

Práctica de laboratorio: detección de amenazas y vulnerabilidades

Objetivos

Utilice Nmap, un escáner de puertos y una herramienta de asignación de red para detectar amenazas y vulnerabilidades en un sistema.

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. 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.

Recursos necesarios

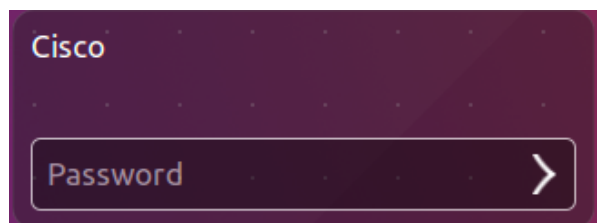
- Computadora con sistema Ubuntu 16.0.4 LTS instalado en una estación de trabajo VMware.

Paso 1: Abra una ventana del terminal en Ubuntu.

- Inicie sesión en Ubuntu con las siguientes credenciales:

Usuario: **cisco**

Contraseña: **password**



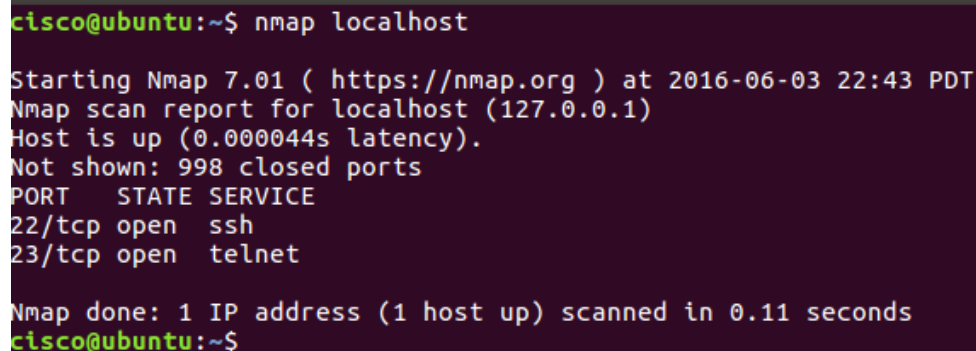
- Haga clic en el icono de **terminal** para abrir una terminal.



Paso 2: Ejecute Nmap.

En la petición de ingreso de comandos, introduzca el siguiente comando para ejecutar un análisis básico de este sistema Ubuntu:

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



```
cisco@ubuntu:~$ nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:43 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
cisco@ubuntu:~$
```

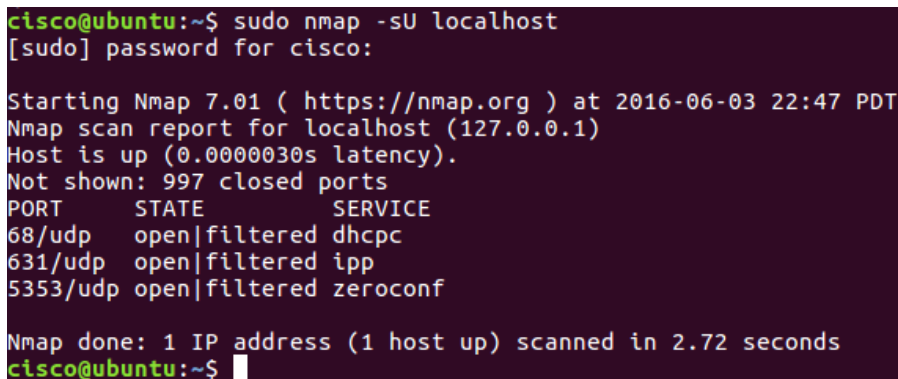
Los resultados son el escaneo de los primeros puertos 1024 TCP.

¿Qué puertos TCP están abiertos?

Paso 3: Utilice los privilegios administrativos con Nmap.

- 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@ubuntu:~$ sudo nmap -sU localhost
```



```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
631/udp    open|filtered ipp
5353/udp   open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

¿Qué puertos UDP están abiertos?

- b. Escriba el siguiente comando en el terminal:

```
cisco@ubuntu:~$ nmap -sV localhost
```

```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
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 0.97 seconds
cisco@ubuntu:~$
```

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.

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

```
cisco@ubuntu:~$ nmap -A localhost
```

```
cisco@ubuntu:~$ nmap -A localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:56 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 83:35:a7:81:c7:04:47:d4:6b:b4:87:b3:e3:5b:c7:ab (RSA)
|_  256 78:97:1f:92:cf:38:63:90:c3:7f:d5:ff:85:43:e6:2f (ECDSA)
23/tcp    open  telnet   Linux telnetd
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 1.16 seconds
cisco@ubuntu:~$
```

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.

Referencias

Nmap: <https://nmap.org/>