Objectifs

Partie 1 : Découvrir l'utilitaire Nmap
Partie 2 : Analyse des ports ouverts sur un réseau

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 Nmap. Nmap est un utilitaire réseau puissant qui est utilisé pour la découverte des ordinateurs et des services du réseau et pour l'audit de sécurité.

Ressources requises

- Poste de travail VM labtainer ou CyberOps cisco
- Accès Internet

Instructions

La première partie de cette activité pratique peut-être réalisée soit sur la VM ubuntu labtainer ou la VM CyberOps.

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.

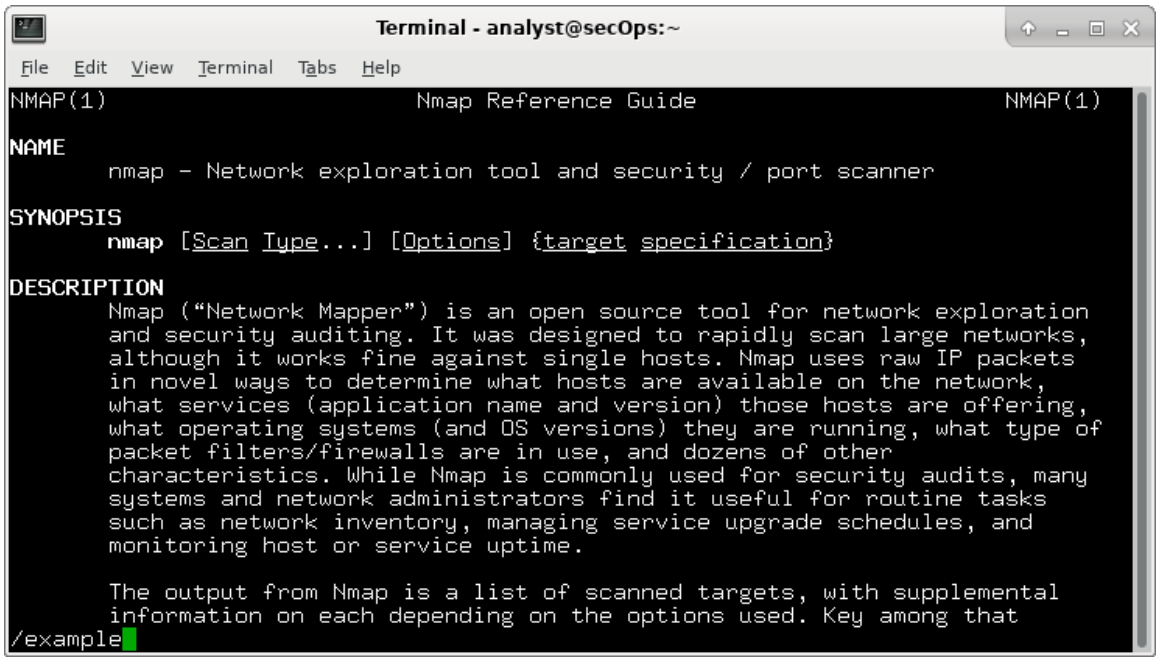
a. A partir du poste de travail virtuel (ubuntu labtainer ou CyberOps), à l'invite du terminal, saisissez **man nmap**.

```
$ man nmap
```

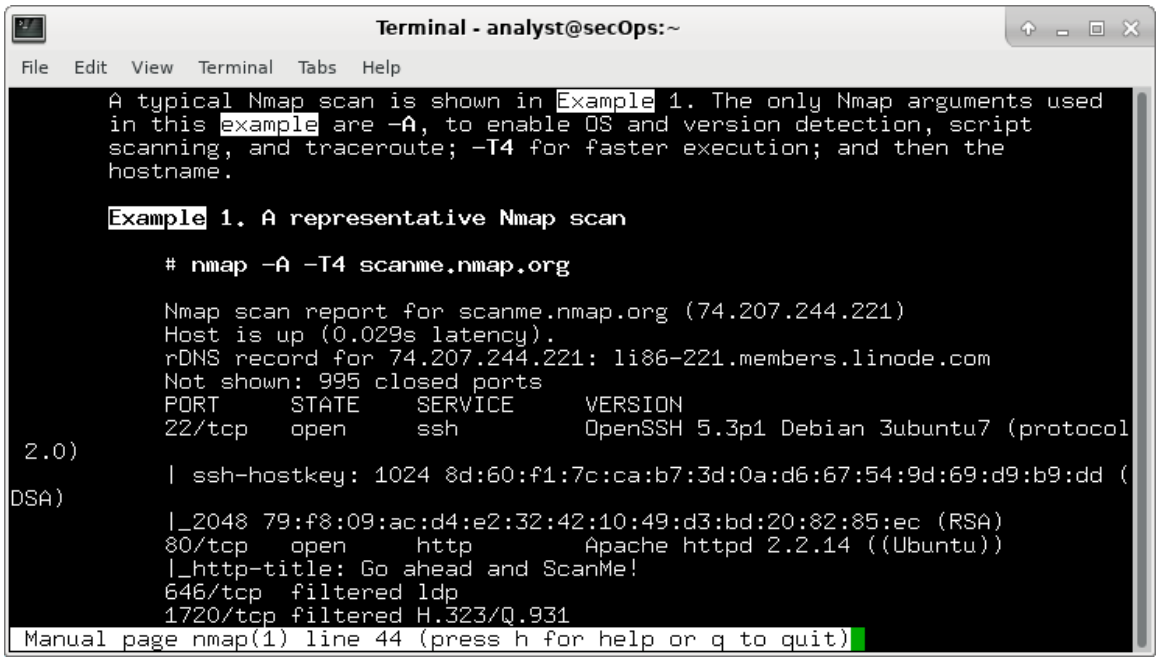
   - Qu'est-ce que Nmap ?
   - À quoi Nmap sert-il ?

b. 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** vers l'avant dans les pages du manuel.



c. Dans le premier exemple, trois correspondances s'affichent. Pour accéder à la correspondance suivante, appuyez sur **n**.



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 ?

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

Partie 2 : Analyse des ports ouverts sur un réseau

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.
AVERTISSEMENT : avant d'utiliser Nmap sur un réseau, demandez l'autorisation des propriétaires du réseau. En particulier le scan d'un hôte distant n'est pas autorisé sauf s'il s'agit d'un « bac à sable », d'un « pot de miel » ou tout hôte pour lequel vous en avez l'autorisation.

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.

```
$ 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
<some output omitted>
```

b. Vérifiez les résultats et répondez aux questions suivantes.

- Quels sont les ports et les services ouverts ?
- Pour chacun des ports ouverts, notez le nom de l'application qui fournit le service.

Étape 2: Analysez votre réseau virtuel interne

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

a. À l'invite de commande du terminal, saisissez **ip address** 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 10.0.2.15 et le masque de sous-réseau est 255.255.255.0.

```
$ ip address
<output omitted>
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 étendue dynamique globale enp0s3
       valid_lft 85777sec preferred_lft 85777sec
    inet6 fe80:: a 00:27 ff:feed:af2c/64 lien de portée
       valid_lft forever preferred_lft forever
```

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 10.0.2.15, où .15 correspond au dernier octet. Par conséquent, l'adresse réseau est 10.0.2.0. /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 10.0.2.0/24 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.

```
$ nmap -A -T4 10.0.2.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2017 17:13 EDT
<output omitted>
Nmap scan report for 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: Anonymous FTP login allowed (FTP code 230)
|_-rw-r—r— 1 0 0 0 26 mars 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
```

- Dans l'exemple ci-dessus, combien d'hôtes sont actifs ?
- Quelles adresses IP et quels ports et services sont ouverts ?

- Dans vos résultats Nmap, **nmap -A -T4 *network address/prefix*** avec *address* et *prefix* correspondants au réseau de la machine virtuelle
  - Combien d'hôtes sont actifs ?
  - Répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle.
  - Répertoriez les services qui sont disponibles sur les ordinateurs hôtes détectés.

Étape 3: Tâche labtainer – découverte du réseau et accès ssh à un serveur distant

Depuis le terminal de la VM labtainer, exécutez le **labtainer nmap-discovery** à l'aide la commande :

```
labtainer nmap-discovery
```

Taches

Votre responsable Randall veut que vous prépariez une réunion sur un projet sur lequel vous n'avez pas travaillé depuis des mois. Vous avez un fichier récapitulatif sur le serveur « friedshrimp » auquel vous avez précédemment accédé via ssh; cependant, vous ne vous souvenez pas de l'adresse IP de « friedshrimp », et vous avez également oublié quel port a été affecté au service ssh sur ce serveur. Vous savez que c'est entre 2000 et 3000.

La seule chose que vous savez avec certitude est que votre nom d'utilisateur et votre mot de passe sont tous deux « ubuntu ». Il ne vous reste qu'une seule option : utiliser la commande **nmap** pour trouver l'adresse IP et le numéro de port utilisés par le service ssh. Après avoir trouvé cette information, examinez le contenu du fichier « friedshrimp.txt » à partir d'une session ssh.

Notez que pour accéder en ssh à un hôte par l'intermédiaire d'un port autre que celui par défaut, il faut utiliser la commande :

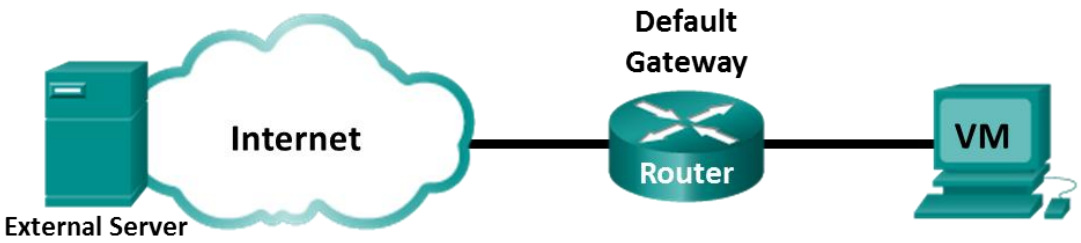
```
ssh -p <port> <host>
```

a. Réalisez la mission et répondez aux questions suivantes
   - Quelle est l'adresse IP de friedshrimp ?
   - Sur quel port le service ssh est-il configuré ?
   - Quelle commande devez-vous utiliser pour accéder à la machine friedshrimp en ssh ?
   - Quelles commandes devez-vous utiliser pour examiner le contenu du fichier « friedshrimp.txt » via ssh ?
   - Quelle information concernant le projet Fried Shrimp contient le fichier « friedshrimp.txt » ?

NB : pour évaluer l'avancée de votre lab vous pouvez à tout moment taper la commande `checkwork` dans le terminal qui vous a permis de lancer le labtainer.

b. Une fois terminé arrêtez le lab avec la commande `stoplab`

Étape 4: Analysez un serveur distant.



a. Ouvrez un navigateur web et accédez à l'adresse **scanme.nmap.org**. Veuillez lire le message posté.

   - Quel est l'objectif de ce site ?

   Le résultat de la commande **nmap -A -T4 scanme.nmap.org**. a donné les résultats suivants :

```
Starting Nmap 7.40 ( https://nmap.org ) at 01/05/2020 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
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
```

- 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 ?

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

```
$ nmap -A -T4 scanme.nmap.org
```

Vérifiez les résultats obtenus et répondez aux questions suivantes :

- Quels sont les ports et les services ouverts ?
- Quels sont les ports et les services filtrés ?

Question de réflexion

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 ?

Portqry est un outil microsoft en ligne de commandes équivalent à nmap qui peut être utilisé sur un ordinateur Windows
https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/networking/portqry-exe-command-line-utility
Zenmap est la version « graphique » de nmap disponible pour Linux, Mac, Windows
https://nmap.org/zenmap/

Crédits : d'après les laboratoires labtainer nmap-discovery et Cisco CyberOperations Associate 1.0 FR 9.3.8 Lab - Exploring Nmap