

## Laboratório — Detecção de Ameaças e Vulnerabilidades Objetivos

Utilizar o Nmap, um scanner de portas e ferramenta de mapeamento de rede, utilizado para detetar ameaças e vulnerabilidades num sistema.

### Contextualização/cenário

O Network Mapper, ou Nmap, é um utilitário de código aberto usado para deteção de rede e auditoria de segurança. Os administradores também usam o Nmap para monitorizar os computadores anfitrião ou gerir os agendamentos de atualizações de serviço. O Nmap determina quais os anfitriões que estão disponíveis numa rede, quais os serviços que estão a ser executados, quais os sistemas operativos que estão a ser executados e quais os filtros de pacotes ou firewalls que estão a ser executados.

### Recursos Necessários

- Um PC com Ubuntu 16.0.4 LTS instalado numa máquina virtual - pode usar a VM dos laboratórios concluídos no capítulo 2.

### Passo 1. Abrir uma janela de terminal no Ubuntu.

- Inicie uma sessão no Ubuntu usando as seguintes credenciais:

User: **cisco**

Password: **password**



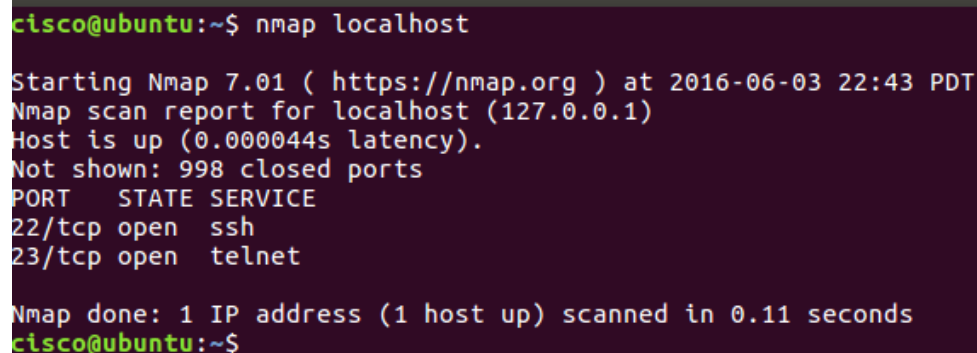
- Clique no ícone **terminal** para abrir uma janela de terminal.



## Passo 2. Executar o Nmap.

No prompt de comandos, introduza o seguinte comando para executar uma varredura básica (scan) deste 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:~$
```

Os resultados são uma varredura (scan) das primeiras 1024 portas TCP.

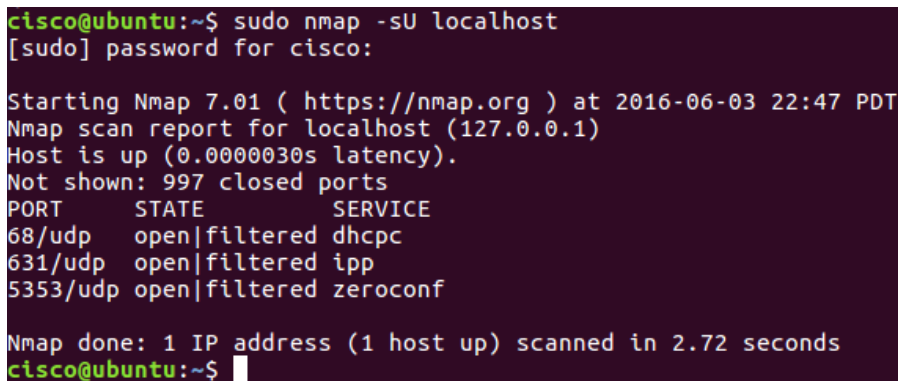
Quais as portas TCP que estão abertas?

---

## Passo 3. Utilizar os privilégios de administrador com o Nmap.

- Introduza o seguinte comando no terminal para verificar as portas UDP do computador (lembre-se que o Ubuntu faz a distinção entre maiúsculas e minúsculas) e insira a **palavra-passe** quando for pedida:

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



```
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:~$
```

Quais as portas UDP que estão abertas?

---

- b. Introduza o seguinte comando no 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:~$
```

A utilização da opção **—sV** no comando **nmap** serve para realizar a detecção da versão que pode usar para procurar vulnerabilidades.

### Passo 4. Capturar as chaves SSH.

- Introduza o seguinte comando no terminal para iniciar um script de scan:

```
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:~$
```

Capturou as chaves SSH para o sistema anfitrião. O comando executa um conjunto de scripts incorporados no Nmap para testar vulnerabilidades específicas.

### SKUs

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