

Documentation – NMAP



Classe : BTS SIO 25.1A

Nom : Rayan Bellahouel

Table des matières

1- Définition

2- Prérequis

3- Installation

4- Fonctionnement

1- Définition

NMAP : NMAP est un outil de scan de réseau utilisé pour découvrir des hôtes et services sur un réseau informatique, facilitant ainsi l'audit de sécurité et l'exploration de réseau. Il envoie des paquets spéciaux et analyse les réponses pour recueillir des informations telles que les services ouverts, les systèmes d'exploitation en cours d'exécution, les types de filtres de pare-feu, etc. Utilisé par les professionnels de la sécurité, NMAP aide à évaluer la sécurité d'un réseau en identifiant les points d'entrée potentiels pour les attaquants.

Tshark : Tshark est la version en ligne de commande de Wireshark, utilisée pour capturer et analyser le trafic réseau. Elle permet de visualiser en temps réel ou d'examiner des fichiers de capture de données réseau, offrant une analyse détaillée des protocoles et des échanges sur le réseau sans nécessiter d'interface graphique.

SSH : SSH (Secure Shell) est un protocole de communication sécurisé utilisé pour l'accès à distance aux serveurs et appareils réseau. Il assure une connexion cryptée, sécurisant les échanges de données contre les écoutes indiscretes.

Telnet : Telnet est un protocole réseau permettant des sessions de commande à distance, sans cryptage des données, rendant son usage moins sécurisé par rapport à SSH pour les connexions sur des réseaux non sûrs.

TCPDUMP : TCPDUMP est un puissant outil en ligne de commande pour la capture et l'analyse de paquets réseau sur des systèmes Unix/Linux. Il intercepte et enregistre le trafic passant par les interfaces réseau de l'ordinateur, permettant une inspection détaillée des données et des échanges réseau pour le diagnostic et la surveillance de la sécurité.

2- Prérequis

Hyperviseur de Type 2 : Utilisez VirtualBox ou tout autre hyperviseur de type 2. Ces hyperviseurs s'exécutent comme une application au sein de votre système d'exploitation hôte.

ISO Ubuntu Labtainer : Vous aurez besoin de l'image disque ISO spécifique pour Ubuntu Labtainer. Cette version d'Ubuntu est préconfigurée pour inclure Labtainer, un ensemble d'outils de laboratoire pour les cours de cybersécurité.

(Disponible au téléchargement ici :

<https://nps.box.com/shared/static/dn636n6h2d556nwqezx5w6cfc4cfeacl.ova>)

Nmap : un Analyseur de réseau (ports et version de logiciel)

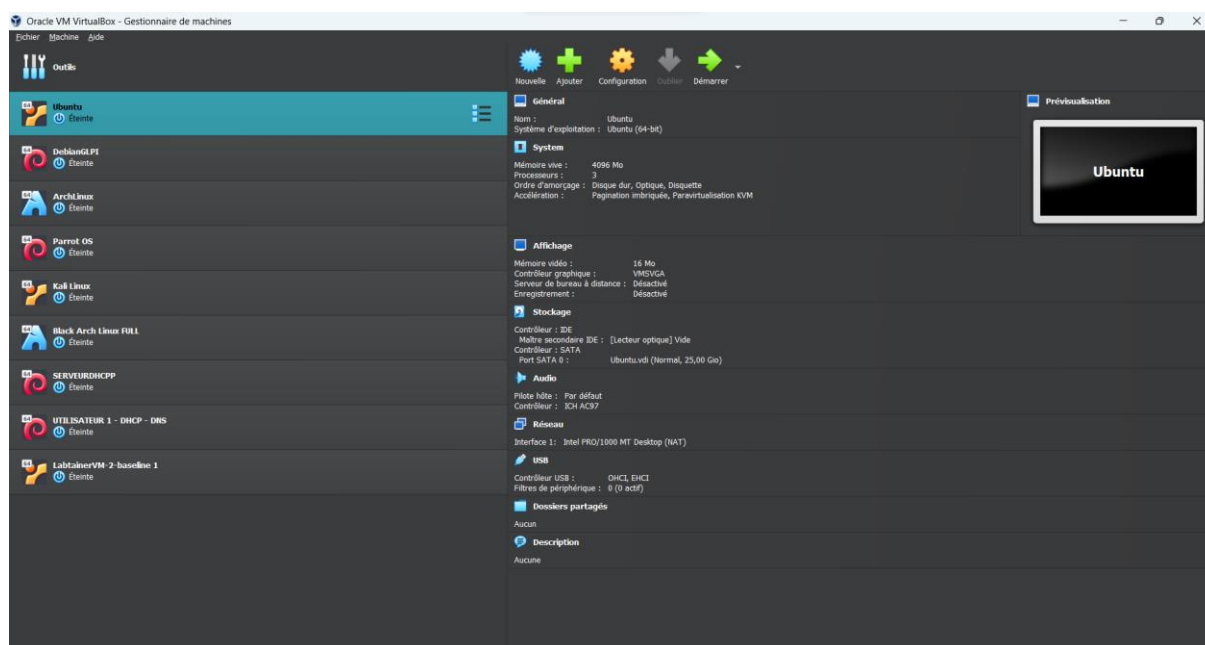
3- Installation

Premièrement nous allons installer l'iso préconfigurée via le lien donné dans « prérequis »

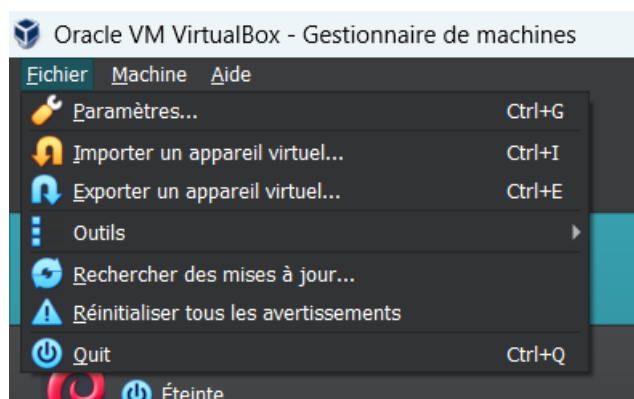
Maintenant que l'iso est installé et sur votre bureau, vous pouvez lancer VirtualBox (si vous ne l'avez pas installé, vous pouvez l'installer via le lien suivant :

<https://www.virtualbox.org/wiki/Downloads>)

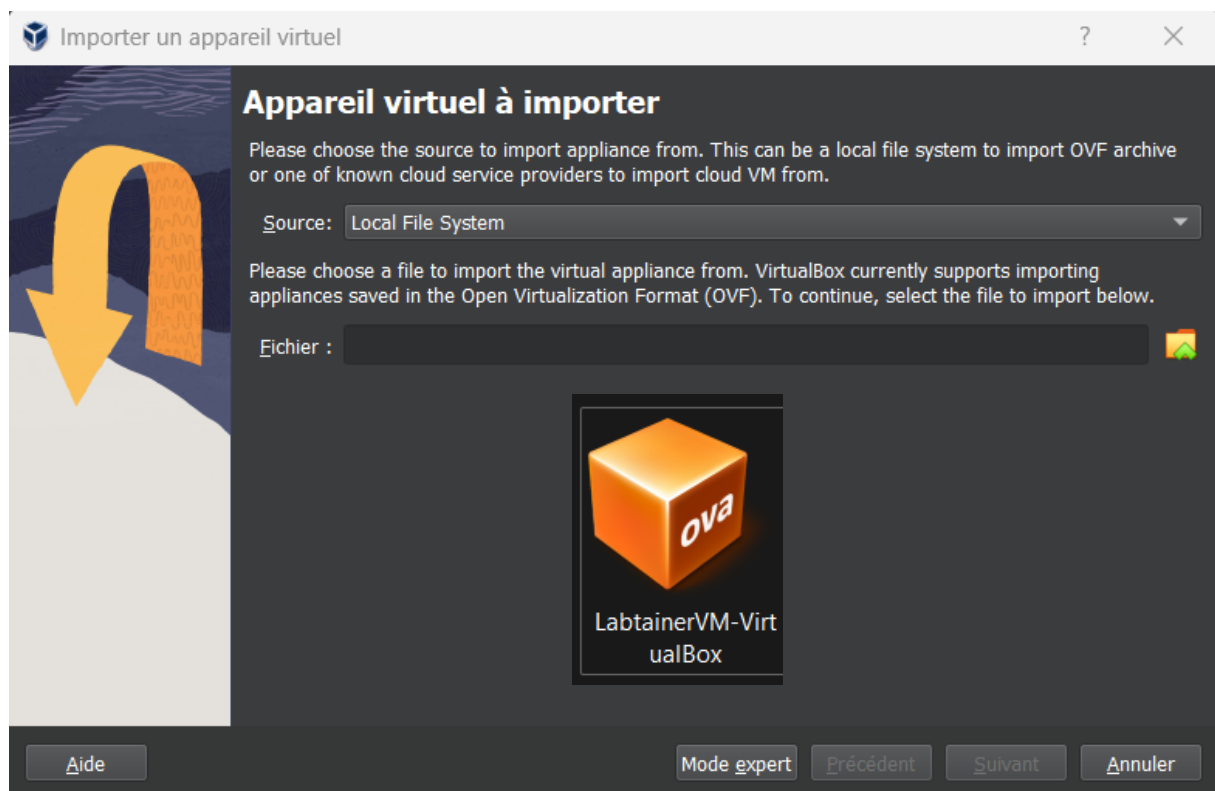
Maintenant, vous voici sur cette interface.



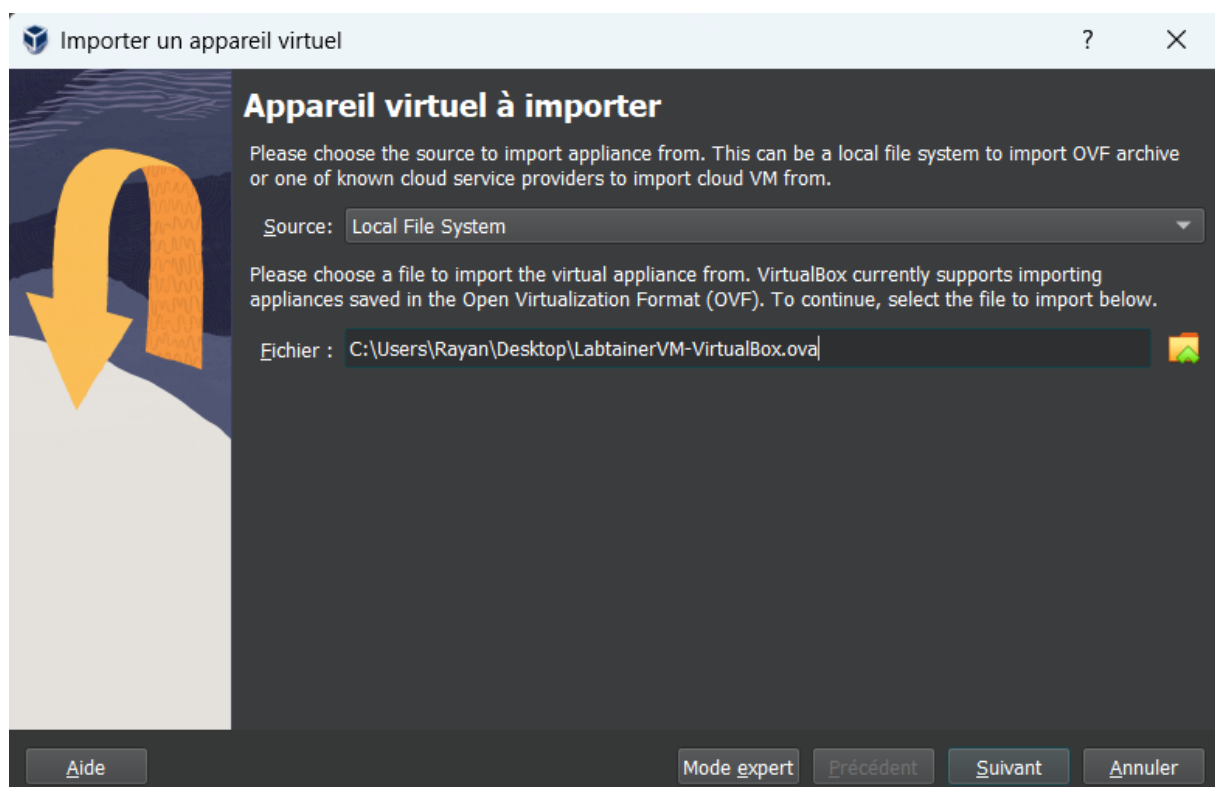
Cliquer sur « Fichier » en haut à gauche et cliquer sur « Importer un appareil virtuel... ».



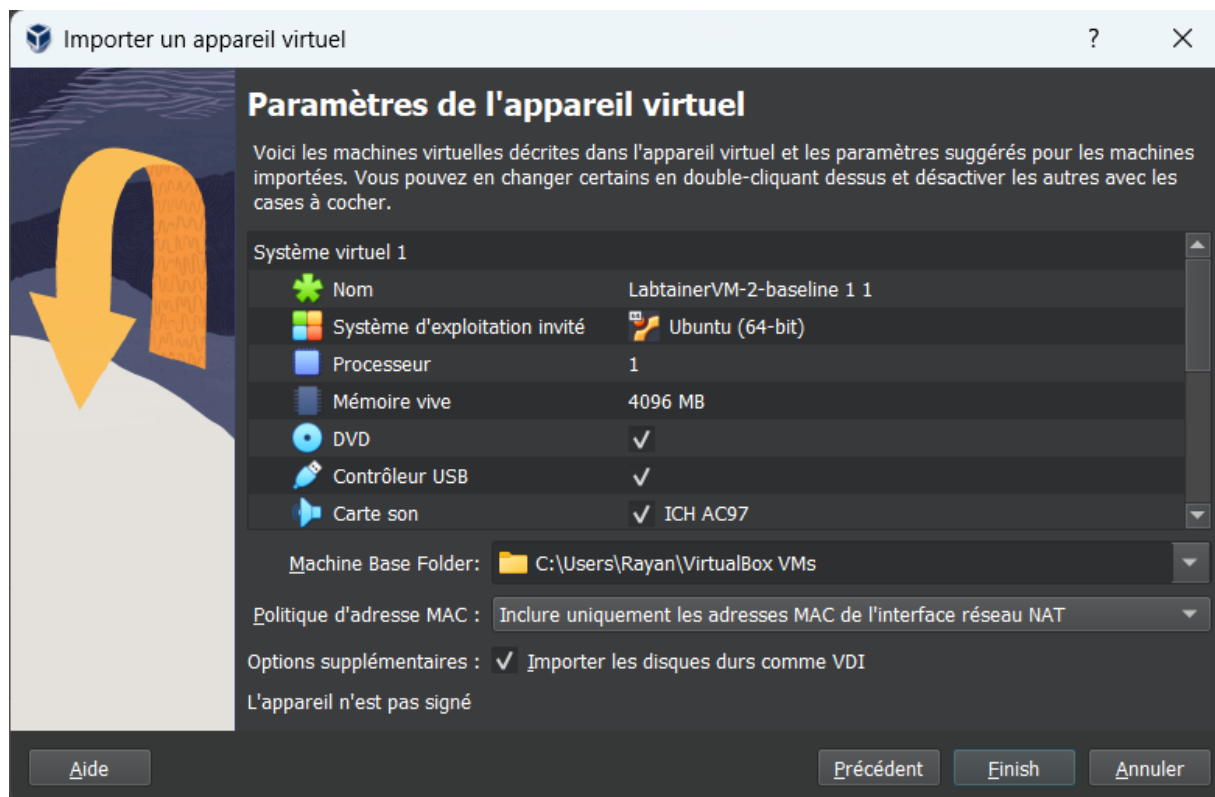
Arriver sur cette interface, sélectionner votre iso qui est sur votre bureau.



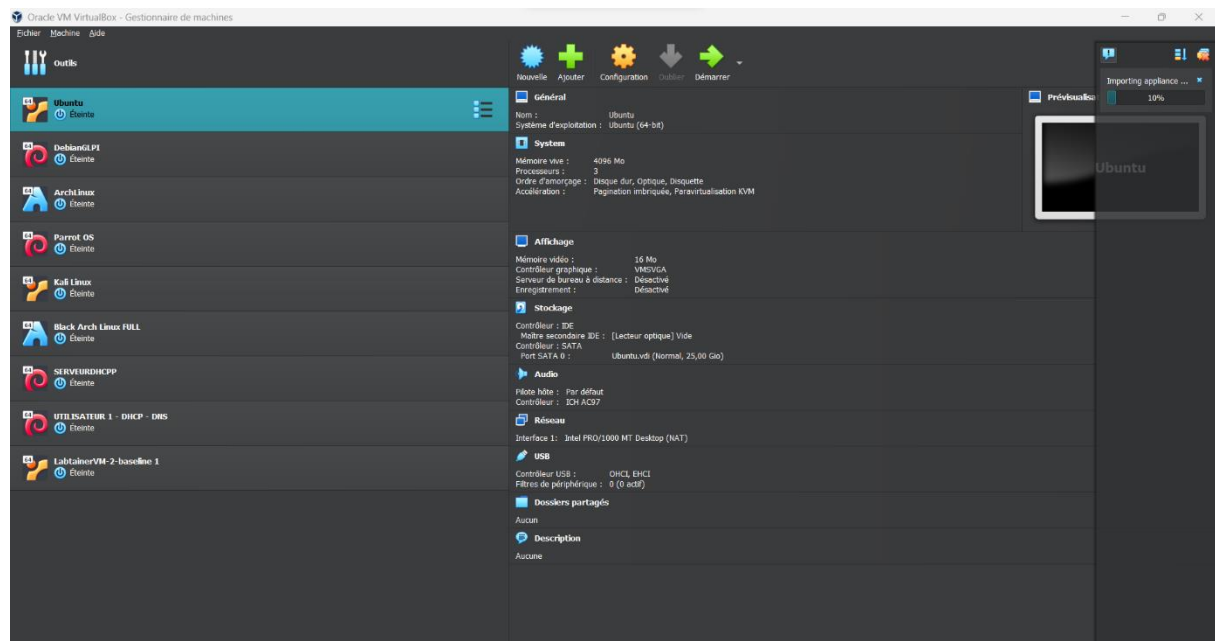
Si le chemin du fichier qui mène vers l'iso est correct, vous pouvez cliquer sur suivant.



Vous pouvez configurer votre machine et changer le processeur par exemple (je vous conseille de le mettre à 2). Après cela cliquer sur « finish ».



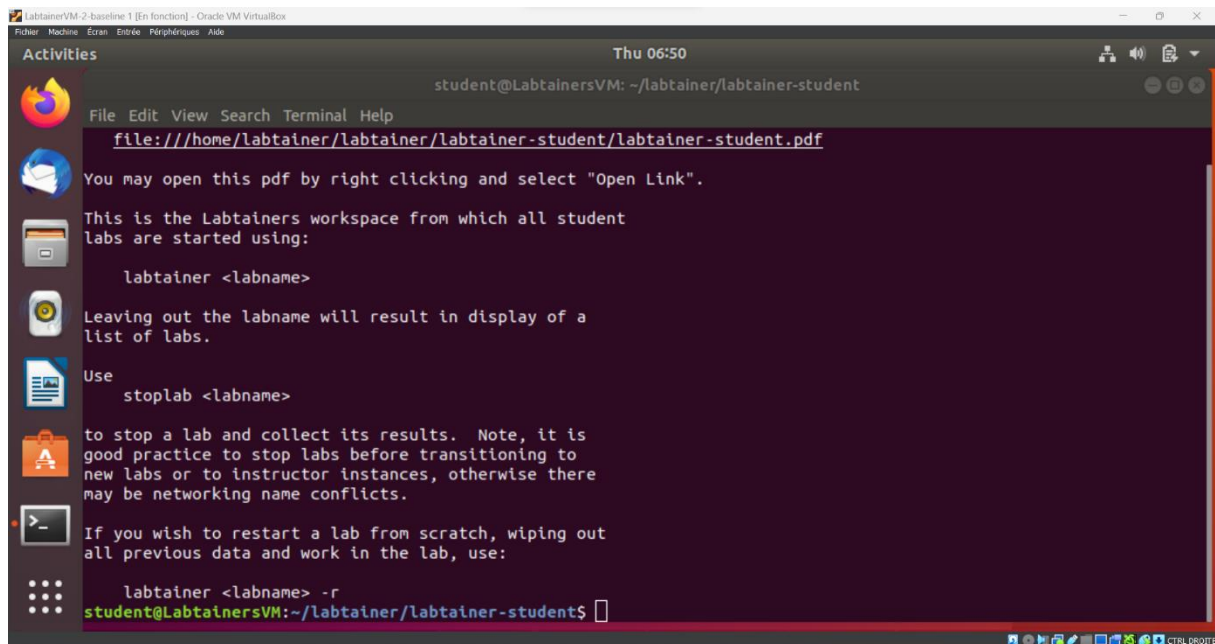
En haut à droite l'iso s'installe, attendez la fin de l'installation.



Et voilà vous pouvez lancer votre ISO.



Après avoir double cliquer sur l'iso, vous arriverais sur cette interface avec un terminale



The screenshot shows a terminal window titled "LabtainerVM-2-baseline 1 [En fonction] - Oracle VM VirtualBox". The terminal displays the following text:

```
student@LabtainersVM: ~/labtainer/labtainer-student
file:///home/labtainer/labtainer/labtainer-student/labtainer-student.pdf
You may open this pdf by right clicking and select "Open Link".
This is the Labtainers workspace from which all student
labs are started using:
    labtainer <labname>
Leaving out the labname will result in display of a
list of labs.
Use
    stoplab <labname>
to stop a lab and collect its results. Note, it is
good practice to stop labs before transitioning to
new labs or to instructor instances, otherwise there
may be networking name conflicts.
If you wish to restart a lab from scratch, wiping out
all previous data and work in the lab, use:
    labtainer <labname> -r
student@LabtainersVM:~/labtainer/labtainer-student$
```

Pour lancer NMAP & SSH, vous allez effectuer la commande suivante « labtainer nmap-ssh ».

4- Fonctionnement

Adresse IP client 172.24.0.2

Adresse IP du réseau clients : 172.24.0.0

Adresse IP de chaque interface du routeur eth0 & eth1

Adresse IP du réseau des serveurs 172.25.0.0

```
analyst@mycomputer:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
22: eth0@if23: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:18:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.24.0.2/24 brd 172.24.0.255 scope global eth0
        valid_lft forever preferred_lft forever
analyst@mycomputer:~$
```

```
analyst@router:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
24: eth0@if25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:18:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.24.0.3/24 brd 172.24.0.255 scope global eth0
        valid_lft forever preferred_lft forever
26: eth1@if27: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:19:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.25.0.3/24 brd 172.25.0.255 scope global eth1
        valid_lft forever preferred_lft forever
analyst@router:~$
```

Utilisation de la commande NMAP pour découvrir les hôtes d'un réseau et les services ouverts sur la machine client et la machine routeur (scanner l'ip du réseau des servers)

```
analyst@mycomputer:~$ nmap -A -T4 172.25.0.3/24

Starting Nmap 7.01 ( https://nmap.org ) at 2024-02-28 09:17 UTC
Nmap scan report for 172.25.0.1
Host is up (0.00021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.12)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.12
|_http-title: Directory listing for /
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.25.0.2
Host is up (0.00023s latency).
All 1000 scanned ports on 172.25.0.2 are closed

Nmap scan report for 172.25.0.3
Host is up (0.00025s latency).
All 1000 scanned ports on 172.25.0.3 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 26.94 seconds
analyst@mycomputer:~$
```

On modifie légèrement la commande pour mettre une plus grande plage de port entre 2000 & 3000 (garder la même adresse ip mais mettre la plage)

```
analyst@router:~$ nmap 172.25.0.2 -p 1000-3000

Starting Nmap 7.01 ( https://nmap.org ) at 2024-04-29 13:33 UTC
Nmap scan report for nmap-ssh.pserver.student.server_network (172.25.0.2)
Host is up (0.000081s latency).
Not shown: 2000 closed ports
PORT      STATE SERVICE
2280/tcp  open  lnvpoller
```

Maintenant au tour de cette commande :

Sudo tcpdump -i eth0 -x tcp -c 50

```
analyst@router:~$ sudo tcpdump -i eth0 -x tcp -c 50
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:21:31.799289 IP nmap-ssh.client.student.client_network.49386 > nmap-ssh.pserver.student.server_network.http: Flags [S], seq 321948248, win 29200, options [mss 1460,sackOK,TS val 3346071178 ec r 0,nop,wscale 7], length 0
    0x0000:  4500 003c 6c3e 4000 4006 7649 ac18 0001
    0x0010:  ac19 0002 c0ea 0050 1330 8a58 0000 0000
    0x0020:  a002 7210 5863 0000 0204 05b4 0402 080a
    0x0030:  c770 fe8a 0000 0000 0103 0307
09:21:31.799324 IP nmap-ssh.pserver.student.server_network.http > nmap-ssh.client.student.client_network.49386: Flags [R.], seq 0, ack 321948249, win 0, length 0
    0x0000:  4500 0028 6c30 4000 3f06 776b ac19 0002
    0x0010:  ac18 0001 0050 c0ea 0000 0000 1330 8a59
    0x0020:  5014 0000 f8d7 0000
09:21:32.805930 IP nmap-ssh.client.student.client_network.41510 > nmap-ssh.tserver.student.server_network.http: Flags [S], seq 243887376, win 29200, options [mss 1460,sackOK,TS val 769140203 ecr 0,nop,wscale 7], length 0
    0x0000:  4500 003c 8a72 4000 4006 5816 ac18 0001
    0x0010:  ac19 0001 a226 0050 0e89 6d10 0000 0000
    0x0020:  5014 0000 f8d7 0000
```

Le commutateur -X sert à : affiche le contenu de chaque paquet en hexadécimal.

Le commutateur -C sert à : Ce commutateur limite le nombre de paquets à capturer avant que tcpdump ne termine automatiquement (dans le cas présent tcpdump est limité à 50 paquets)

Pour voir la documentation de tshark (Tshark est WireShark en ligne de commande)

tshark -h Ou Man tshark

```
analyst@router:~$ tshark -h
TShark (Wireshark) 2.0.2 (SVN Rev Unknown from unknown)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
  -i <interface>      name or idx of interface (def: first non-loopback)
  -f <capture filter>  packet filter in libpcap filter syntax
  -s <snaplen>         packet snapshot length (def: 65535)
  -p                  don't capture in promiscuous mode
  -I                  capture in monitor mode, if available
  -B <buffer size>     size of kernel buffer (def: 2MB)
  -y <link type>       link layer type (def: first appropriate)
  -D                  print list of interfaces and exit
  -L                  print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>    stop after n packets (def: infinite)
  -a <autostop cond.> ... duration:NUM - stop after NUM seconds
                        filesize:NUM - stop this file after NUM KB
                        filesize:NUM,unit - stop this file after NUM unit
                        filesize:NUM,unit,duration:NUM - stop this file after NUM unit and NUM seconds
```

Nous permet de lister les interfaces dont le trafic peut être capturable

```
analyst@router:~$ tshark -D
1. eth0
2. eth1
3. any
4. lo (Loopback)
5. nflog
6. nfqueue
7. usbmon1
analyst@router:~$
```

Sur ce screen nous voyant des échanges via le protocole telnet

```
analyst@router:~$ sudo tshark -i eth0 -c 100
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as
a superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wi
reshark as an unprivileged user.
Capturing on 'eth0'
 1 0.000000000 172.24.0.1 -> 172.25.0.1 TCP 74 42146 -> 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
60 SACK_PERM=1 TSval=769459444 TSecr=0 WS=128
 2 0.000075218 172.25.0.1 -> 172.24.0.1 TCP 74 80 -> 42146 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
en=0 MSS=1460 SACK_PERM=1 TSval=1393885241 TSecr=769459444 WS=128
 3 0.000106996 172.24.0.1 -> 172.25.0.1 TCP 66 42146 -> 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
TSval=769459445 TSecr=1393885241
 4 0.000271177 172.24.0.1 -> 172.25.0.1 HTTP 213 GET /link1.html HTTP/1.1
 5 0.000294891 172.25.0.1 -> 172.24.0.1 TCP 66 80 -> 42146 [ACK] Seq=1 Ack=148 Win=30080 Len=
0 TSval=1393885241 TSecr=769459445
 6 0.001067894 172.25.0.1 -> 172.24.0.1 TCP 95 [TCP segment of a reassembled PDU]
 7 0.001260218 172.24.0.1 -> 172.25.0.1 TCP 66 42146 -> 80 [ACK] Seq=148 Ack=30 Win=29312 Len
=0 TSval=769459446 TSecr=1393885242
 8 0.001328546 172.25.0.1 -> 172.24.0.1 TCP 104 [TCP segment of a reassembled PDU]
 9 0.001342022 172.24.0.1 -> 172.25.0.1 TCP 66 42146 -> 80 [ACK] Seq=148 Ack=68 Win=29312 Len
=0 TSval=769459446 TSecr=1393885242
10 0.001384302 172.25.0.1 -> 172.24.0.1 TCP 103 [TCP segment of a reassembled PDU]
11 0.001394338 172.24.0.1 -> 172.25.0.1 TCP 66 42146 -> 80 [ACK] Seq=148 Ack=105 Win=29312 Le
n=0 TSval=769459446 TSecr=1393885242
12 0.001415773 172.25.0.1 -> 172.24.0.1 TCP 85 [TCP segment of a reassembled PDU]
```

Maintenant grâce à cette commande nous allons extraire tout le contenu du paquets telnet.data sur l'interface eth0

```
analyst@router:~$ sudo tshark -T fields -e telnet.data -i eth0
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See
https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Capturing on 'eth0'
```

Voici le contenu extrait :

```
Ubuntu 16.04.4 LTS

tserver login:
```

```
ubuntu
ubuntu

Password:

26c98e
```

```
,Last login: Mon Apr 29 13:25:25 UTC 2024 from 172.24.0.1 on pts/1

Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

,
, * Documentation:  https://help.ubuntu.com
, * Management:    https://landscape.canonical.com
, * Support:       https://ubuntu.com/advantage
```

```
ls
ls

MyHTTPServer.py  filetoview.txt  index.html  link1.html  link2.html

ubuntu@tserver:~$

exit
exit

logout
```

Nous referions la commande suivi de « > capture.txt » pour mettre le résultat de la commande dans le fichier capture.txt

```
^C164 packets captured
analyst@router:~$ sudo tshark -T fields -e telnet.data -i eth0 > capture.txt
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See
https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Capturing on 'eth0'
523 ^C
analyst@router:~$ cat capture.txt
```

Une fois que nous avons eu le mots d'utilisateur et le mot de passe nous pouvons nous connecter

Utilisateur : Ubuntu

Password : 26c98e

A l'aide de la commande suivante :

Ssh -p 2280 ubuntu@172.25.0.2

```
analyst@router:~$ ssh -p 2280 ubuntu@172.25.0.2
ubuntu@172.25.0.2's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

Voila ! Vous êtes connecté à la machine « cible »