

Laboratório – Detecção de ameaças e vulnerabilidades

Objetivos

Use Nmap, um scanner de porta e ferramenta de mapeamento de rede, para detectar ameaças e vulnerabilidades em um sistema.

Histórico/Cenário

O Network Mapper, ou Nmap, é um utilitário de código aberto usado para descoberta de rede e auditoria de segurança. Os administradores também usam o Nmap para monitorar hosts ou gerenciar agendamentos de atualizações de serviços. O Nmap determina quais hosts estão disponíveis em uma rede, quais serviços, sistemas operacionais e filtros de pacotes ou firewalls estão sendo executados.

Recursos necessários

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

Passo 1: Abra uma janela de terminal no Ubuntu.

- Inicie uma sessão no Ubuntu usando as seguintes credenciais:

Usuário: **cisco**

Senha: **password**



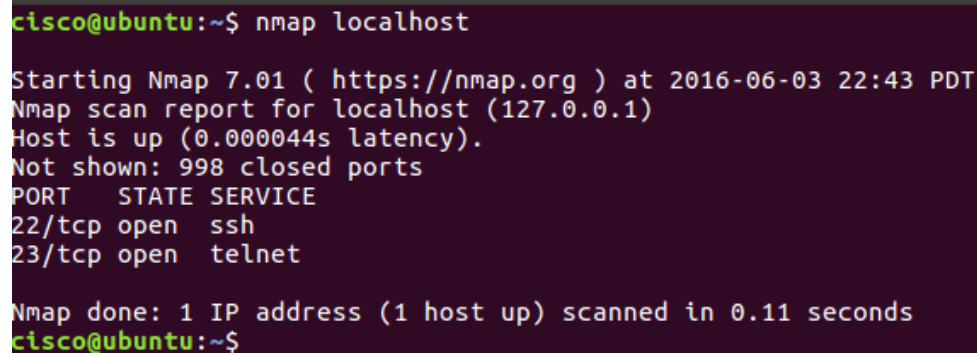
- Clique no ícone de **terminal** para abrir um terminal.



Passo 2: Execute o Nmap.

No prompt de comando, digite o seguinte comando para executar uma varredura básica nesse 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:~$
```

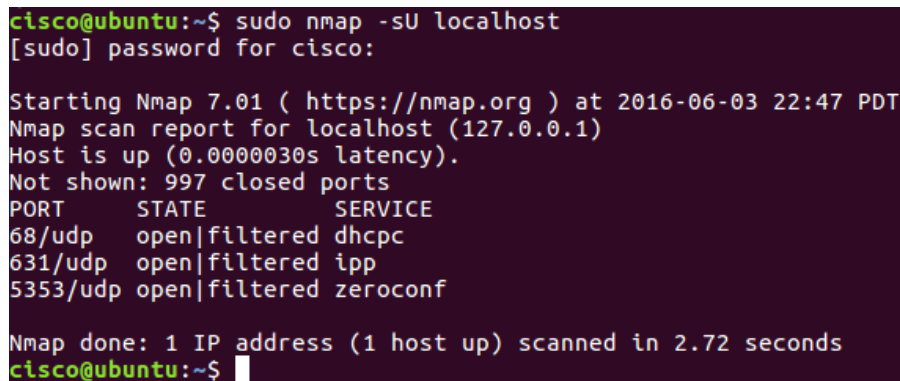
Os resultados são uma varredura das primeiras 1024 portas TCP.

Quais portas TCP estão abertas?

Passo 3: Use privilégios administrativos com Nmap.

- Digite o seguinte comando no terminal para varrer as portas UDP do computador (lembre-se o Ubuntu faz distinção entre maiúsculas e minúsculas) e insira a senha **password** quando solicitado:

```
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:~$
```

Quais portas UDP estão abertas?

- b. Digite 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:~$
```

Usar a opção **-sV** com o comando **nmap** executa uma detecção de versão que pode ser usada para pesquisar vulnerabilidades.

Passo 4: Capturar chaves SSH.

- Digite o seguinte comando no terminal para iniciar uma varredura 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:~$
```

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

Referências

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