Práctica de laboratorio: uso de un escáner de puertos para detectar puertos abiertos

NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB O LO REALIZADO POR USTED.

Objetivos

Utilice Nmap, un escáner de puertos y una herramienta de asignación de redes para detectar puertos abiertos.

Aspectos básicos/Situación

El asignador de red, o Nmap, es una utilidad de código abierto utilizada para la detección de redes y la auditoría de seguridad. Una tarea común es analizar las máquinas locales para determinar posibles vulnerabilidades, incluidos los puertos abiertos y no administrados. Todas las estaciones de trabajo requieren puertos y servicios abiertos para comunicarse y realizar tareas como imprimir, compartir un archivo o navegar por la Web. Los administradores también utilizan Nmap para monitorear los hosts o administrar los programas de actualización del servicio. Nmap determina qué hosts están disponibles en una red, qué servicios, qué sistemas operativos y qué filtros de paquetes o firewalls se están ejecutando. En esta práctica de laboratorio, utilizará Nmap dentro de su entorno de VM para detectar puertos abiertos.

Introducción a los puertos TCP / UDP

Toda la comunicación que se realiza a través de Internet se intercambia mediante puertos. Cada host IP puede utilizar dos tipos de puertos: TCP y UDP. Puede haber hasta 65 535 de cada uno para cualquier dirección IP.

Los servicios que se conectan a Internet (como navegadores web, clientes de correo electrónico y servicios de transferencia de archivos) utilizan puertos específicos para recibir información. Por lo tanto, a cada conexión lógica se le asigna un número específico. El número de puerto también identifica a través de qué puerto debe enviar o recibir tráfico al comunicarse. La Autoridad de Números Asignados de Internet (IANA) asignó los números de puerto oficiales y dividió estos puertos en tres subcategorías:

- Well-Known Ports (0-1023)
- Registered Ports (1024 - 49,151)
- Dynamic / Private Ports (49,152 - 65,535)

A continuación se enumeran los puertos comunes:

20 - File Transfer Protocol - Data (FTP-DATA)

21 - File Transfer Protocol - Control (FTP)

22 - Secure Shell (SSH)

23 - Telnet (TELNET)

25 - Simple Mail Transfer Protocol (SMTP)

53 - Domain Name System (DNS)

67 - Client to server Dynamic Host Configuration Protocol v4 (DHCPv4)

68 - Server to client Dynamic Host Configuration Protocol v4 (DHCPv4)

69 - Trivial File Transfer Protocol (TFTP)

80 - Hypertext Transfer Protocol (HTTP)

Seguridad de puertos lógicos

Cada puerto lógico está sujeto a una amenaza y representa una vulnerabilidad a un sistema, pero algunos de los puertos de uso común reciben mucha atención de los atacantes. Más del 75% de todos los ataques cibernéticos implican solo unos pocos puertos comunes. Los atacantes analizan los sistemas para identificar los puertos abiertos en un sistema de destino. Aquí hay una lista de posibles puertos lógicos que son los objetivos más comunes de los ciberdelincuentes:

20/21 FTP	67/68 BOOTP	123 NTP
22 SSH	69 TFTP	137-139 NetBIOS
23 Telnet	80 HTTP	143 IMAP
25 SMTP	110 POP3	161 SNMP
50/51 IPsec	111 Port Map	389 LDAP
53 DNS	119 NNTP	443 SSL

Recursos necesarios

- PC con **CSE-LABVM** instalado en VirtualBox.

Instrucciones

Paso 1: Abra una ventana de terminal en CSE-LABVM.

a. Inicie **CSE-LABVM**.

b. Haga doble clic en el icono de **Terminal** para abrir un terminal.

Paso 2: Ejecute Nmap.

En el command prompt, ingrese el siguiente comando para ejecutar un análisis básico contra este sistema:

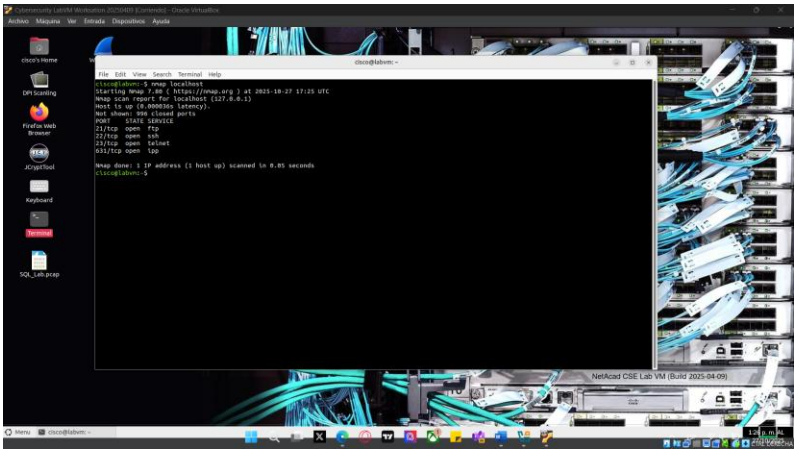
```
cisco@labvm:~$ nmap localhost
```



```
Starting Nmap 7.80 (https://nmap.org) at 2021-03-19 14:14 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000035s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
631/tcp open ipp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Los resultados son el escaneo de los primeros puertos 1024 TCP.



¿Qué puertos TCP están abiertos?

21/tcp open ftp

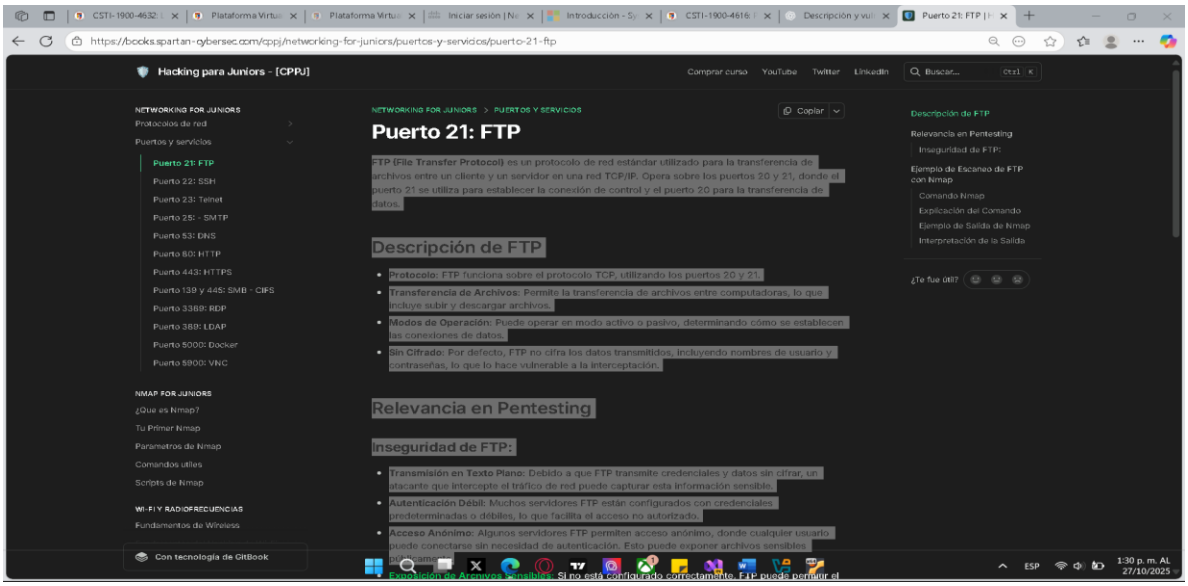
22/tcp open ssh

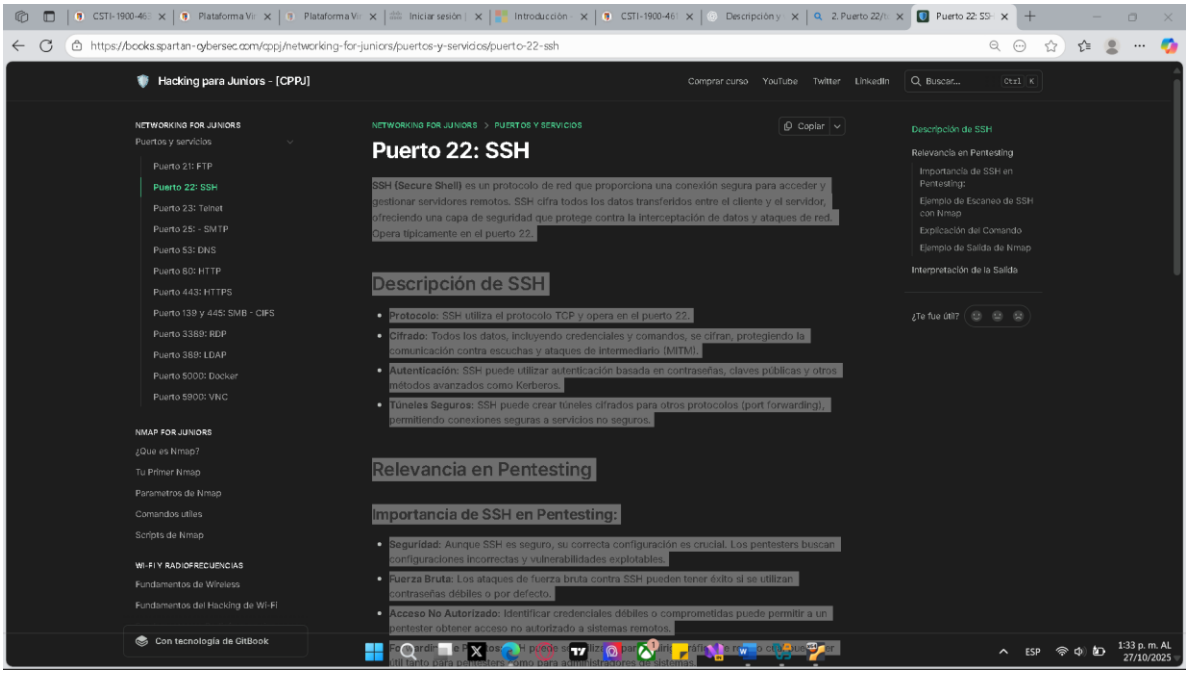
23/tcp open telnet

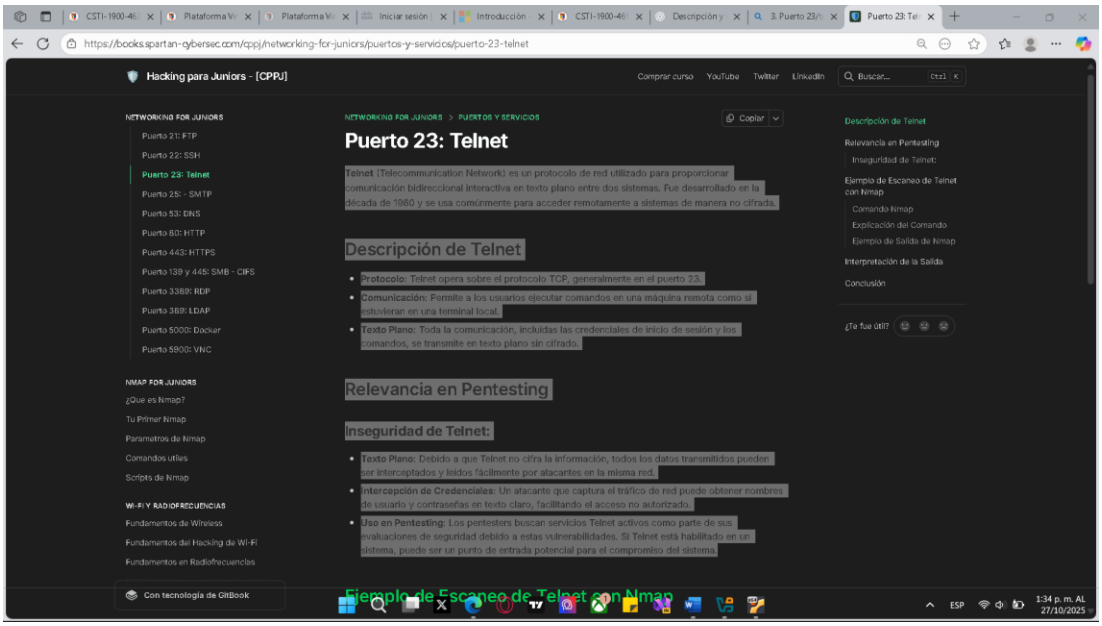
631/tcp open ipp

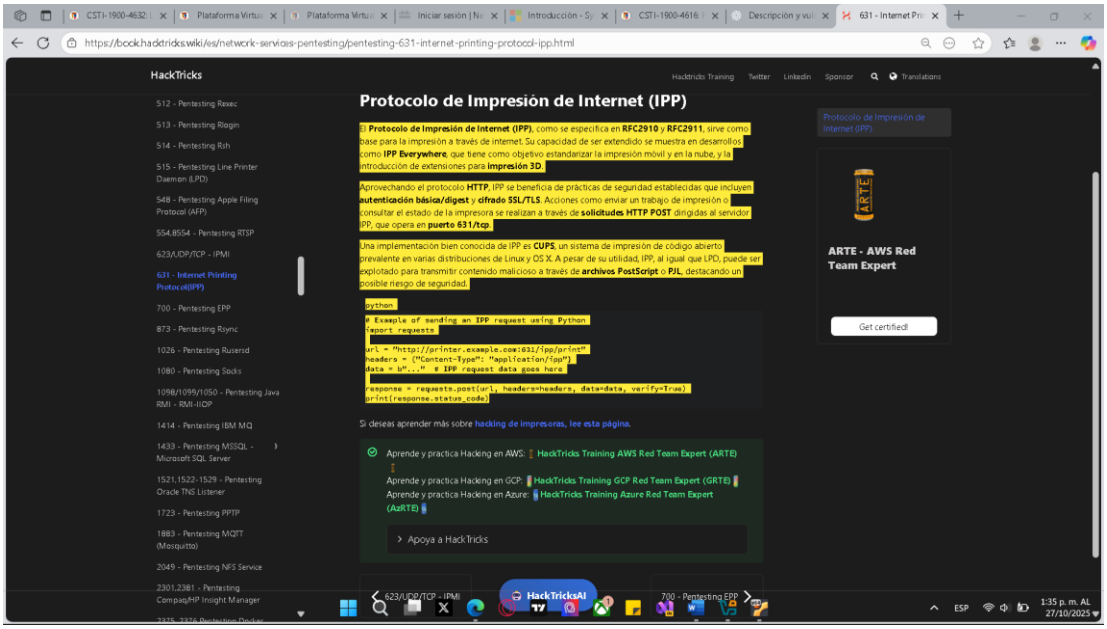
Proporcione una descripción del servicio asociado con cada puerto abierto.

Investigue las vulnerabilidades asociadas con cada uno de estos puertos abiertos.


https://books.spartan-cybersec.com/cppj/networking-for-juniors/puertos-y-servicios/puerto-21-ftp
Hacking para Juniors - [CPPJ]
Puerto 21: FTP
Descripción de FTP
Relevancia en Pentesting
Inseguridad de FTP:


https://books.spartan-cybersec.com/cppj/networking-for-juniors/puertos-y-servicios/puerto-22-ssh
Hacking para Juniors - [CPPJ]
Puerto 22: SSH
Descripción de SSH
Relevancia en Pentesting
Importancia de SSH en Pentesting:





Paso 3: Utilice los privilegios administrativos con Nmap.

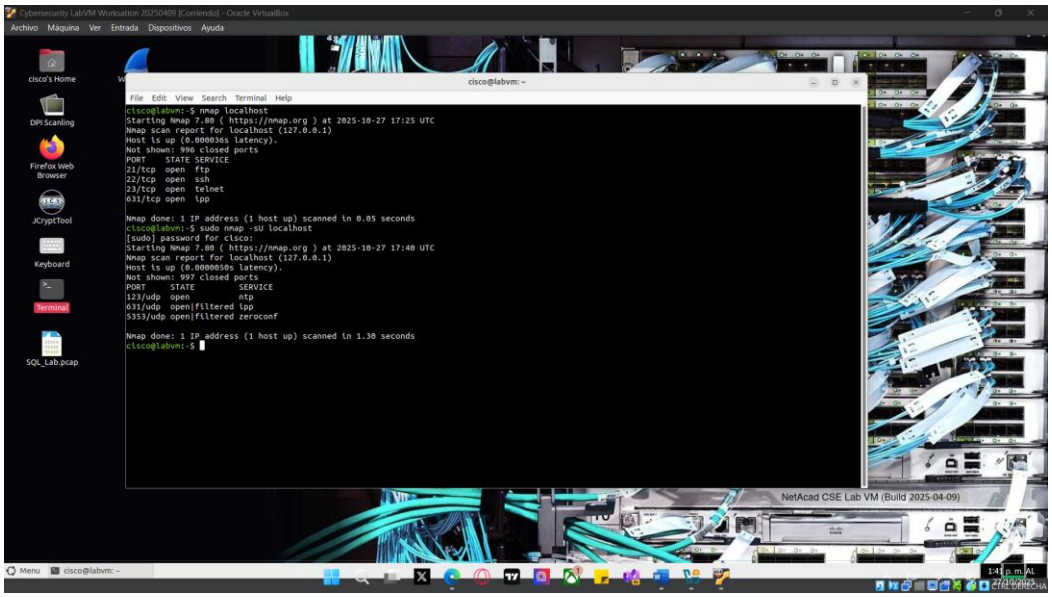
a. Escriba el siguiente comando en el terminal para analizar los puertos UDP de la computadora (recuerde, Ubuntu distingue entre mayúsculas y minúsculas) e introducir la contraseña **password** cuando se le solicite:

```
cisco@labvm:~$ sudo nmap -sU localhost
[sudo] password for cisco:
Starting Nmap 7.80 (https://nmap.org) at 2021-03-19 14:18 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
```

```
PORT STATE SERVICE
631/udp open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

¿Qué puertos UDP están abiertos?



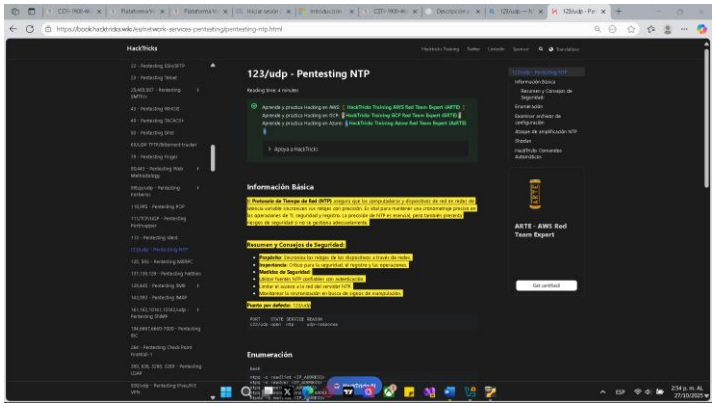
PORT STATE SERVICE

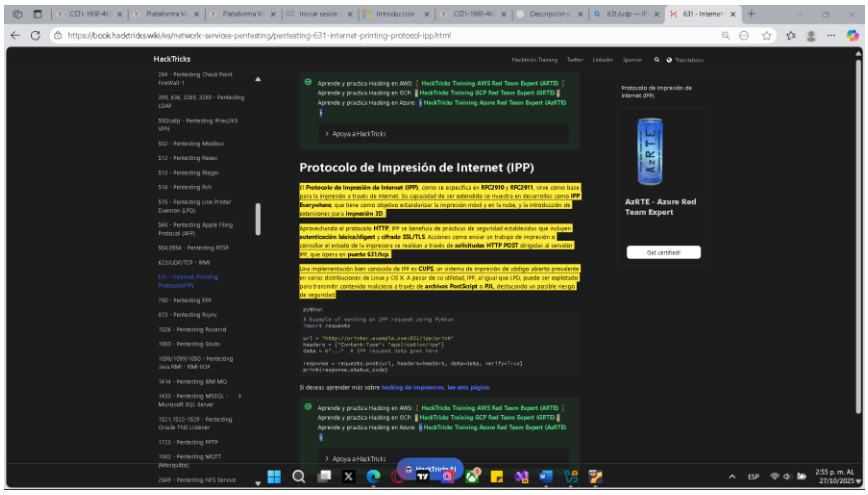
123/udp open ntp

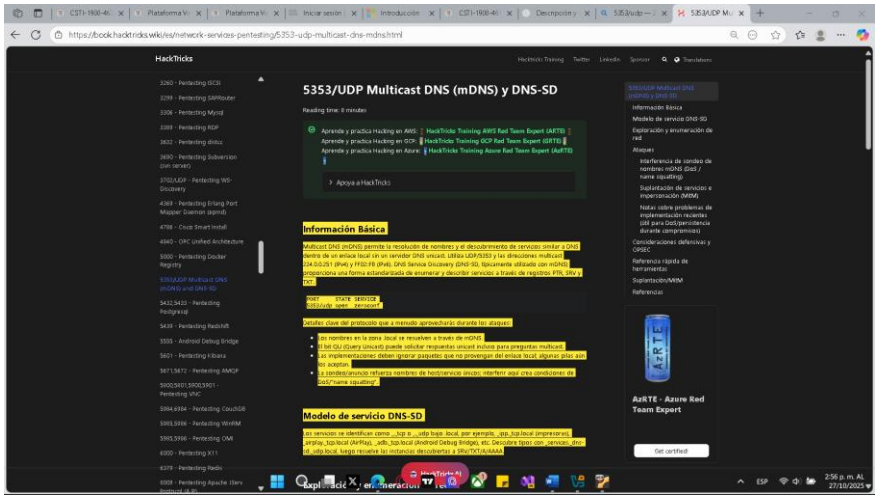
631/udp open|filtered ipp

5353/udp open|filtered zeroconf

Describa el propósito de los servicios UDP asociados con cada puerto.







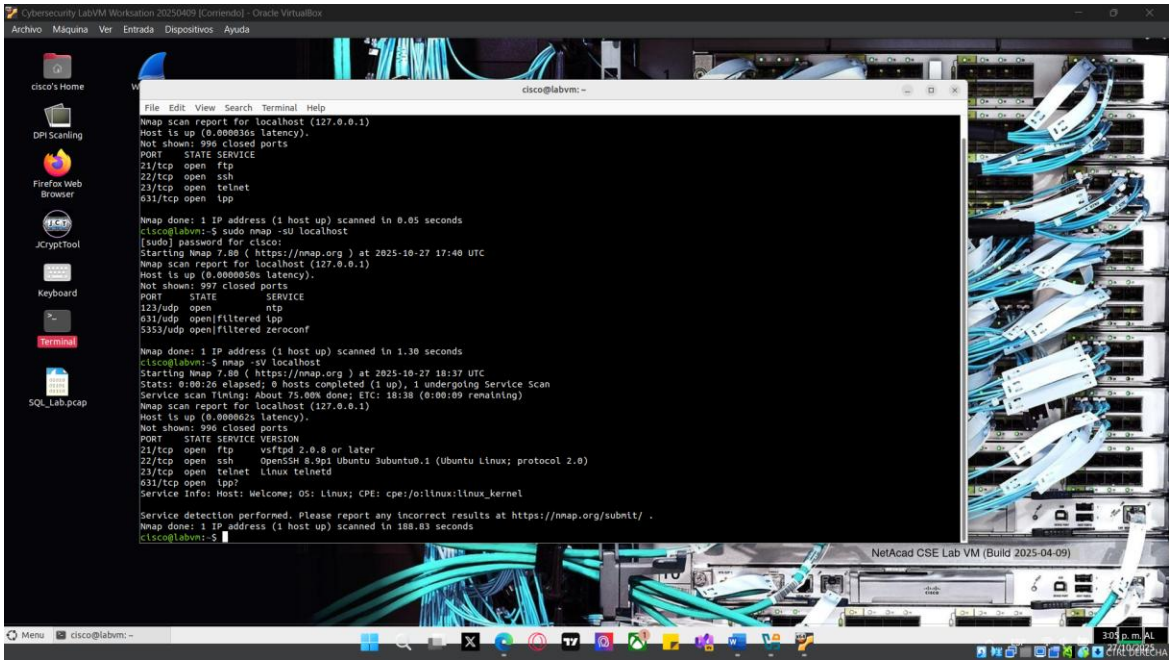
Investigue las vulnerabilidades asociadas con cada uno de estos puertos abiertos.

b. Escriba el siguiente comando en el terminal:

```
cisco@labvm:~$ nmap -sV localhost
Starting Nmap 7.80 (https://nmap.org) at 2021-03-19 14:19 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
23/tcp open telnet Linux telnetd
631/tcp open ipp CUPS 2.3
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds
```

Al usar el switch **–sV** con el comando **nmap** realiza una detección de versión que puede utilizar para investigar las vulnerabilidades.`



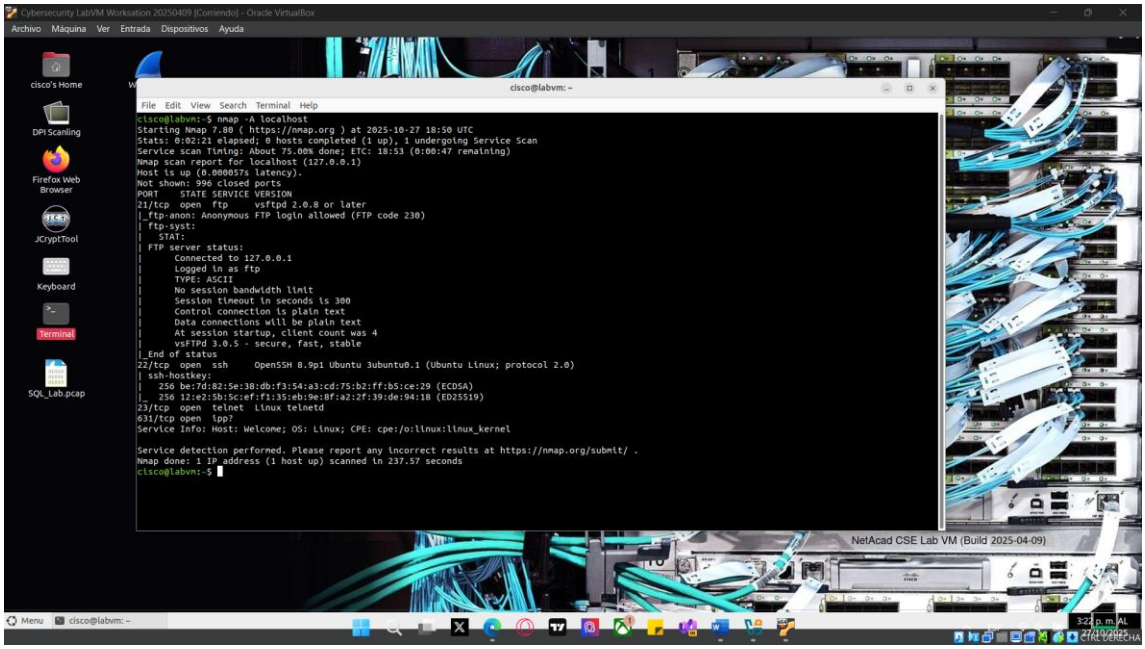
Paso 4: Capturar claves de SSH.

a. Escriba el siguiente comando en el terminal para iniciar un análisis de script:

```
cisco@labvm:~$ nmap -A localhost
Starting Nmap 7.80 (https://nmap.org) at 2021-03-19 14:21 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000037s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 56:68:77:00:41:7f:50:17:5b:73:82:36:47:c4:bc:2d (RSA)
| 256 0e:52:78:ba:08:2a:df:e5:be:1b:07:a7:98:3a:c8:50 (ECDSA)
|_ 256 f7:9e:03:10:96:94:cc:f4:4f:2a:f2:7c:6a:37:c1:6f (ED25519)
23/tcp open telnet Linux telnetd
631/tcp open ipp CUPS 2.3
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/2.3 IPP/2.1
|_http-title: Home - CUPS 2.3.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Usted capturó las claves de SSH para el sistema de host. El comando ejecuta un conjunto de scripts integrados en el comando Nmap para probar las vulnerabilidades específicas.



¿Cuáles son los valores de las claves de host SSH?

ssh-hostkey:

256 be:7d:82:5e:38:db:f3:54:a3:cd:75:b2:ff:b5:ce:29 (ECDSA)

256 12:e2:5b:5c:ef:f1:35:eb:9e:8f:a2:2f:39:de:94:18 (ED25519).

¿Cómo usaría esta información un atacante?

Usarlos para **reconocimiento** y correlación (identificar hosts clonados o la misma imagen en varios sitios).

Ayudarse en ataques **MITM** (intentar suplantar el host y luego engañar a usuarios, o validar si su suplantación pasó desapercibida).

Dirigir intentos de robo de la **clave privada** si ya tiene acceso a la red o al sistema.
(Importante: el fingerprint POR SÍ MISMO no permite iniciar sesión.)

¿Cómo podría evitar que el atacante cibernético robe la información clave?

Proteger las claves privadas: permisos root-only (chmod 600) y auditar accesos.

Regenerar/rotar claves al clonar imágenes o tras sospecha de compromiso.

Usar certificados SSH (CA) en lugar de confiar solo en fingerprints.

Limitar acceso SSH por firewall / VPN, deshabilitar autenticación por contraseña y usar claves + MFA.

Monitorear cambios en /etc/ssh/ y logs para detectar manipulaciones.

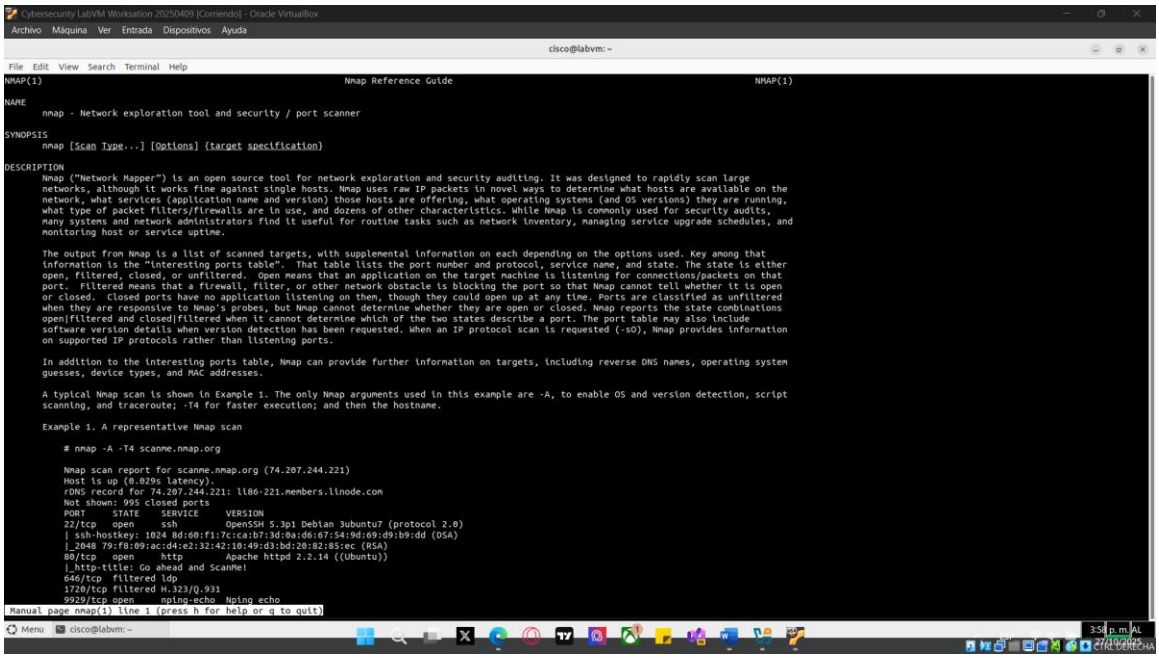
b. Ingrese el comando **man nmap** para abrir las páginas del manual de la utilidad Nmap.

```
cisco@labvm:~$ man nmap
NMAP(1) Nmap Reference Guide NMAP(1)
```



```
NAME
nmap - Network exploration tool and security / port scanner

SYNOPSIS
nmap [Scan Type...] [Options] {target specification}
<output omitted>
```



Puede utilizar este recurso para buscar otras opciones disponibles para la utilidad Nmap. En cualquier momento, ingrese **q** o **quit** para salir de las páginas del manual. Puede leer las páginas del manual disponibles para cualquier servicio o comando ingresando el comando **man** seguido del nombre de la utilidad o comando.

Resumen

Puertos altamente vulnerables

Muchos puertos deben estar abiertos para que un host funcione en un entorno de computación y comunicación normal. Sin embargo, estos puertos comunes deben monitorearse periódicamente para garantizar que no se vean comprometidos y se utilicen para atacar a una víctima, proporcionar acceso remoto no autorizado o para secuestrar un host para participar en un ataque distribuido a otras víctimas.

El puerto 21 de TCP es uno de los puertos más populares para los atacantes. Este puerto está diseñado para transmitir y recibir archivos de un host a otro. Los atacantes usan este puerto para realizar los siguientes tipos de actividad maliciosa:

- Transferencia, eliminación y modificación no autorizadas de archivos
- Transferencia no autorizada de código malicioso o cargas útiles
- Autenticación anónima para alojar sistemas de archivos
- Inyectar scripts maliciosos como ataque XSS
- Impacto en la disponibilidad de otros servicios de host

Otro objetivo común es el puerto 23 (Telnet). Este puerto proporciona acceso remoto autorizado a un host IP. Este puerto representa una vulnerabilidad porque los datos transferidos están en texto sin formato. Los atacantes usan este puerto para realizar los siguientes tipos de actividad maliciosa:

- Obtener acceso remoto no autorizado a un host
- Puertas traseras de la planta y otros tipos de código malicioso
- Ver datos confidenciales y credenciales
- Realizar ataques man-in-the-middle.
- Impactar en la disponibilidad de otros servicios de host

Otro puerto favorito para los atacantes es el puerto 53. Este puerto se utiliza para DNS o para buscar nombres de dominio al navegar por Internet o transferir información. Este puerto es la ruta de salida más común para el atacante después de un ataque. Debido a que este puerto rara vez se monitorea, los atacantes usan este puerto para salir después de borrar sus archivos, registros y otra información para cubrir sus huellas.

El puerto más común utilizado por los atacantes es el puerto TCP 80. Este puerto transfiere páginas web entre un servidor web y el navegador de host. Los atacantes usan este puerto para realizar los siguientes tipos de actividad maliciosa:

- Transferencia, eliminación y modificación no autorizadas de datos.
- Transferencia no autorizada de código malicioso o cargas útiles
- Inyección de scripts maliciosos (como un ataque XSS)
- Impactar en la disponibilidad de otros servicios de host

