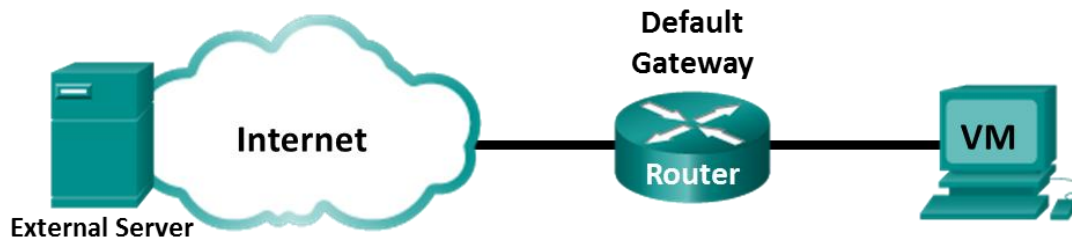


## Laboratório – Explorando Nmap

### Topologia



### Objectivos

Parte 1: Explorando Nmap

Parte 2: Verificação de portas abertas

### Plano de fundo / Cenário

Varredura de porta é geralmente parte de um ataque de reconhecimento. Há uma variedade de métodos que podem ser usados de varredura de portas. Nós exploraremos como usar o utilitário do Nmap. Nmap é um utilitário de rede poderosa que é usado para a descoberta de rede e auditoria de segurança.

### Recursos necessários

- Máquina Virtual de CyberOps Workstation
- Acesso à Internet

### Parte 1: Explorando o Nmap

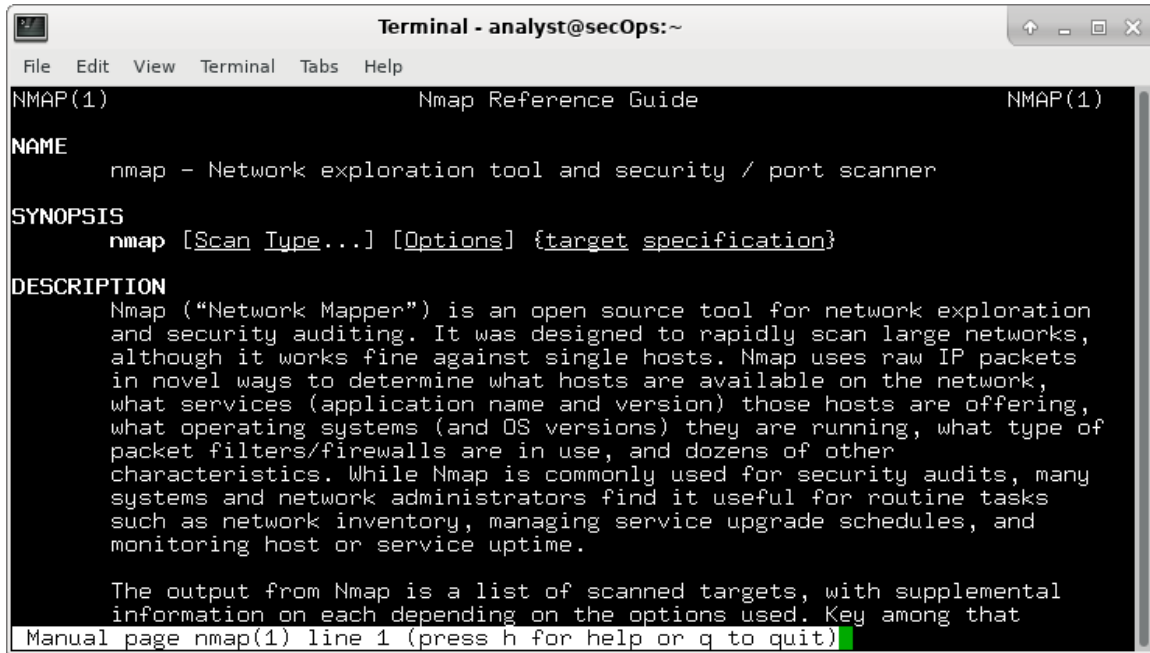
Nesta parte, você usará páginas de manual (ou páginas de manual para o short) para saber mais sobre o Nmap.

The **man** [ *program* | *utility* | *function* ] esse comando exibe as páginas de manual associadas com os argumentos. As páginas de manual são os manuais de referência encontrados em Sistemas operacionais Unix e Linux. Estas páginas podem incluir as seções: nome, Sinopse, descrições, exemplos e consulte também.

## Lab - Exploring Nmap

- Começar CyberOps Workstation VM.
- Abra um terminal.
- No prompt do terminal, digite **man nmap**.

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



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The terminal displays the man page for nmap. The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content is as follows:

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks
    such as network inventory, managing service upgrade schedules, and
    monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    Manual page nmap(1) line 1 (press h for help or q to quit)
```

O que é o Nmap?

---

---

---

O nmap é usado para?

---

---

---

---

- Enquanto na página man, você pode usar as teclas up and down e as de seta para percorrer as páginas. Você também pode pressionar a barra de espaço para encaminhar uma página por vez.

Para pesquisar um termo específico ou frase use inserir uma barra (/) ou ponto de interrogação (?) seguido do termo ou frase. A barra procura para a frente através do documento e o ponto de interrogação pesquisas para trás através do documento. A chave **n** se move para o próximo item a ser pesquisado.

Digite **/example** e pressione ENTER. Isto irá procurar a palavra **example** para a frente através da página do man.

```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks
    such as network inventory, managing service upgrade schedules, and
    monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    /example
  
```

e. Em primeira instância de exemplo, você vê três seleção. Para mover para o próximo, pressione **n**.

```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open  http     Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered ldap
1720/tcp  filtered H.323/Q.931

Manual page nmap(1) line 44 (press h for help or q to quit)
  
```

Veja o exemplo 1. Qual é o comando **nmap** usado?

Use a função de pesquisa para responder às seguintes perguntas.

O que faz o parâmetro-A?

---

O que faz o parâmetro -T4?

---

---

f. Rolar através da página para saber mais sobre o nmap. Digite **q** quando terminou.

## Parte 2: Varredura de portas abertas

Nesta parte, você usará os interruptores do exemplo as páginas de man do Nmap para digitalizar seu localhost, sua rede local e um servidor remoto em [scanme.nmap.org](https://scanme.nmap.org).

### Passo 1: Varrendo seu localhost.

- a. Se necessário, abra um terminal na VM. No prompt, digite **nmap -A -T4 localhost**. Dependendo da sua rede local e dispositivos, o scan vai demorar em qualquer lugar de alguns segundos a alguns minutos.

```
[analyst@secOps Desktop] $ 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: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--    1 0          0          0 Apr 19 15:23 ftp_test
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)
|_  256 94:33:25:a5:0e:02:d7:bc:c8:b0:90:8a:a2:16:59:e5 (ECDSA)
23/tcp    open  telnet   Openwall GNU/*/Linux telnetd
80/tcp    open  http     nginx 1.12.0
|_ http-server-header: nginx/1.12.0
|_ http-title: Welcome to nginx!
Service Info: Host: Welcome; 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 18.81 seconds
```

- b. Vamos rever os resultados e responder às seguintes perguntas.

Quais portas e serviços são abertos?

---

Para cada uma das portas abertas, grave o software que está fornecendo os serviços.

---

O que é o sistema operacional?

---

### Passo 2: Varrendo sua rede.

**Aviso:** Antes de usar o Nmap em qualquer rede, por favor, obter a permissão dos proprietários de rede antes de prosseguir.

- a. No prompt de comando do terminal, digite **ifconfig** para determinar a IP endereço e máscara de sub-rede para esse host. Para este exemplo, o endereço IP para essa VM é 192.168.1.19 e a máscara de sub-rede é 255.255.255.0.

```
[analyst@secOps ~] $ ifconfig

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.19 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::997f:9b16:5aae:1868 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:c9:fa:a1 txqueuelen 1000 (Ethernet)
    RX packets 34769 bytes 5025067 (4.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10291 bytes 843604 (823.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0xd000
```

Grave a IP endereço e máscara de sub-rede para sua VM. Qual rede pertence o seu VM?

---

---

---

- b. Para localizar outros hosts esta LAN, digite **nmap -A -T4 network address/prefix**. O último octeto do endereço IP deve ser substituído com um zero. Por exemplo, o endereço IP 192.168.1.19, o.19 é o último octeto. Portanto, o endereço de rede é 192.168.1.0. O 24 é chamado o prefixo e é uma forma abreviada para a máscara de rede 255.255.255.0. Se sua VM tem uma máscara de rede diferente, procurar na Internet uma "tabela de conversão de CIDR" para encontrar seu prefixo. Por exemplo, 255.255.0.0 seria 16. A rede endereço 192.168.1.0/24 é usado neste exemplo

**Nota :** Esta operação pode levar algum tempo, especialmente se você tiver muitos dispositivos conectados à rede. No ambiente de teste, a digitalização levou cerca de 4 minutos.

```
[analyst@secOps ~] $ nmap -A -T4 192.168.1.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0097s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE  VERSION
```

## Lab - Exploring Nmap

---

```
21/tcp open  ftp      Bftpd 1.6.6
53/tcp open  domain    dnsmasq 2.15-OpenDNS-1
| dns-nsid:
| id.server:
|_ bind.version: dnsmasq-2.15-OpenDNS-1
80/tcp open  tcpwrapped
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_ Basic realm=NETGEAR WNR3500Lv2
|_http-title: 401 Unauthorized
5000/tcp open  tcpwrapped
Service Info: Host: 192.168.1.1
```

```
Nmap scan report for 192.168.1.19
Host is up (0.00016s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
21/tcp open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--    1 0          0          0 Apr 19 15:23 ftp_test
22/tcp open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)
|_  256 94:33:25:a5:0e:02:d7:bc:c8:b0:90:8a:a2:16:59:e5 (ECDSA)
23/tcp open  telnet   Openwall GNU/*/Linux telnetd
80/tcp open  http     nginx 1.12.0
|_http-server-header: nginx/1.12.0
|_http-title: Welcome to nginx!
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel
<some output omitted>
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 256 IP addresses (5 hosts up) scanned in 34.21 seconds

Quantos hosts são acima?

---

---

De seus resultados do Nmap, liste os endereços IP dos hosts que estão na mesma LAN como sua VM. Lista de alguns dos serviços que estão disponíveis nos hosts detectados.

---

---

---

### Passo 3: Scan de um servidor remoto.

r. Abra um navegador da web e navegue até **scanme.nmap.org**. Por favor, leia a mensagem postada. Qual é a finalidade deste site?

---

## Lab - Exploring Nmap

b. 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).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::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:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (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: Go ahead and ScanMe!
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
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
```

c. Revise os resultados e responda às perguntas a seguir.

Quais portas e serviços estão abertos?

---

Quais portas e serviços são filtrados?

---

Qual é o endereço IP do servidor?

---

Qual é o sistema operacional?

---

## Reflexão

O Nmap é uma ferramenta poderosa para exploração e gerenciamento de redes. Como o Nmap pode ajudar na segurança da rede? Como o Nmap pode ser usado por um agente de ameaça como uma ferramenta nefasta?

---

---

---

---