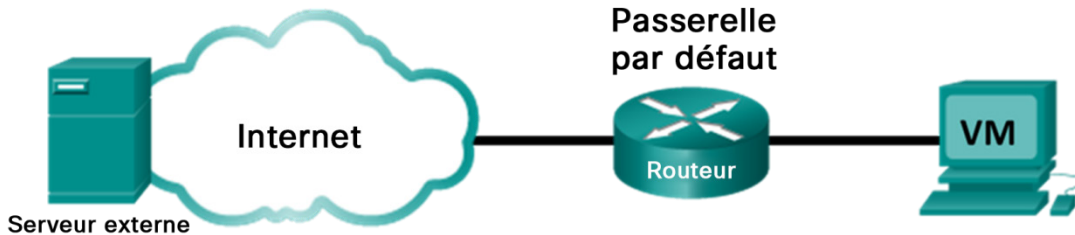


Travaux pratiques – Découvrir Nmap

Topologie



Objectifs

Partie 1 : Découvrir Nmap

Partie 2 : Rechercher des ports ouverts

Contexte/scénario

L'analyse des ports fait généralement partie d'une attaque de reconnaissance. Diverses méthodes d'analyse des ports peuvent être utilisées. Nous allons étudier comment se servir de l'utilitaire de Nmap. Nmap est un utilitaire réseau puissant qui est utilisé pour la découverte du réseau et pour l'audit de sécurité.

Ressources requises

- Poste de travail virtuel CyberOps
- Accès Internet

Partie 1 : Découvrir Nmap

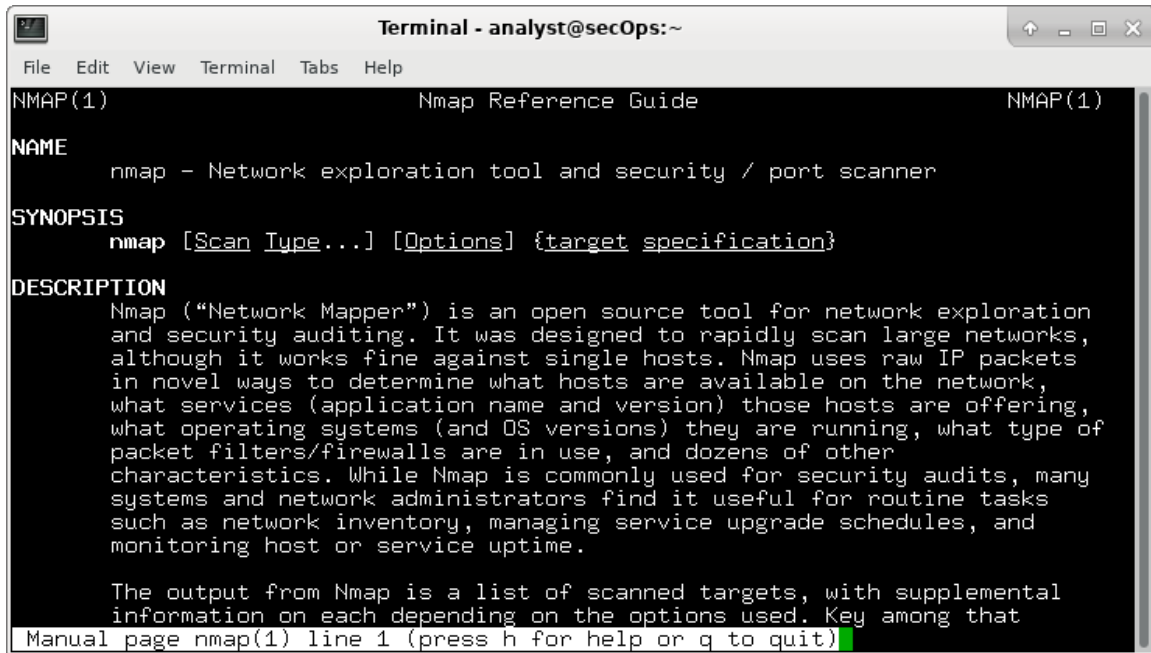
Dans cette partie, vous allez utiliser les pages de manuel pour en savoir plus sur Nmap.

La commande **man** [*program* | *utility* | *function*] affiche les pages de manuel associées aux arguments. Les pages de manuel correspondent aux manuels de référence trouvés sur les systèmes d'exploitation Unix et Linux. Ces pages incluent ces sections : Nom, Synopsis, Descriptions, Exemples et Voir aussi.

- a. Lancez le poste de travail virtuel CyberOps.
- b. Ouvrez un terminal.

- c. À l'invite du terminal, saisissez `man nmap`.

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



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

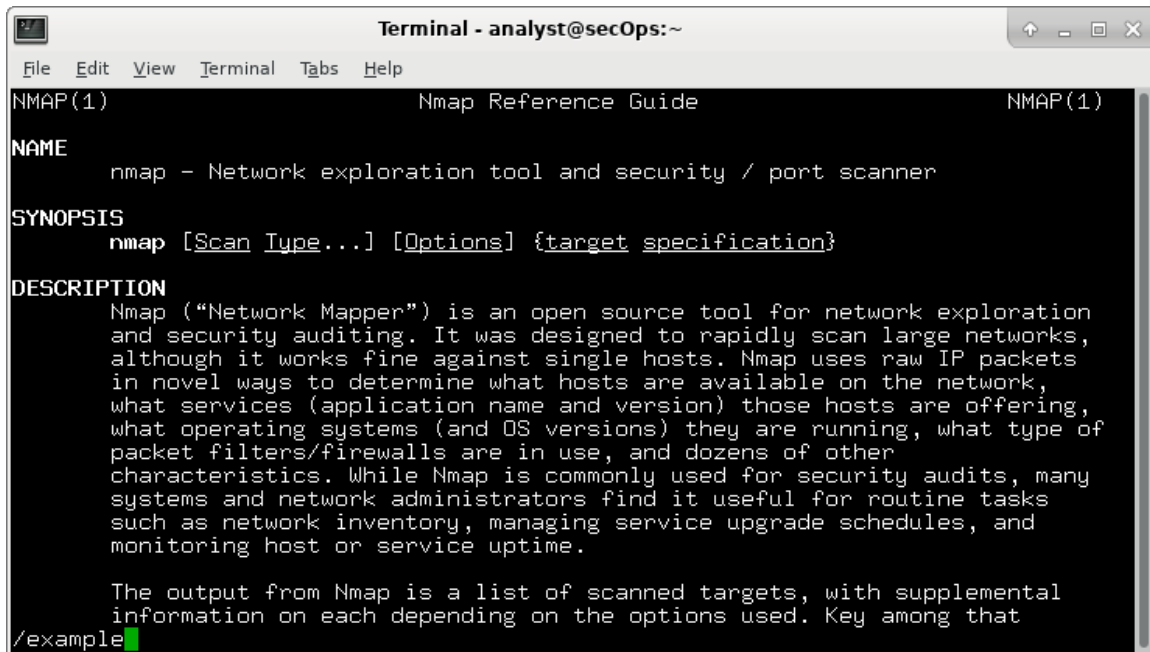
Qu'est-ce que Nmap ?

À quoi Nmap sert-il ?

- d. Lorsque vous êtes sur la page du manuel, vous pouvez utiliser les touches fléchées haut/bas pour faire défiler les pages. Vous pouvez également appuyer sur la barre d'espace pour avancer d'une page à la fois.

Pour rechercher un terme ou une expression spécifique, saisissez une barre oblique (/) ou un point d'interrogation (?) suivi de ce terme ou de cette expression. La barre oblique permet d'effectuer une recherche vers l'avant dans tout le document, tandis que le point d'interrogation effectue une recherche en arrière dans le document. La touche `n` permet d'accéder à la correspondance suivante.

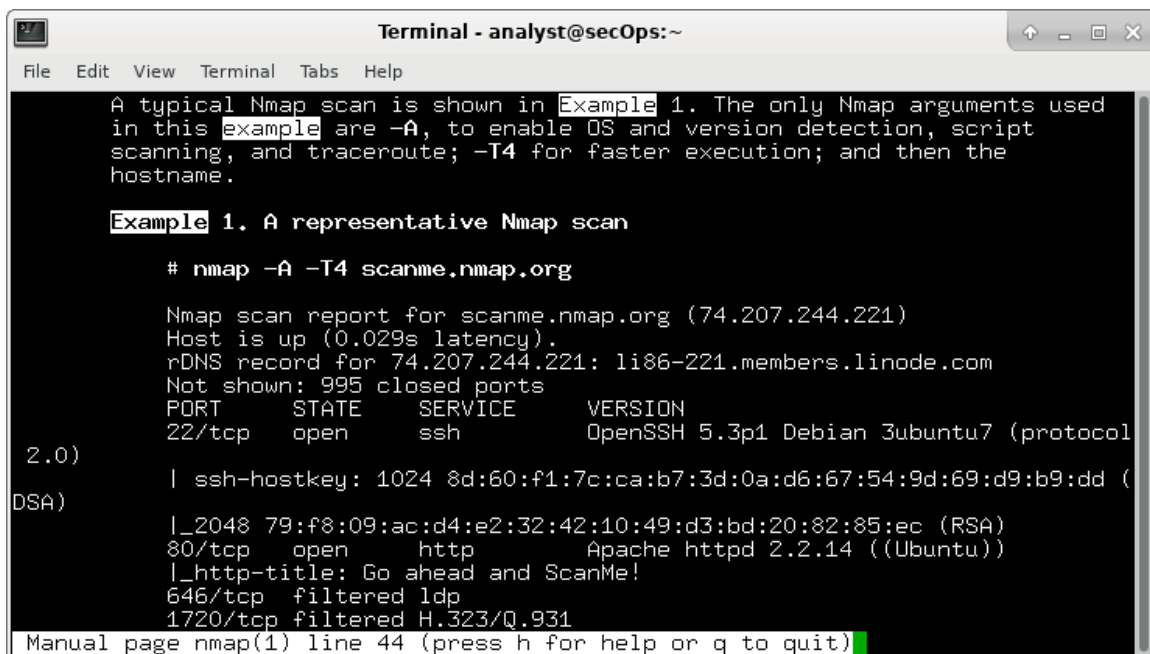
Saisissez **/example** et appuyez sur ENTRÉE. Cette opération permet de rechercher le mot **example** dans les pages suivantes du manuel.



```
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. Dans le premier exemple, trois correspondances s'affichent. Pour accéder à la correspondance suivante, appuyez sur **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 ldp
1720/tcp  filtered H.323/Q.931
Manual page nmap(1) line 44 (press h for help or q to quit)
```

Regardez l'exemple 1. Quelle est la commande **nmap** utilisée ?

Utilisez la fonction de recherche pour répondre aux questions suivantes.

À quoi sert le commutateur **-A** ?

À quoi sert le commutateur -T4 ?

- f. Faites défiler la page pour en savoir plus sur nmap. Saisissez « q » lorsque vous avez terminé.

Partie 2 : Analyse des ports ouverts

Dans cette partie, vous allez utiliser les commutateurs issus de l'exemple des pages de manuel Nmap pour analyser votre hôte local, votre réseau local et un serveur distant à scanme.nmap.org.

Étape 1 : Analysez votre hôte local.

- a. Si nécessaire, ouvrez un terminal sur la machine virtuelle. À l'invite, saisissez **nmap -A -T4 localhost**. Selon votre réseau local et vos périphériques, l'analyse peut durer de quelques secondes à quelques minutes.

```
[analyst@secOps Desktop]$ nmap -A -T4 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 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. Vérifiez les résultats et répondez aux questions suivantes.

Quels sont les ports et les services ouverts ?

Pour chacun des ports ouverts, notez le logiciel qui fournit les services.

Quel est le système d'exploitation ?

Étape 2 : Analysez votre réseau

AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau.

- a. À l'invite de commande du terminal, saisissez **ifconfig** pour déterminer l'adresse IP et le masque de sous-réseau de cet hôte. Dans cet exemple, l'adresse IP de cette machine virtuelle est 192.168.1.19 et le masque de sous-réseau est 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
```

Enregistrez l'adresse IP et le masque de sous-réseau de votre machine virtuelle. À quel réseau votre machine virtuelle appartient-elle ?

- b. Pour localiser les autres hôtes sur ce réseau local, saisissez **nmap -A -T4 network address/prefix**. Le dernier octet de l'adresse IP doit être remplacé par un zéro. Par exemple, l'adresse IP 192.168.1.19, où .19 correspond au dernier octet. Par conséquent, l'adresse réseau est 192.168.1.0. /24 est le préfixe. Il s'agit du raccourci pour le masque de sous-réseau 255.255.255.0. Si le masque de réseau votre machine virtuelle est différent, recherchez votre préfixe dans le « tableau de conversion CIDR » sur Internet. Par exemple, 255.255.0.0 correspond à /16. L'adresse réseau 192.168.1.0/24 est utilisée dans cet exemple.

Remarque : cette opération peut prendre un certain temps, surtout si plusieurs périphériques sont connectés au réseau. Dans l'environnement de test, l'analyse a pris environ 4 minutes.

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

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 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
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

Comment d'hôtes sont activés ?

Dans vos résultats Nmap, répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle. Répertoriez certains des services qui sont disponibles sur les ordinateurs hôtes détectés.

Étape 3 : Analysez un serveur distant.

- Ouvrez un navigateur web et accédez à l'adresse **scanme.nmap.org**. Veuillez lire le message posté. Quel est l'objectif de ce site ?

- À l'invite du terminal, saisissez **nmap -A -T4 scanme.nmap.org**.

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

```
Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 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
```

Travaux pratiques – Découvrir Nmap

```
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. Vérifiez les résultats et répondez aux questions suivantes.

Quels sont les ports et les services ouverts ?

Quels sont les ports et les services filtrés ?

Quelle est l'adresse IP du serveur ?

Quel est le système d'exploitation ?

Remarques générales

Nmap est un outil puissant pour l'exploration et la gestion du réseau. Comment Nmap peut-il contribuer à la sécurité du réseau ? Comment Nmap peut-il être utilisé par un hacker comme outil néfaste ?
