Laboratório - Explorando o Nmap

# Topologia



# Objetivos

Parte 1: Explorando Nmap

Parte 2: Verificação de Portas Abertas

# Histórico/Cenário

A varredura de portas geralmente faz parte de um ataque de reconhecimento. Há uma variedade de métodos de varredura de portas que podem ser usados. Vamos explorar como usar o utilitário Nmap. Nmap é um utilitário de rede poderoso usado para descoberta de rede e auditoria de segurança.

# Recursos necessários

* Máquina virtual CyberOps Workstation
* Acesso à Internet

# Instruções

## Explorando Nmap

Nesta parte, você usará páginas de manual (ou páginas de man para abreviar) para saber mais sobre o Nmap.

O comando **man** [ *programa |utilitário | função*] exibe as páginas de manual associadas aos argumentos. As páginas de manual são os manuais de referência encontrados em sistemas operacionais Unix e Linux. Essas páginas podem incluir estas seções: Nome, Sinopse, Descrições, Exemplos e Consulte Também.

* + - 1. Inicie o CyberOps Workstation VM.
      2. Abra um terminal.
      3. No prompt do terminal, digite **man nmap**.

[analyst@secOps ~]$ **man nmap**

#### Perguntas:

O que é Nmap?

Digite suas respostas aqui.

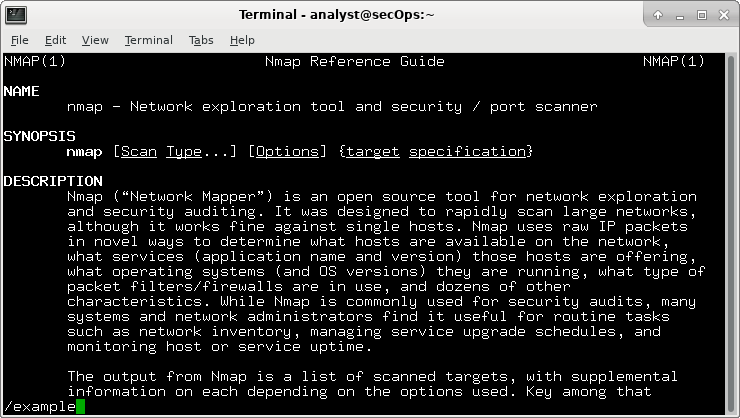
Para que é utilizado o nmap?

Digite suas respostas aqui.

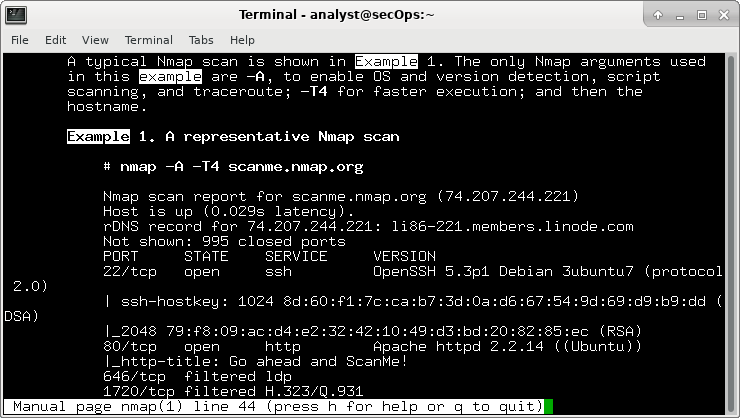
* + - 1. Enquanto estiver na página do manual, você pode usar as teclas de seta para cima e para baixo para percorrer as páginas. Você também pode pressionar a barra de espaço para encaminhar uma página de cada vez.

Para procurar um termo ou frase específico, use uma barra (/) ou um ponto de interrogação (?) seguido pelo termo ou frase. A barra pesquisa para a frente no documento e o ponto de interrogação pesquisa para trás no documento. A chave **n** se move para a próxima correspondência.

Digite **/exemplo** e pressione ENTER Isso pesquisará a palavra **exemplo** adiante na página do manual.



* + - 1. Na primeira instância do exemplo, você vê três correspondências. Para ir para a próxima correspondência, pressione **n.**



Olhe para o Exemplo 1.

#### Pergunta:

Qual é o comando **nmap** usado?

Digite suas respostas aqui.

Use a função de pesquisa para responder às seguintes perguntas.

#### Perguntas:

O que o opção -A faz?

Digite suas respostas aqui.

O que o opção -T4 faz?

Digite suas respostas aqui.

* + - 1. Percorra a página para saber mais sobre o nmap. Digite **q** quando terminar.

## Varrendo em busca de portas abertas

Nesta parte, você usará as opções do exemplo nas páginas do manual Nmap para digitalizar seu localhost, sua rede local e um servidor remoto em scanme.nmap.org.

### Analise o seu host local.

* + - 1. Se necessário, abra um terminal na VM. No prompt, digite **nmap -A -T4 localhost**. Dependendo da rede local e dos dispositivos, a verificação levará de alguns segundos a alguns minutos.

[analyst@secOps ~] $ **nmap -A -T4 localhost**

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:20 EDT

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000056s latency).

Other addresses for localhost (not scanned): ::1

rDNS record for 127.0.0.1: localhost.localdomain

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

| ftp-anon: Login FTP anônimo permitido (código FTP 230)

|\_-rw-r—r— 1 0 0 0 abr 19 15:23 ftp\_test

<some output omitted>

* + - 1. Reveja os resultados e responda às seguintes perguntas.

#### Perguntas:

Quais portas e serviços são abertos?

Digite suas respostas aqui.

Para cada uma das portas abertas, registre o software que está fornecendo os serviços./t

Digite suas respostas aqui.

### Analise a sua rede.

**Aviso: Antes de usar o Nmap em qualquer rede, obtenha a permissão dos proprietários da rede antes de prosseguir.**

* + - 1. No prompt de comando do terminal, digite **ip address** para determinar o endereço IP e a máscara de sub-rede para esse host. Para este exemplo, o endereço IP para esta VM é 10.0.2.15 e a máscara de sub-rede é 255.255.255.0.

[analyst@secOps ~]$ **ip address**

<output omitted>

2: enp0s3: <BROADCAST, MULTICAST, UP, LOWER\_UP> mtu 1500 qdisc fq\_codel estado UP grupo padrão qlen 1000

link/éter 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff:ff

inet 10.0.2.15/24 brd 10.0.2.255 escopo dinâmico global enp0s3

valid\_lft 85777seg preferred\_lft 85777seg

inet6 fe80። um 00:27 ff:feed:af2c/64 link escopo

valid\_lft forever preferred\_lft forever

Registre o endereço IP e a máscara de sub-rede para sua VM.

#### Pergunta:

A qual rede sua VM pertence?

Digite suas respostas aqui.

* + - 1. Para localizar outros hosts nesta LAN, digite **nmap -A -T4 *endereço/prefixo de rede***. O último octeto do endereço IP deve ser substituído por um zero. Por exemplo, no endereço IP 10.0.2.15, o.15 é o último octeto. Portanto, o endereço de rede é 10.0.2.0. O /24 é chamado de prefixo e é uma abreviação para a máscara de rede 255.255.255.0. Se sua VM tiver uma máscara de rede diferente, pesquise na Internet uma “tabela de conversão CIDR” para localizar seu prefixo. Por exemplo, 255.255.0.0 seria /16. O endereço de rede 10.0.2.0/24 é usado neste exemplo

**Observação**: essa operação pode levar algum tempo, especialmente se você tiver muitos dispositivos conectados à rede. Em um ambiente de teste, a varredura demorou cerca de 4 minutos.

[analyst@secOps ~] $ **nmap -A -T4 10.0.2.0/24**

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:13 EDT

<output omitted>

Relatório de varredura Nmap para 10.0.2.15

Host is up (0.00019s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

| ftp-anon: Login FTP anônimo permitido (código FTP 230)

|\_-rw-r—r— 1 0 0 0 Mar 26 2018 ftp\_test

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 10.0.2.15

| 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 1

| vsFTPd 3.0.3 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 8.2 (protocol 2.0)

23/tcp open telnet Openwall GNU/\*/Linux telnetd

Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Post-scan script results:

| clock-skew:

| 0s:

| 10.0.2.4

| 10.0.2.3

|\_ 10.0.2.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 346.89 seconds

#### Perguntas:

Quantos hosts estão ativos?

Digite suas respostas aqui.

Nos resultados do Nmap, liste os endereços IP dos hosts que estão na mesma LAN da VM. Liste alguns dos serviços que estão disponíveis nos hosts detectados.

Digite suas respostas aqui.

### Faça a varredura em um servidor remoto.

* + - 1. Abra um navegador da Web e navegue até **scanme.nma.org**. Por favor, leia a mensagem postada.

#### Pergunta:

Qual é o propósito deste site?

Digite suas respostas aqui.

* + - 1. No prompt do terminal, digite **nmap -A -T4 scanme.nmap.org**.

[analyst@secOps Desktop] $ **nmap -A -T4 scanme.nmap.org**

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:46 EDT

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.040s latency).

Outros endereços para scanme.nmap.org (não digitalizados): 2600:3 c01። f03c:91ff:fe18:bb2f

Not shown: 992 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)

| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)

|\_ 256 96:02:bb:5e: 57:54:1 c:4e: 45:2 f: 56:4 c:4a:24:b 2:57 (ECDSA)

25/tcp filtered smtp

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

|\_http-server-header: Apache/2.4.7 (Ubuntu)

|\_http-title: Vá em frente e ScanMe!

135/tcp filtered msrpc

139/tcp netbios-ssn filtrado

445/tcp filtered microsoft-ds

593/tcp filtered http-rpc-epmap

4444/tcp filtered krb524

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

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 23.96 seconds

* + - 1. Reveja os resultados e responda às seguintes perguntas.

#### Perguntas:

Quais portas e serviços são abertos?

Digite suas respostas aqui.

Quais portas e serviços são filtrados?

Digite suas respostas aqui.

Qual é o endereço IP do servidor?

Digite suas respostas aqui.

O que é o sistema operacional?

Digite suas respostas aqui.

# Perguntas para reflexão

Nmap é uma ferramenta poderosa para exploração e gerenciamento de redes. Como o Nmap pode ajudar com a segurança da rede? Como o Nmap pode ser usado por um ator ameaçador como uma ferramenta nefasta?

Digite suas respostas aqui.

Fim do documento