

Activité DÉCOUVRIR LE RÉSEAU AVEC NMAP



Objectifs

Partie 1 : découvrir l'utilitaire Nmap

Partie 2 : analyse des ports ouverts sur un réseau

SRIKANTHAN Sabiran

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

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

1. Partie 1 : découvrir l'utilitaire 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 ?

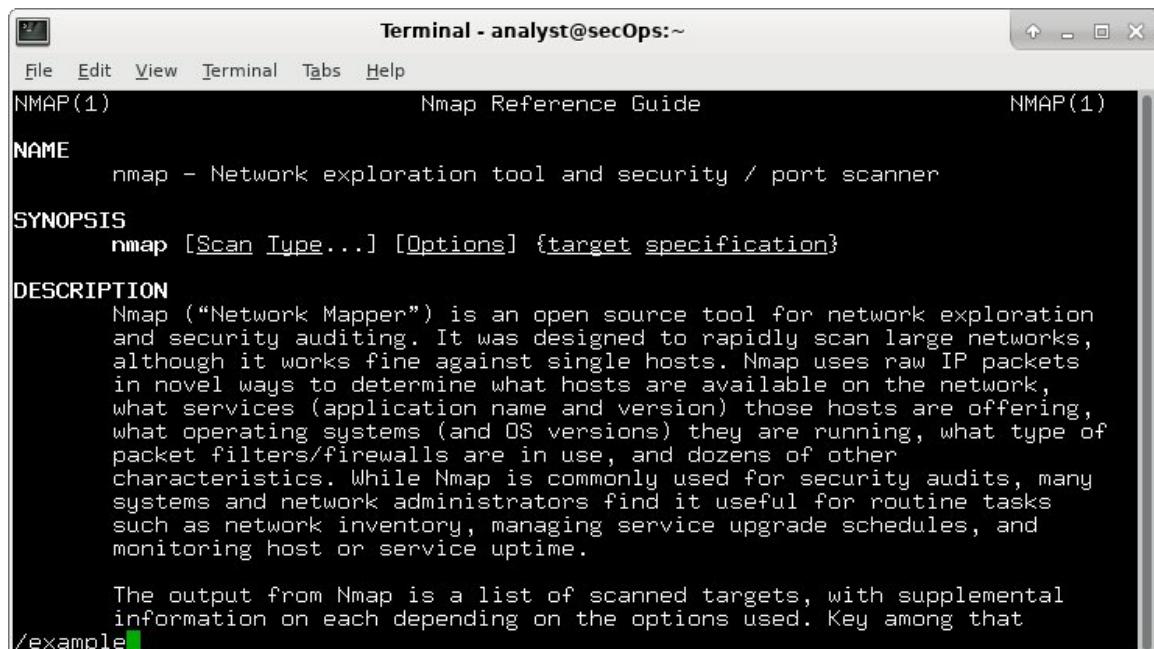
⇒ Nmap (Network Mapper) est un outil permettant de découvrir les hôtes d'un réseau, d'analyser les ports ouverts et d'identifier les services et systèmes d'exploitation

⇒ À quoi Nmap sert-il ?

⇒ Il sert à : Découvrir les machines connectées à un réseau, identifier les ports ouverts, détecter les services actifs, Réaliser des audits de sécurité

- 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.



```
Terminal - analyst@secOps:~
```

NMAP(1) Nmap Reference Guide **NMAP(1)**

NAME
nmap - Network exploration tool and security / port scanner

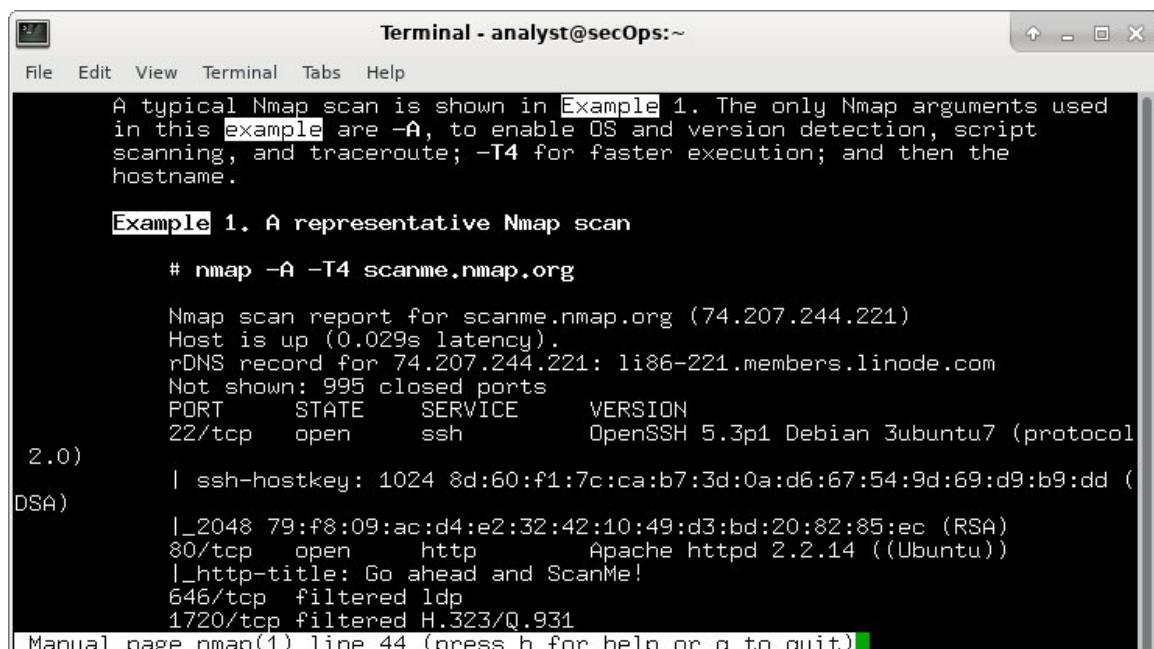
SYNOPSIS
`nmap [Scan Type...] [Options] {target specification}`

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

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



```
Terminal - analyst@secOps:~
```

NMAP(1) Nmap Reference Guide **NMAP(1)**

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)
DSA)      | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd
|_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 ?

Nmap -A -T4 scanme.nmap.org

Utilisez la fonction de recherche pour répondre aux questions suivantes.

⇒ À quoi sert le commutateur -A ?

Le commutateur -A active la détection OS, versions de services, scripts NSE et traceroute en une seule commande.

À quoi sert le commutateur -T4 ?

Le commutateur -T4 de Nmap définit un timing agressif (4/5) pour accélérer les scans en réduisant les délais et augmentant la parallélisation, idéal sur réseaux rapides tout en restant discret

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

• **2. 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.

•

• **2A. 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 ?

Le port 21/tcp est ouvert et fournit le service FTP

Pour chacun des ports ouverts, notez le nom de l'application qui fournit le service.

L'application vsftpd fournit le service FTP sur le port 21/tcp

• **2B. Étape 2 : analysez votre réseau virtuel interne**

- 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
```

⇒ Relevez l'adresse IP et le masque de sous-réseau de votre machine virtuelle.

Adresse IP : 172.25.0.2

Masque de sous-réseau : /16 (255.255.0.0)

⇒ À quel réseau votre machine virtuelle appartient-elle ?

La machine virtuelle appartient au réseau 172.25.0.0/16

- 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 ?

Les adresses IP actifs sont : 10.0.2.2, 10.0.2.3, 10.0.2.4 et 10.0.2.15

Quelles adresses IP et quels ports et services sont ouverts ?

21 —> FTp (vsftpd)

22 —> SSH

23 —> Telnet

Dans vos résultats Nmap, **nmap -A -T4 172.25.0.2/24** avec *address* et *prefix* correspondants au réseau de la machine virtuelle

⇒ Combien d'hôtes sont actifs ?

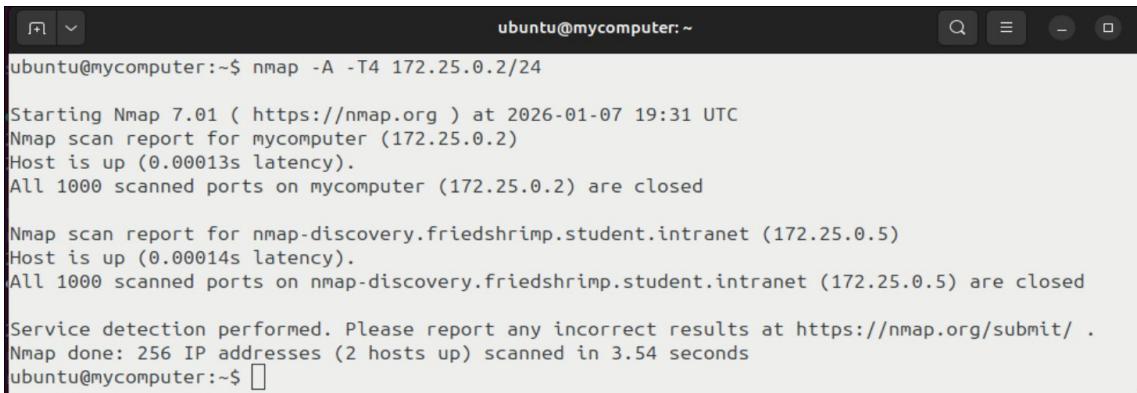
Il y a deux port actifs et aucun ports ouvert

⇒ Répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle.

Les adresses IP détectées sur le réseau local sont 172.25.0.2 et 172.25.0.5.

Répertoriez les services qui sont disponibles sur les ordinateurs hôtes détectés.

Aucun service n'a été détecté comme ouvert ; les 1000 ports analysés sont fermés sur les deux hôtes.



The screenshot shows a terminal window titled "ubuntu@mycomputer: ~". The command entered was "nmap -A -T4 172.25.0.2/24". The output indicates that the scan started at 2026-01-07 19:31 UTC and found two hosts up: mycomputer (172.25.0.2) and nmap-discovery.friedshrimp.student.intranet (172.25.0.5). Both hosts were found to be up with low latency. All 1000 scanned ports on both hosts were closed. Service detection was performed, but no open ports were detected. The entire scan completed in 3.54 seconds, scanning 256 IP addresses.

```
ubuntu@mycomputer:~$ nmap -A -T4 172.25.0.2/24
Starting Nmap 7.01 ( https://nmap.org ) at 2026-01-07 19:31 UTC
Nmap scan report for mycomputer (172.25.0.2)
Host is up (0.00013s latency).
All 1000 scanned ports on mycomputer (172.25.0.2) are closed

Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)
Host is up (0.00014s latency).
All 1000 scanned ports on nmap-discovery.friedshrimp.student.intranet (172.25.0.5) are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.54 seconds
ubuntu@mycomputer:~$
```

Résultat de la commande nmap -A -T4 172.25.0.2/24 montrant deux hôtes actifs sur le réseau local (172.25.0.2 et 172.25.0.5), sans aucun port ouvert détecté sur les hôtes analysés.

• 2C.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

1. Tâches

Votre responsable Randall veut que vous préparez 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 ?

L'adresse IP de friedshirmp : 172.25.0.5

⇒ Sur quel port le service ssh est-il configuré ?

Le service SSH est configuré sur le 2827

```
ubuntu@mycomputer:~$ nmap -sV -p 2827 172.25.0.5
Starting Nmap 7.01 ( https://nmap.org ) at 2026-01-07 19:48 UTC
Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)
Host is up (0.00017s latency).
PORT      STATE SERVICE VERSION
2827/tcp  open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Confirmation du service SSH sur le port 2827/tcp du serveur friedshrimp.

→ Quelle commande devez-vous utiliser pour accéder à la machine friedshrimp en ssh ?

La commande que je devrais utiliser est : ssh -p 2827 ubuntu@172.25.0.5

```
student@Labtainer-VirtualBox:~$ ssh -p 2827 ubuntu@172.25.0.5
ubuntu@172.25.0.5's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 6.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Wed Jan  7 20:00:59 2026 from 172.25.1.101
ubuntu@friedshrimp:~$ 
```

→ Quelles commandes devez-vous utiliser pour examiner le contenu du fichier « friedshrimp.txt » via ssh ?

La commande est : cat friedshrimp.txt ou less friedshrimp.txt

```
student@Labtainer-VirtualBox:~$ ssh -p 2827 ubuntu@172.25.0.5
ubuntu@172.25.0.5's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 6.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Wed Jan  7 20:00:05 2026 from 172.25.1.101
ubuntu@friedshrimp:~$ cat friedshrimp.txt
My summary notes from the fried shrimp project:

Fried Shrimp Project: We concluded it is better to
buy than to build.

=====
Congratulations! You managed to find the summary file
for "fried shrimp" and impress Randall.
ubuntu@friedshrimp:~$ 
```

→ Quelle information concernant le projet Fried Shrimp contient le fichier « friedshrimp.txt » ?

Le fichier indique que, pour le projet Fried Shrimp, il a été décidé qu'il est préférable d'acheter plutôt que de construire.

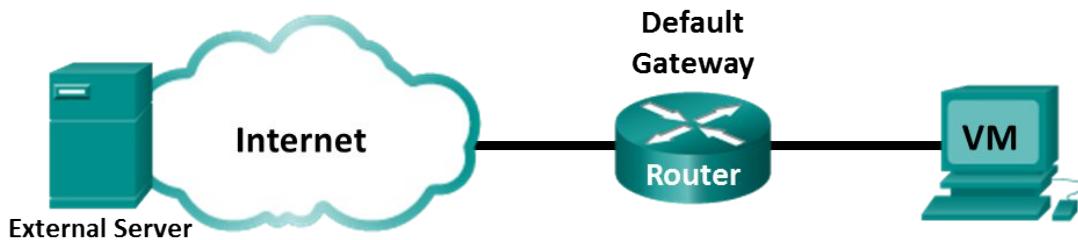
NB : pour évaluer l'avancée de votre lab vous pouvez à tout moment taper la commande checkwork dans le terminal qui vous a permis de lancer le labtainer.

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

```
Digest: sha256:17e2a27454fad4e48cf81a03e59b2e12d30409e10f6ac707d61604f03f5f3d5
Status: Downloaded newer image for labtainers/labtainer.grader:latest
Successfully copied 138kB to nmap-discovery-igrader:/home/instructor/dd.nmap-discovery.lab
Successfully copied 2.05kB to /home/student/labtainer_xfer/nmap-discovery
Labname nmap-discovery

Student           |      nmap_count |      did_ssh |
===== | ===== | ===== |
dd          |      8 |      |
What is automatically assessed for this lab:
  did_ssh: SSH'd to the proper port and viewed the target file
  nmap_count: count of use of nmap
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$
```

- **2D. 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 site scanme.nmap.org permet aux utilisateurs de tester légalement l'outil Nmap sur un serveur prévu à cet effet, afin de s'entraîner et de se familiariser avec l'analyse de ports sans enfreindre de règles de sécurité

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 ?

Les ports ouverts sont 22/tcp (SSH), 80/tcp (HTTP), 9929/tcp (Nping echo) et 31337/tcp (tcpwrapped).

⇒ Quels sont les ports et les services filtrés ?

Les ports 25, 135, 139, 445, 593 et 4444 sont filtrés, ce qui indique la présence de règles de filtrage réseau ou de pare-feu.

⇒ Quelle est l'adresse IP du serveur ?

L'adresse IP du serveur est 45.33.32.156.

⇒ Quel est le système d'exploitation ?

Le système d'exploitation du serveur est Linux (Ubuntu).

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 ?

Les ports ouverts sont 22/tcp, 80/tcp, 9929/tcp et 31337/tcp

⇒ Quels sont les ports et les services filtrés ?

Les ports 25/tcp (SMTP), 139/tcp (NetBIOS-SSN), 389/tcp (LDAP), 445/tcp (Microsoft-DS) et 9200/tcp (WAP-WSP) sont filtrés.

- ### 3. 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 ?

Nmap permet d'identifier les ports ouverts, les services actifs et les failles potentielles, afin de sécuriser le réseau avant qu'il ne soit attaqué.

Comment Nmap peut-il être utilisé par un hacker comme outil néfaste ?

Un hacker peut utiliser Nmap pour repérer des vulnérabilités et préparer des attaques contre des services mal protégés.

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/>