incluye los códigos de estado que se muestran en la tabla:

Estado	Respuesta recibida	Interpretación
Abierto	SYN/ACK de TCP	Hay un servicio a la escucha en el puerto identificado.
Cerrado	TCP RST	No hay ningún servicio a la escucha en el puerto identificado.
Filtrado	No hay respuesta o se recibió un mensaje de destino ICMP inaccesible.	El puerto está siendo filtrado por un firewall.

b. La opción **-O** se puede utilizar para determinar más información sobre el sistema operativo que se ejecuta en el host de destino. Algunas opciones de Nmap requieren permisos adicionales y deben ejecutarse como **root** o con el comando **sudo**. Para encontrar información del sistema operativo en el host de destino, use el comando **nmap -O**. Introduzca la contraseña **kali** cuando se le solicite.

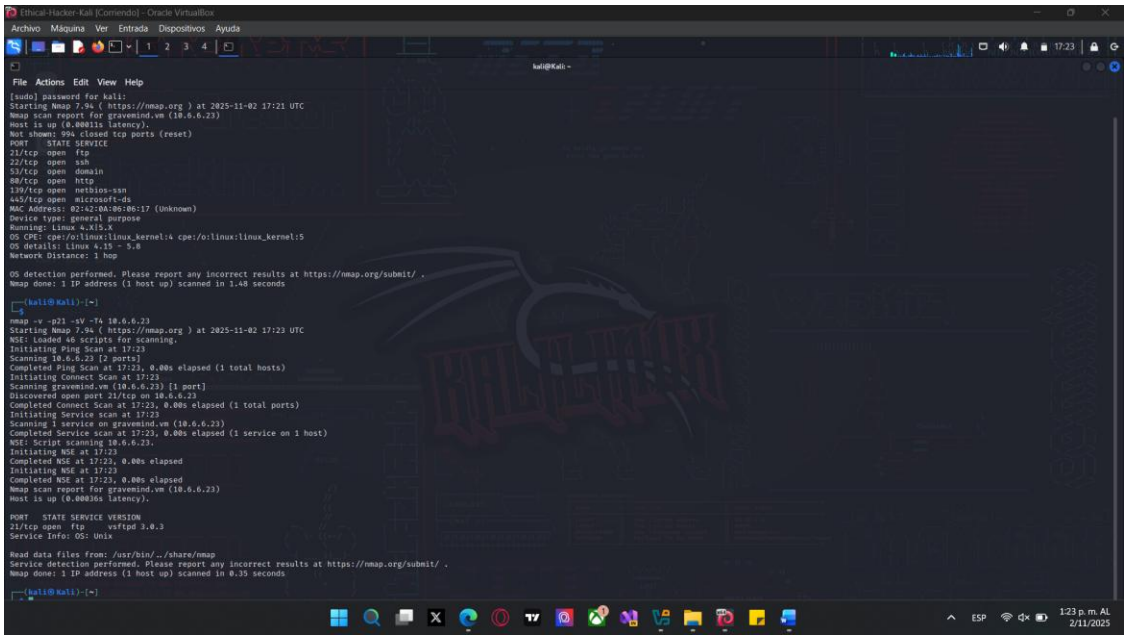
```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 10.6.6.23
```



Paso 2: Obtenga información adicional sobre el host y los servicios.

a. Para proporcionar información adicional sobre el equipo de destino, es posible combinar diferentes opciones en una sola línea de comando. El comando anterior identificó varios puertos potencialmente abiertos en el host 10.6.6.23. Puede utilizar **-v**, **-p**y **-sV** para encontrar información adicional sobre los servicios que se ejecutan en los puertos abiertos. Este comando proporciona información sobre el servicio FTP que se ejecuta en el puerto 21 del destino en modo detallado, con la sincronización establecida en rápido (**-T4**):

```
┌──(kali㉿Kali)-[~]
└─$ nmap -v -p21 -sV -T4 10.6.6.23
```



b. La opción **-A** ejecuta la detección del sistema operativo, la detección de la versión, el escaneo de scripts y el traceroute. El escaneo **-A** puede ser muy intrusivo y, por lo tanto, será detectado por muchos

sistemas IDS, así que asegúrese de tener permiso antes de intentar este escaneo fuera del entorno de laboratorio. Para recopilar más información sobre el servicio FTP, ingrese el comando **nmap -A -p21 10.6.6.23**.

A continuación se muestra un ejemplo detallado de la salida de este comando:

```
┌──(kali㉿Kali)-[~]
└─$ nmap -p21 -sV -A 10.6.6.23
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-16 22:36 UTC
Nmap scan report for 10.6.6.23
Host is up (0.00044s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 10.6.6.1
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r-- 1 0 0 16 Aug 13 2021 file1.txt
| -rw-r--r-- 1 0 0 16 Aug 13 2021 file2.txt
| -rw-r--r-- 1 0 0 29 Aug 13 2021 file3.txt
|_-rw-r--r-- 1 0 0 26 Aug 13 2021 supersecretfile.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```