

Travaux pratiques – Détection des menaces et des vulnérabilités

Objectifs

Utiliser Nmap, un scanner de port et un outil d'exploration du réseau pour détecter les menaces et les vulnérabilités présentes dans un système.

Contexte/Scénario

Network Mapper, ou Nmap, est un utilitaire open source utilisé pour l'exploration de réseaux et les audits de sécurité. Les administrateurs utilisent également Nmap pour contrôler l'activité des hôtes ou pour gérer les programmes de mise à jour des services. Nmap identifie les hôtes disponibles sur un réseau, les services en cours d'exécution, les systèmes d'exploitation utilisés ainsi que les filtres de paquets ou les pare-feu actifs.

Ressources requises

- Ordinateur équipé d'Ubuntu 16.0.4 LTS dans un poste de travail VMware.

Étape 1 : Ouvrez une fenêtre de terminal dans Ubuntu.

- Connectez-vous à Ubuntu à l'aide des informations d'identification suivantes :

Utilisateur : **cisco**

Mot de passe : **password**



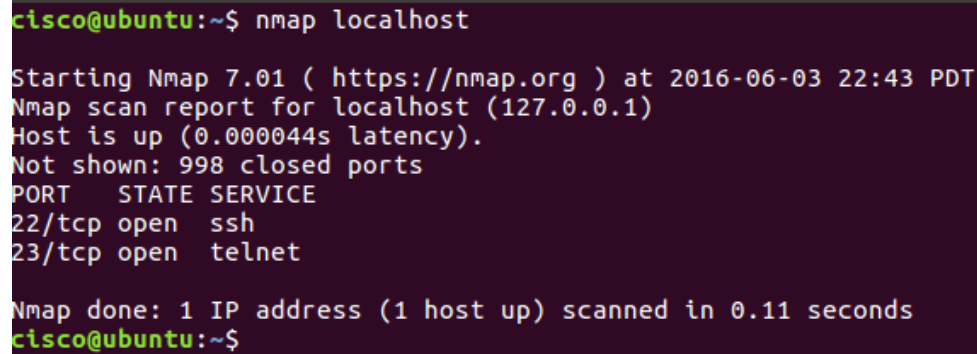
- Cliquez sur l'icône du **terminal** pour ouvrir un terminal.



Étape 2 : Lancez Nmap.

À l'invite de commandes, saisissez la commande suivante pour exécuter une analyse basique sur ce système 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:~$
```

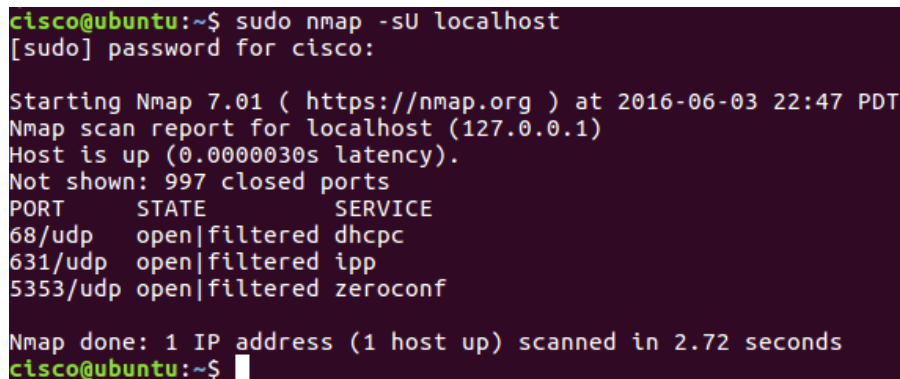
Les résultats affichés correspondent à l'analyse des 1 024 premiers ports TCP.

Quels sont les ports TCP ouverts ?

Étape 3 : Utilisez les privilèges administratifs avec Nmap.

- Saisissez la commande suivante dans le terminal pour analyser les ports UDP de l'ordinateur (n'oubliez pas qu'Ubuntu est sensible à la casse), puis saisissez le mot de passe **password** lorsque vous y êtes invité :

```
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 dhcpd
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:~$
```

Quels ports UDP sont ouverts ?

- b. Saisissez la commande suivante dans le 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:~$
```

L'utilisation du commutateur **-sV** avec la commande **nmap** permet d'afficher les versions, ce qui peut être utile pour rechercher des vulnérabilités.

Étape 4 : Capturez des clés SSH.

- Saisissez la commande suivante dans le terminal pour lancer une analyse des scripts :

```
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:~$
```

Vous avez capturé des clés SSH pour le système hôte. La commande exécute une série de scripts de Nmap pour détecter des vulnérabilités spécifiques.

Références

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