IMT Mines Alès
École Mines-Télécom

Institut Mines-Télécom

IMT Mines Alès - Site Clavières

Département Systèmes et Réseaux (SR)

Ethical Hacking - TryHackMe NMAP

Nathan Martel

Groupe : SR
IMT Mines Alès

21 novembre 2024

TLP :RED

Table des matières

1 Introduction :

Le challenge Nmap de TryHackMe permet d'avoir un aperçu approfondi de l'analyse avec Nmap, un puissant outil d'analyse réseau.

URL du challenge : https://tryhackme.com/r/room/furthernmap

@uthor : Nathan Martel.

Le document est classifié sous la marque **TLP :RED** (Traffic Light Protocol), ce qui signifie que le partage du document doit se limiter uniquement aux destinataires individuels, et qu'aucune autre divulgation n'est autorisée sauf avis favorable du propriétaire.

Ce document est privé et est uniquement déposé dans le répertoire Git de l'auteur. Merci de ne pas le diffuser, l'utiliser ou le modifier sans autorisation.

2 Nmap Walkthrough :

2.1 Task 1 : Deploy

Aucune réponse n'est demandée pour cette partie.

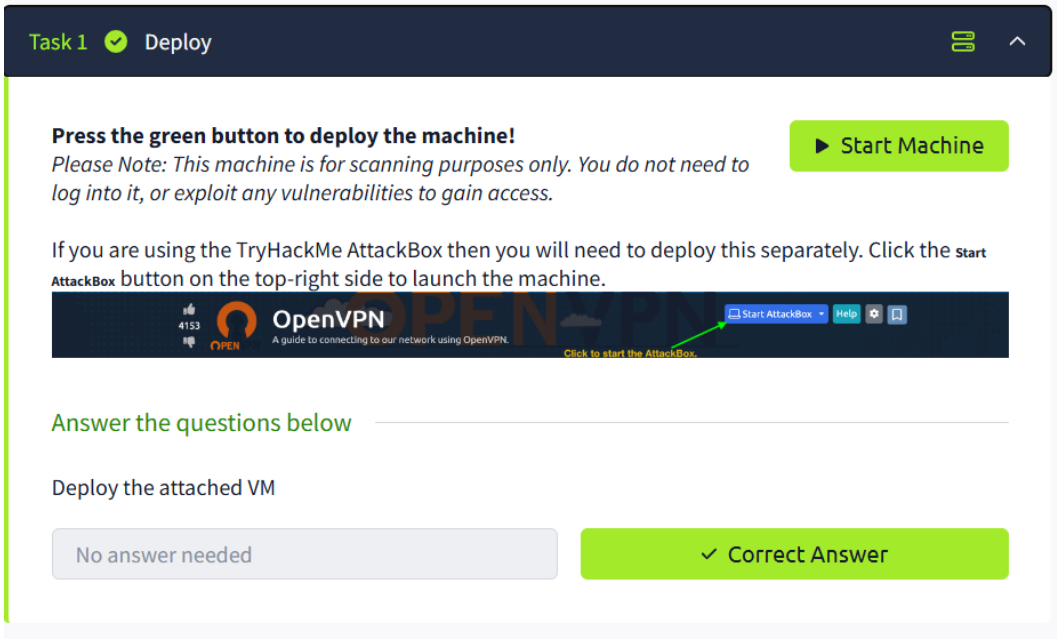


FIGURE 2.1 – Capture Task1

2.2 Task 2 : Introduction

What networking constructs are used to direct traffic to the right application on a server ?

$\Longrightarrow$ La réponse est les **ports**.
Chaque application écoute généralement sur un port spécifique (e.g. port 80 pour HTTP, 443 pour HTTPS, etc.). L'adresse IP permet de localiser le serveur, tandis que le port dirige le trafic vers l'application spécifique.

How many of these are available on any network-enabled computer ?

$\Longrightarrow$ La réponse est **65535**.
Pourquoi ? Parce que chaque port est représenté par un nombre codé sur 16 bits en binaire. Et, avec 16 bits, on a 2^{16} ports disponibles, de 0 à 65535.

[Research] How many of these are considered "well-known" ? (These are the "standard" numbers mentioned in the task)

$\Longrightarrow$ La réponse est **1024**.
Les 1024 premiers ports (de 0 à 1024) sont appelés les ports « bien connus « (Well-Known Ports). Ils sont utilisés par les services standards comme HTTP, HTTPS, FTP, etc.
Sinon, il y a aussi les ports dit « enregistrés » ou en anglais « Registered Ports ». Les numéros de ports sont entre 1024 à 49151. C'est pour les applications utilisateur spécifiques (e.g. applications locales comme BDD ou les WEB). Et enfin, les ports « dynamiques ou privés » ou en anglais « Dynamic/Private Ports ». Ils sont utilisés pour les connexions temporaires, e.g. connexion de messagerie et sont attribués dynamiquement par le système. [Rechercher comment ils sont attribués dynamiquement par le système, fait par la pile TCP/IP ?]

2.3 Task 3 : Nmap Switches

What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!) ?

$\Longrightarrow$ La réponse est **-sS**.

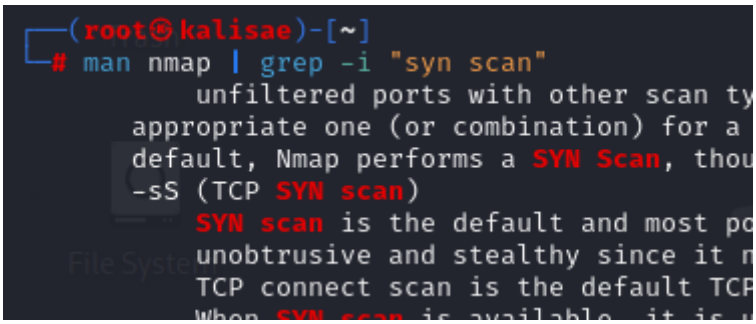


FIGURE 2.2 – Capture option -sS nmap

Remarque : Un Syn Scan est aussi appelé scan half-open ou scan stealth. C'est pour tester l'ouverture des ports mais sans faire l'handshake TCP entièrement.

Which switch would you use for a "UDP scan"?

$\Longrightarrow$ La réponse est **-sU**.

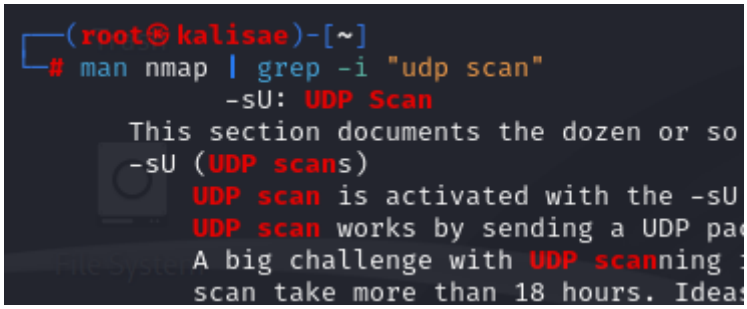


FIGURE 2.3 – Capture option -sU nmap

Remarque : Le scan UDP est plus dur que le scan TCP. Logique car UDP est un protocole sans connexion, il n'y a pas de réponse directe pour confirmer l'ouverture d'un port, comme c'est le cas avec TCP. Du coup, pour le scan UDP, il envoie certes des paquets UDP et il attend des réponses ICMP (si un port est fermé), ou aucune réponse si le port est ouvert. [https://www.it-connect.fr/technique-de-scan-de-port-udp/]

If you wanted to detect which operating system the target is running on, which switch would you use ?

$\Longrightarrow$ La réponse est **-O**.

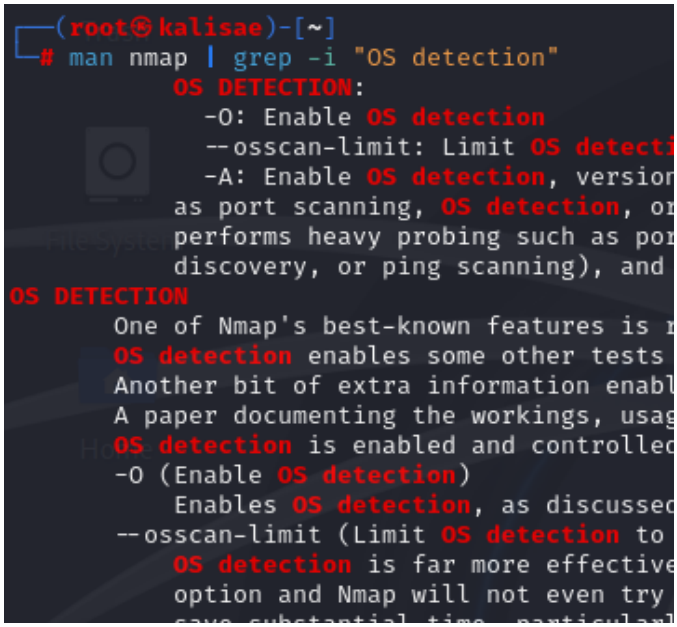


FIGURE 2.4 – Capture option -O nmap

La scan repose sur une base de données de signature d'OS (OS FingerPrinting).

Nmap provides a switch to detect the version of the services running on the target. What is this switch ?

$\Longrightarrow$ La réponse est **-sV**.

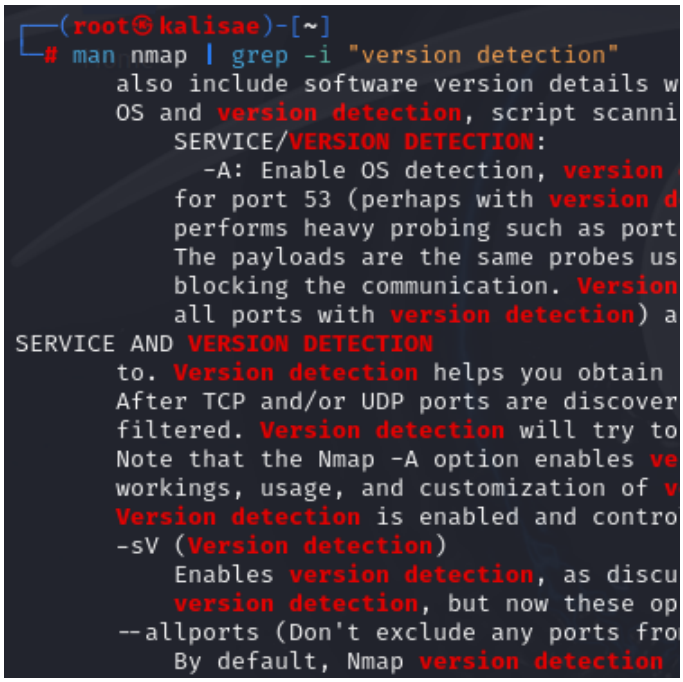


FIGURE 2.5 – Capture option -sV nmap

Ça permet d'avoir les versions par exemple d'un Apache, SSH, FTP, etc. Il (nmap) utilise une BDD pour comparer ce qu'il a obtenu, aux versions connues des services.

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity ?

$\Longrightarrow$ La réponse est **-v**.

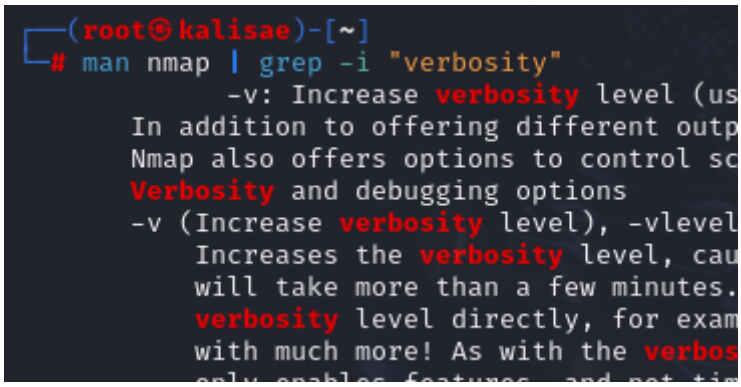


FIGURE 2.6 – Capture option -v nmap

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two ?

$\Longrightarrow$ La réponse est **-vv**.

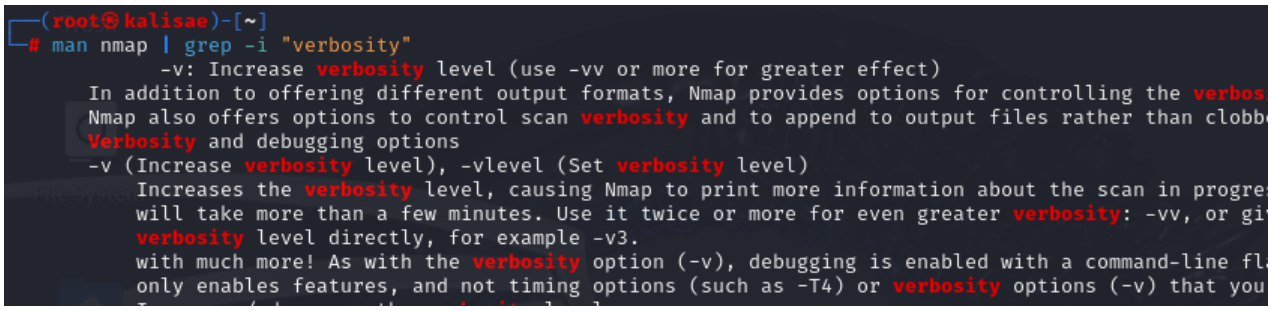


FIGURE 2.7 – Capture option -vv nmap

We should always save the output of our scans – this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.
What switch would you use to save the nmap results in three major formats ?

$\Longrightarrow$ La réponse est **-oA**.

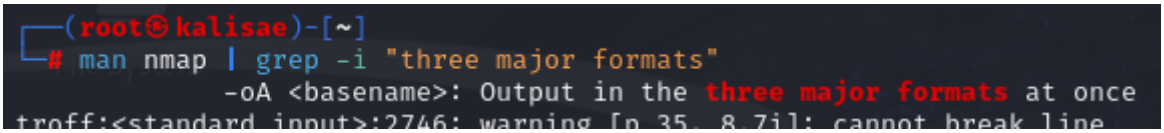


FIGURE 2.8 – Capture option -oA nmap

What switch would you use to save the nmap results in a "normal" format ?

$\Longrightarrow$ La réponse est **-oN**.

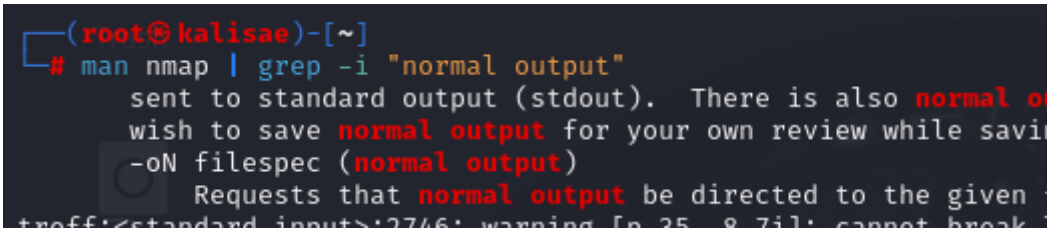


FIGURE 2.9 – Capture option -oN nmap

A very useful output format : how would you save results in a “grepable” format ?

$\Longrightarrow$ La réponse est **-oG**.

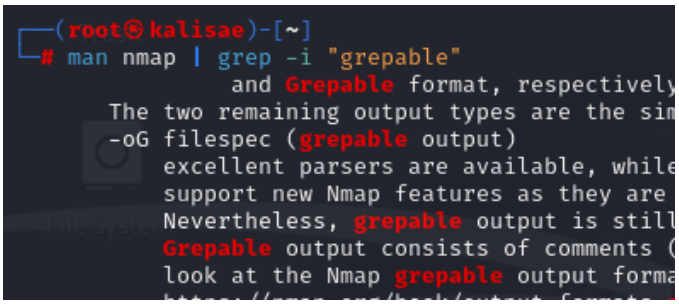


Figure 2.10 – Capture option -oG nmap

Sometimes the results we’re getting just aren’t enough. If we don’t care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning. How would you activate this setting ?

$\Longrightarrow$ La réponse est **-A**.

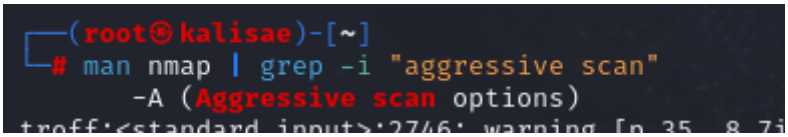


Figure 2.11 – Capture option -A nmap

[En sachant qu’il est agressif, il doit générer plus de trafic réseau ?]

Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though : higher speeds are noisier, and can incur errors !
How would you set the timing template to level 5 ?

$\Longrightarrow$ La réponse est **-T5**.

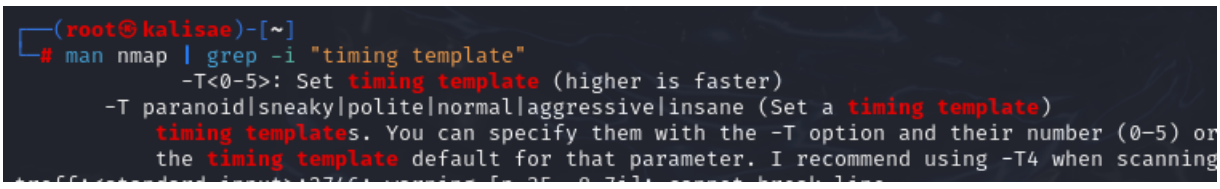


Figure 2.12 – Capture option -T5 nmap

How would you tell nmap to only scan port 80 ?

$\Longrightarrow$ La réponse est **-p 80**.

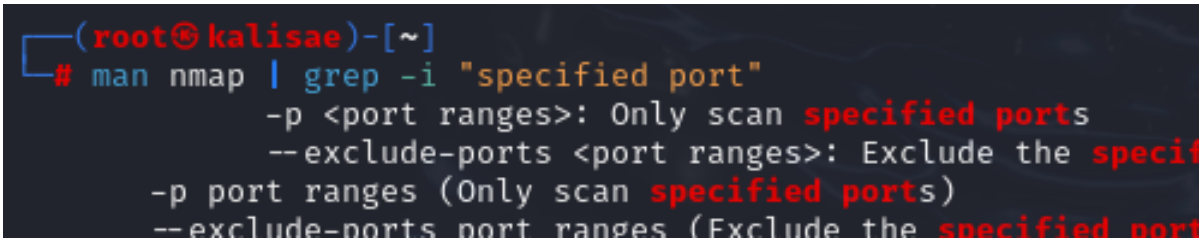


FIGURE 2.13 – Capture option -p 80 nmap

How would you tell nmap to scan ports 1000-1500 ?

$\Longrightarrow$ La réponse est **-p 1000-1500**.

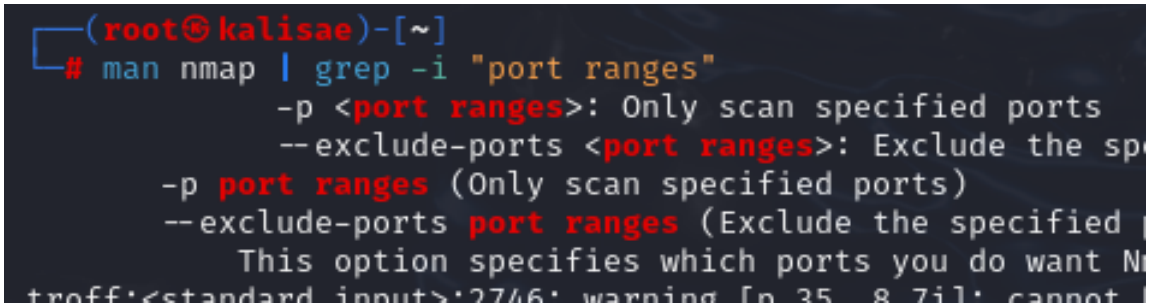


FIGURE 2.14 – Capture option -p 1000-1500 nmap

How would you tell nmap to scan all ports ?

$\Longrightarrow$ La réponse est **-p-**.

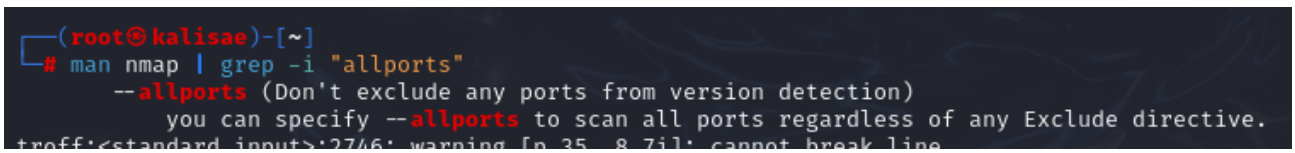


FIGURE 2.15 – Capture option -p- nmap

How would you activate a script from the nmap scripting library (lots more on this later!)?

$\Longrightarrow$ La réponse est - **-script**.

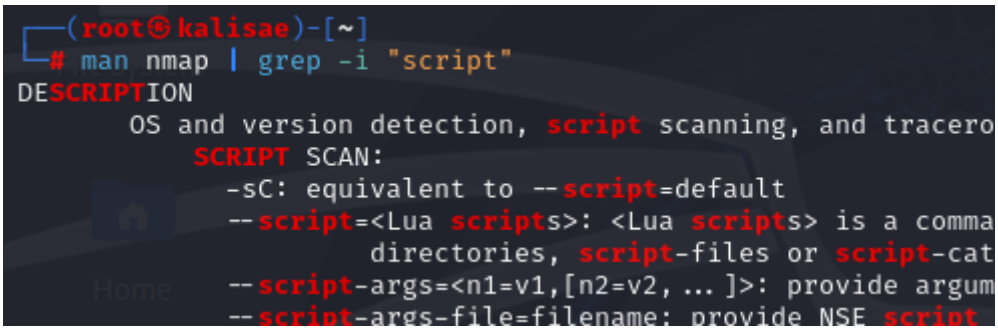


FIGURE 2.16 – Capture option - -script nmap

Nmap utilise des scripts NSE (Nmap Scripting Engine).

How would you activate all of the scripts in the "vuln" category?

$\Longrightarrow$ La réponse est - **-script=vuln**.

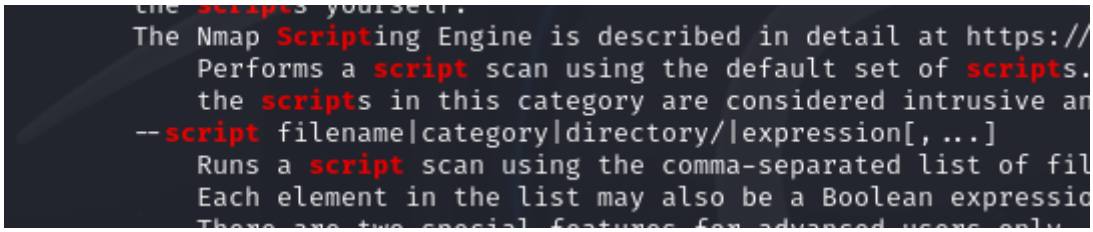


FIGURE 2.17 – Capture option –script=vuln nmap

Ça détecte par exemple les missconfigurations, les services non sécurisés, etc. Cf voir https://nmap.org/nsedoc/

2.4 Task 4 : Overview

Aucune réponse n'est demandée pour cette partie.

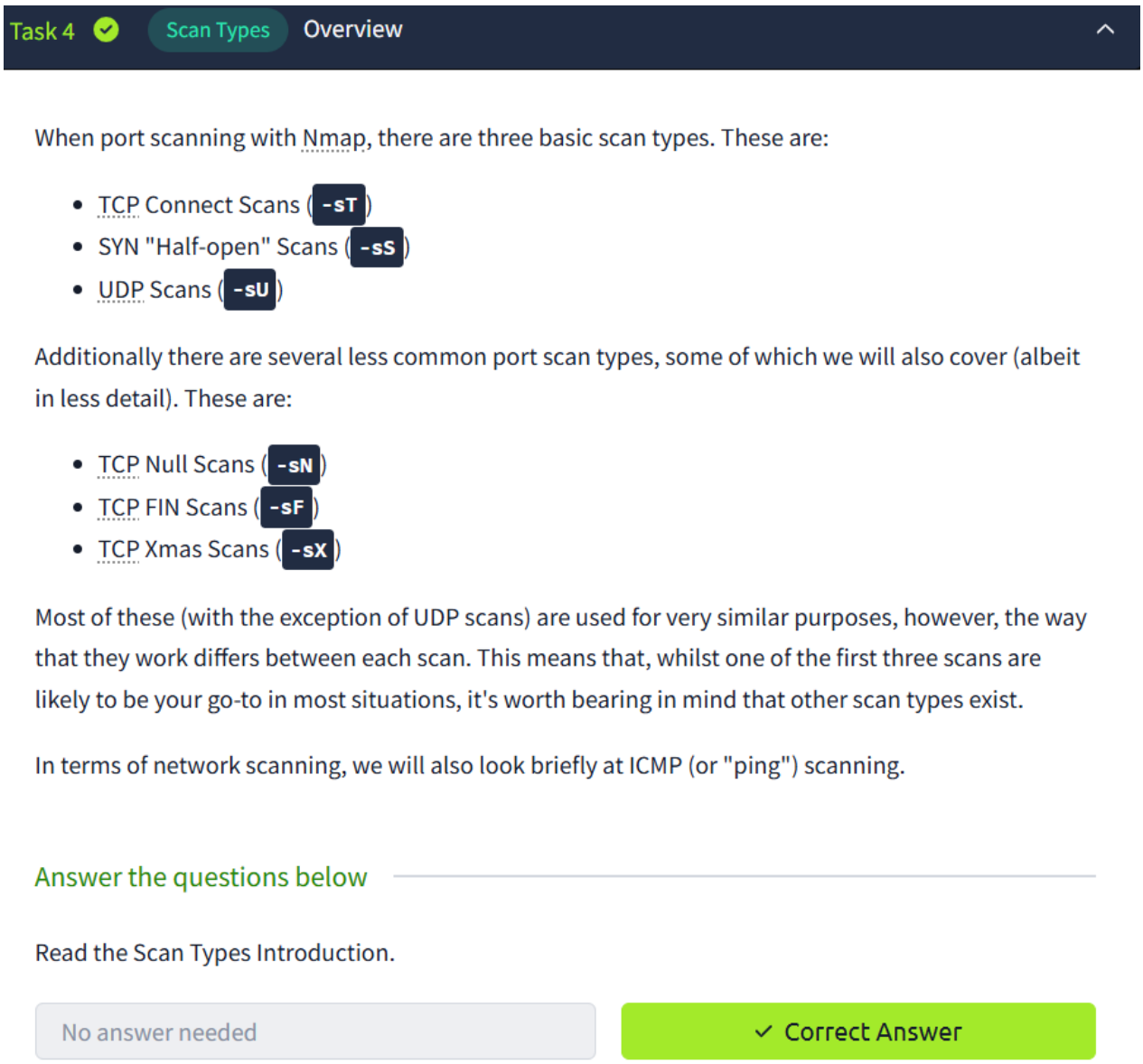


FIGURE 2.18 – Capture Task1

2.5 Task 5 : TCP Connect Scans

Which RFC defines the appropriate behaviour for the TCP protocol ?

$\Longrightarrow$ La réponse est **RFC9293**.

Elle est intitulée « Transmission Control Protocol (TCP) Specification ». Avant, il y avait la RFC 793 mais du coup la 9293 est la nouvelle version (publiée en 2022)

If a port is closed, which flag should the server send back to indicate this ?

$\Longrightarrow$ La réponse est **RST**.

Pour comprendre, quand un port est fermé, il reçoit (bien souvent je pense) un paquet SYN pour la tentative de connexion TCP. L'hôte (sur lequel la tentative de connexion a eu lieu) répondra avec un paquet TCP contenant le flag RST pour ReSeT pour dire qu'il n'y a pas de service qui tourne sur ce port.

2.6 Task 6 : SYN Scans

There are two other names for a SYN scan, what are they ?

$\Longrightarrow$ Les deux réponses sont **Half-Open et Stealth**.

Pourquoi Half-Open ? Parce que, dans un SYN scan, la connexion n'est pas établie : envoie d'un paquet SYN par le client pour l'initialisation de la connexion et si le port est ouvert, le serveur répond par un SYN-ACK. Et, au lieu de finir l'handshake TCP avec un ACK, le client envoie un RST pour interrompre le processus de connexion. Donc, c'est « à moitié ouvert ».
Pourquoi Stealth scan ? Parce que, à l'instart d'Half-Open, la connexion n'est jamais totalement établie. [Selon moi, le scan est donc plus discret.] D'où Stealth pour « furtivité ».

Can Nmap use a SYN scan without Sudo permissions (Y/N) ?

$\Longrightarrow$ La réponse est **N**.

Nmap ne peut pas utiliser un SYN scan sans permissions sudo ou sans être exécuté en tant que root.

2.7 Task 7 : UDP Scans

If a UDP port doesn't respond to an Nmap scan, what will it be marked as ?

$\Longrightarrow$ La réponse est **open|filtered**.

Si un port UDP ne répond pas à un scan Nmap, il sera marqué comme "open|filtered". UDP n'a pas d'accusé de réception contrairement à TCP.

When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so ?

$\Longrightarrow$ La réponse est **ICMP**.

La cible renvoie un message « Port unreachable »avec le protocole ICMP. ICMP Destination Unreachable (code 3)

2.8 Task 8 : NULL, FIN and Xmas

Which of the three shown scan types uses the URG flag ?

$\Longrightarrow$ La réponse est **xmas**.

Un Xmas scan est un type de scan TCP où les flags URG, PUSH et FIN sont activés simultanément.

Remarque : Xmas comme dans un arbre de Noël car les trois flags sont allumés (un peu comme des décorations de Noël)

Why are NULL, FIN and Xmas scans generally used ?

$\Longrightarrow$ La réponse est **Firewall Evasion**.

Pour comprendre, ce sont des scans dont l'objectif est d'éviter la détection par les firewall [et IDS/IPS je suppose].

Pour le scan NULL, le but est d'envoyer des paquets TCP sans aucun flag et certain firewall ne traite pas correctement ce type de paquet car il n'y a pas de flags de connexion.

Pour le scan FIN, le but est d'envoyer un paquet avec un flag FIN activé (= connexion TCP doit être fermée). De ce fait, si un port est ouvert, il n'y a souvent pas de réponse ou une réponse non détectée [je suppose aussi, à creuser] mais le but est de bypasser les rules du firewall.

Pour le scan Xmas, le but est d'envoyer un paquet avec les flags URG, PUSH et FIN pour avoir un paquet TCP inhabituel. C'est un type de paquet « étrange », pas commun. Même stratégie que le scan FIN, si un port est ouvert, il n'y a souvent pas de réponse ou une réponse non détectée [je suppose aussi, à creuser] mais le but est de bypasser les rules du firewall.

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port ?

$\Longrightarrow$ La réponse est **Microsoft Windows**.

Le SE Microsoft Windows (et aussi de nombreux appareils réseau Cisco) répondent avec un RST à tous les paquets TCP « étrange » que le port soit ouvert ou fermé. Donc, tous les ports apparaissent comme fermés [faux positifs ?].

2.9 Task 9 : ICMP Network Scanning

How would you perform a ping sweep on the 172.16.x.x network (Netmask : 255.255.0.0) using Nmap ? (CIDR notation)

$\Longrightarrow$ La réponse est **nmap -sn 172.160.0.0/16**.

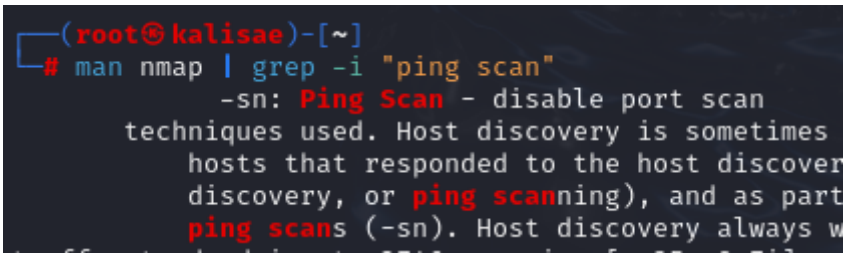


FIGURE 2.19 – Commande nmap sweet ping

L'option « -sn » permet de faire un scan de découverte. Et, dans l'exemple suivant de 172.16.0.0 à 172.16.255.255. Le scan envoie des paquets ICMP Echo Request pour connaître les hôtes actifs.

2.10 Task 10 : Overview

What language are NSE scripts written in ?

$\Longrightarrow$ La réponse est **Lua**.

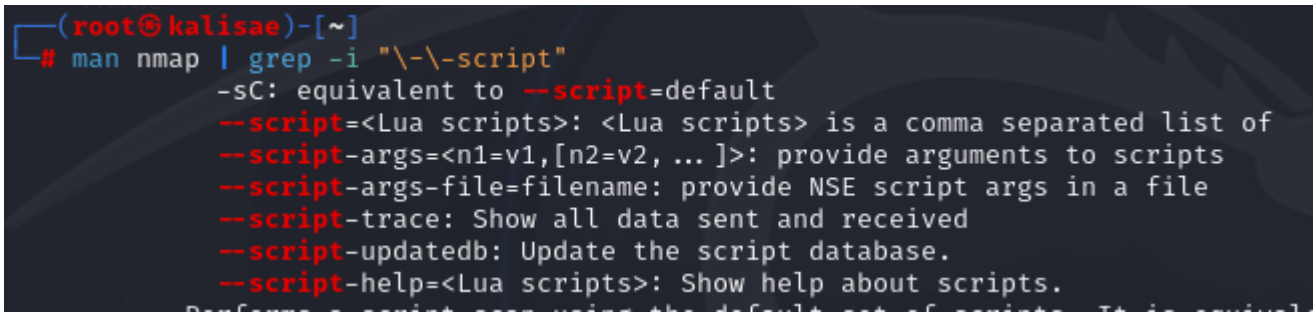


FIGURE 2.20 – Langage des scripts NSE

Tous les scripts NSE se trouvent dans le répertoire suivant : « /usr/share/nmap/scripts ».

```
┌──(root㉿kalisae)-[~]
└─# ls -alhk /usr/share/nmap/scripts/
total 4.9M
drwxr-xr-x 2 root root  36K Feb  3  2024 .
drwxr-xr-x 4 root root 4.0K Feb  3  2024 ..
-rw-r--r-- 1 root root 3.9K Nov  2  2023 acarsd-info.nse
-rw-r--r-- 1 root root 8.6K Nov  2  2023 address-info.nse
-rw-r--r-- 1 root root 3.3K Nov  2  2023 afp-brute.nse
-rw-r--r-- 1 root root 6.4K Nov  2  2023 afp-ls.nse
-rw-r--r-- 1 root root 6.9K Nov  2  2023 afp-path-vuln.nse
-rw-r--r-- 1 root root 5.5K Nov  2  2023 afp-serverinfo.nse
-rw-r--r-- 1 root root 2.6K Nov  2  2023 afp-showmount.nse
-rw-r--r-- 1 root root 2.3K Nov  2  2023 ajp-auth.nse
```

FIGURE 2.21 – Répertoire des scripts NSE

Which category of scripts would be a very bad idea to run in a production environment ?

$\Longrightarrow$ La réponse est **intrusive**.

C'est une mauvaise idée car les scripts peuvent affecter les services, type interruptions ou ralentissements. Les scripts NSE sont marqués s'ils sont intrusifs ou non avec « brute » dans le nom du script.

```
┌──(root㉿kalisae)-[~]
└─# ll /usr/share/nmap/scripts/ | grep "brute"
-rw-r--r-- 1 root root  3345 Nov  2  2023 afp-brute.nse
-rw-r--r-- 1 root root  2983 Nov  2  2023 ajp-brute.nse
-rw-r--r-- 1 root root  9050 Nov  2  2023 backorifice-brute.nse
-rw-r--r-- 1 root root  3742 Nov  2  2023 cassandra-brute.nse
-rw-r--r-- 1 root root 11113 Nov  2  2023 cics-user-brute.nse
-rw-r--r-- 1 root root  4749 Nov  2  2023 citrix-brute-xml.nse
-rw-r--r-- 1 root root  3879 Nov  2  2023 cvs-brute-repository.nse
-rw-r--r-- 1 root root  2948 Nov  2  2023 cvs-brute.nse
-rw-r--r-- 1 root root  4398 Nov  2  2023 deluge-rpc-brute.nse
-rw-r--r-- 1 root root  2275 Nov  2  2023 dicom-brute.nse
-rw-r--r-- 1 root root 10100 Nov  2  2023 dns-brute.nse
-rw-r--r-- 1 root root  3865 Nov  2  2023 domcon-brute.nse
```

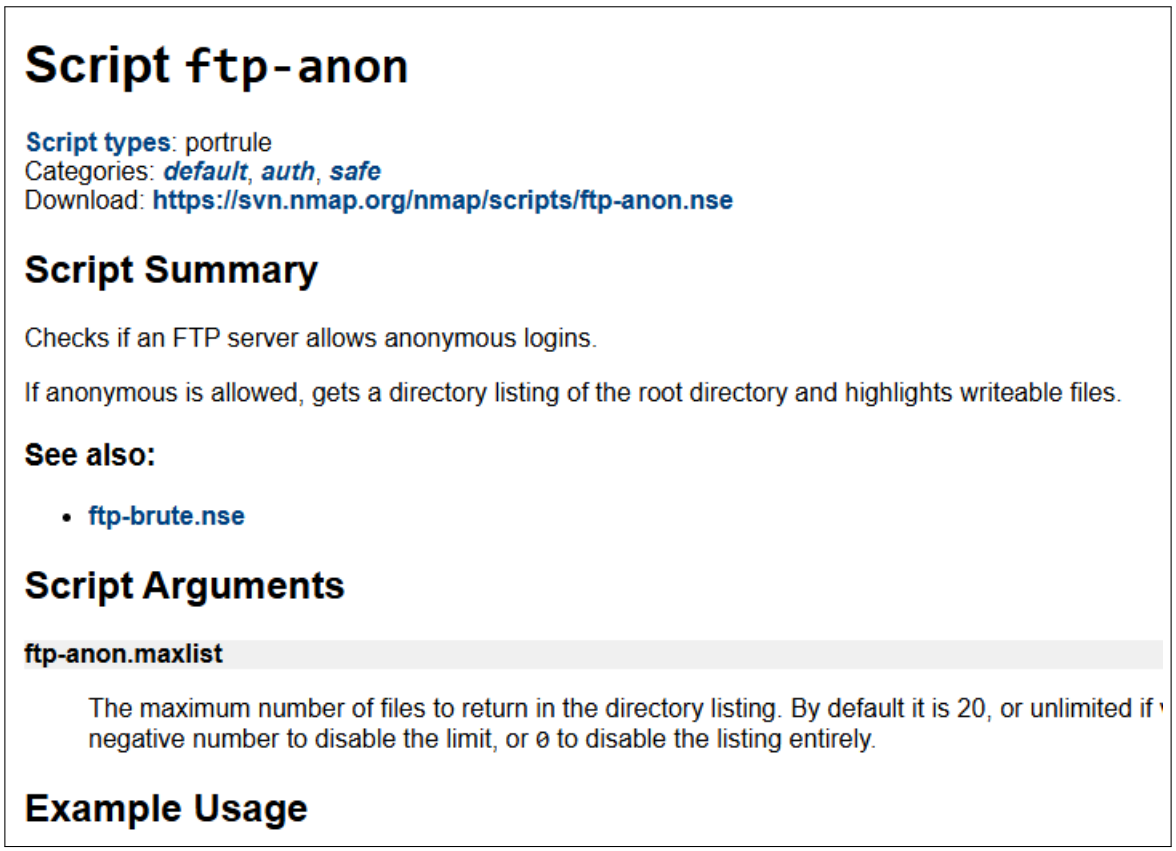
FIGURE 2.22 – Scripts de catégorie intrusif

2.11 Task 11 : Working with the NSE

What optional argument can the ftp-anon.nse script take ?

$\Longrightarrow$ La réponse est **maxlist**.

Capture de : https://nmap.org/nsedoc/scripts/ftp-anon.html :



Script ftp-anon

Script types: portrule
Categories: ***default***, ***auth***, ***safe***
Download: **https://svn.nmap.org/nmap/scripts/ftp-anon.nse**

Script Summary

Checks if an FTP server allows anonymous logins.

If anonymous is allowed, gets a directory listing of the root directory and highlights writeable files.

See also:

- **ftp-brute.nse**

Script Arguments

ftp-anon.maxlist

The maximum number of files to return in the directory listing. By default it is 20, or unlimited if
negative number to disable the limit, or 0 to disable the listing entirely.

Example Usage

FIGURE 2.23 – Argument ftp-anon.nse

L'argument spécifie le nombre maximal de fichiers à retourner dans la liste de répertoires obtenue par le script. La valeur par défaut est de 20 fichiers et si la verbosité est activée, la limite est supprimée.

2.12 Task 12 : Searching for Scripts

What is the filename of the script which determines the underlying OS of the SMB server ?

$\Longrightarrow$ La réponse est **smb-os-discovery.nse**.

```
┌──(root㉿kalisae)-[~]
└─# ll /usr/share/nmap/scripts/ | grep -Ei "smb.*os"
-rw-r--r-- 1 root root  8220 Nov  2  2023 smb-os-discovery.nse
-rw-r--r-- 1 root root  4400 Nov  2  2023 smb-vuln-regsvc-dos.nse
```

FIGURE 2.24 – Script NSE smb-os-discovery

Ce script permet de récupérer le SE d'un serveur SMB. Par curiosité, en aiguillant le code, le script tente de récupérer sur le port 139 et/ou 445 l'OS, le nom de l'ordinateur, du domaine, le FQDN, le nom et domaine NetBIOS de l'ordinateur, le nom du

groupe de travail, l'heure système, etc. Il (le script) utilise un compte anonyme ou valide pour établir la session et obtenir ces informations en réponse à la connexion SMB.

Read through this script. What does it depend on ?

$\Longrightarrow$ La réponse est **smb-brute**.

```
┌──(root㉿kalisae)-[~]
└─# grep -i "depend" /usr/share/nmap/scripts/smb-os-discovery.nse
The following fields may be included in the output, depending on the
dependencies = {"smb-brute"}
```

FIGURE 2.25 – Dépendance du script smb-brute

Le script smb-brute permet de tester les mots de passe sur les services SMB. C'est un script de brute force.

2.13 Task 13 : Firewall Evasion

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch ?

$\Longrightarrow$ La réponse est **ICMP**.

```
┌──(root㉿kalisae)-[~]
└─# lang=en man nmap | grep "\-Pn"
           -Pn: Treat all hosts as online -- skip host discovery
           nmap -v -iR 10000 -Pn -p 80
         bored one rainy afternoon, try the command nmap -Pn -sS -p
      with a list scan (-sL) or by disabling host discovery (-Pn), c
      about the -sn option to learn how to perform only host discove
         host discovery while still performing such higher level fu
      -Pn (No ping)
         found to be up. Disabling host discovery with -Pn causes N
         options -Pn -sn together.
         hosts. In previous versions of Nmap, -Pn was -P0 and -PN.
```

FIGURE 2.26 – Capture option -Pn nmap

Nmap n'effectuera pas de découverte d'hôte à l'aide ICMP avec l'option -Pn. Les firewall bloquent le trafic ICMP pour empêcher la découverte de réseau [ou pour rendre les hôtes invisibles].

Which Nmap switch allows you to append an arbitrary length of random data to the end of packets ?

$\Longrightarrow$ La réponse est - **-data-lengh**.

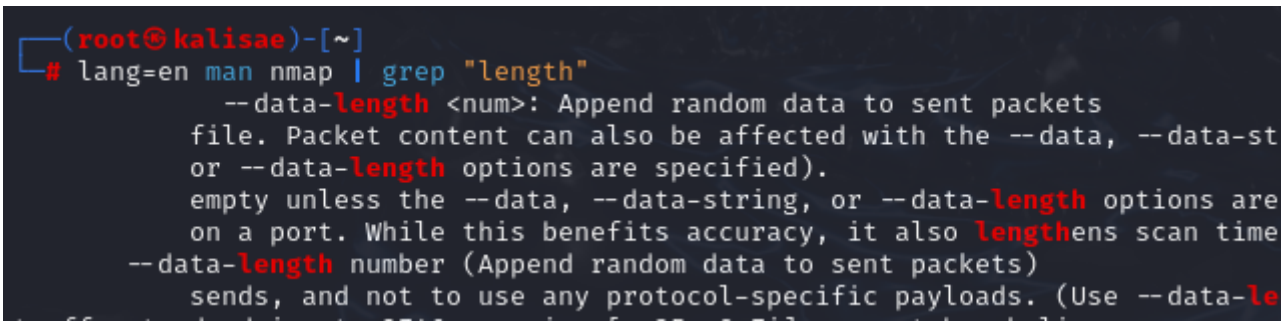


FIGURE 2.27 – Capture option - -length nmap

Ça permet d'ajouter des « paddings » à la fin des paquets envoyés. [Je suppose que c'est pour échapper à la détection par des IDS/IPS]. Je pense aussi que les paddings peuvent masquer la nature du scan.

2.14 Task 14 : Practical

Does the target IP respond to ICMP echo (ping) requests (Y/N) ?

$\Longrightarrow$ La réponse est **N**.

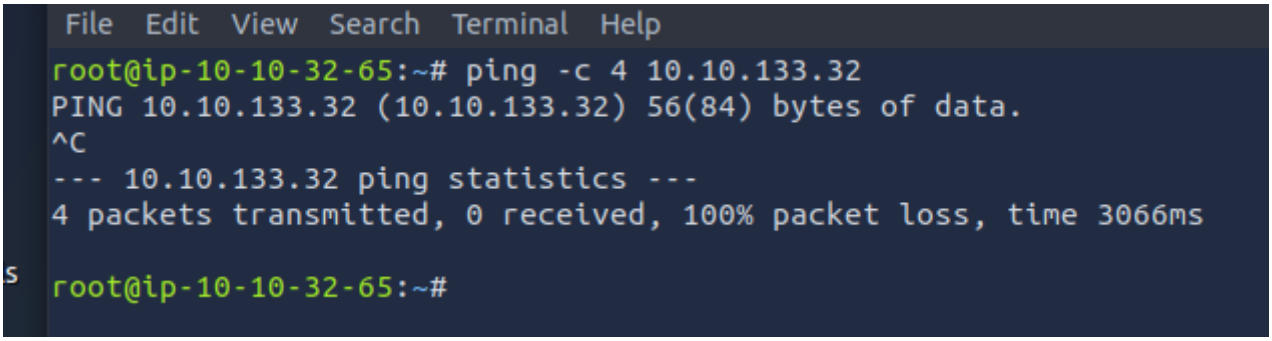


FIGURE 2.28 – La cible ne répond pas au ping

Perform an Xmas scan on the first 999 ports of the target — how many ports are shown to be open or filtered ?

$\Longrightarrow$ La réponse est **999**.

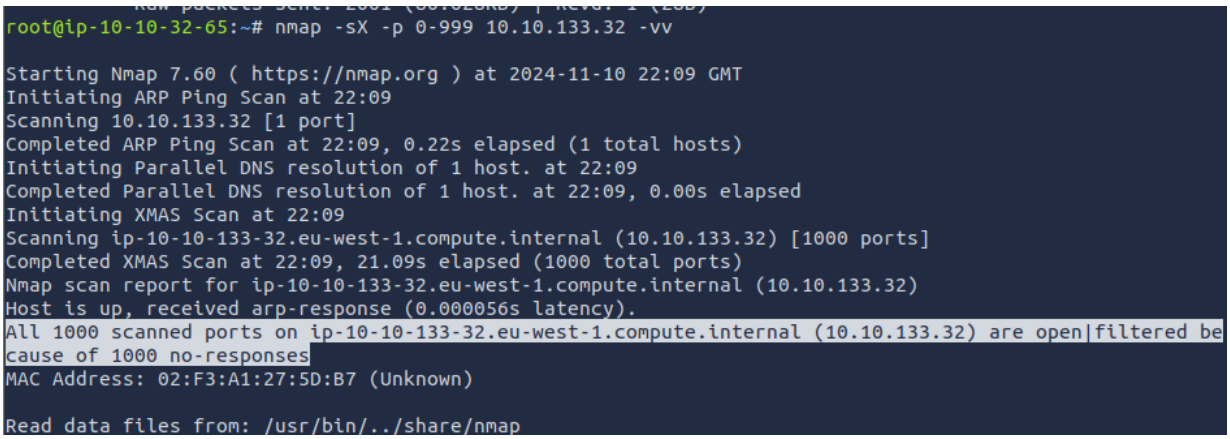


FIGURE 2.29 – Résultat scan Xmas nmap

Il n'y a pas eu de réponse sur les ports. Les ports sont soit ouverts ou soit filtrés (protégé par un firewall).

There is a reason given for this — what is it ?

$\Longrightarrow$ La réponse est **no response**.

Ici, tous les ports sont marqués « open|filtered », cela signifie que nmap n'a pas reçu de réponse. Comme dit au-dessus, pour qu'un port soit marqué comme ouvert, nmap s'attend à recevoir une connexion ou un accusé de réception (e.g. handshake TCP)

Perform a TCP SYN scan on the first 5000 ports of the target — how many ports are shown to be open ?

$\Longrightarrow$ La réponse est **5**.

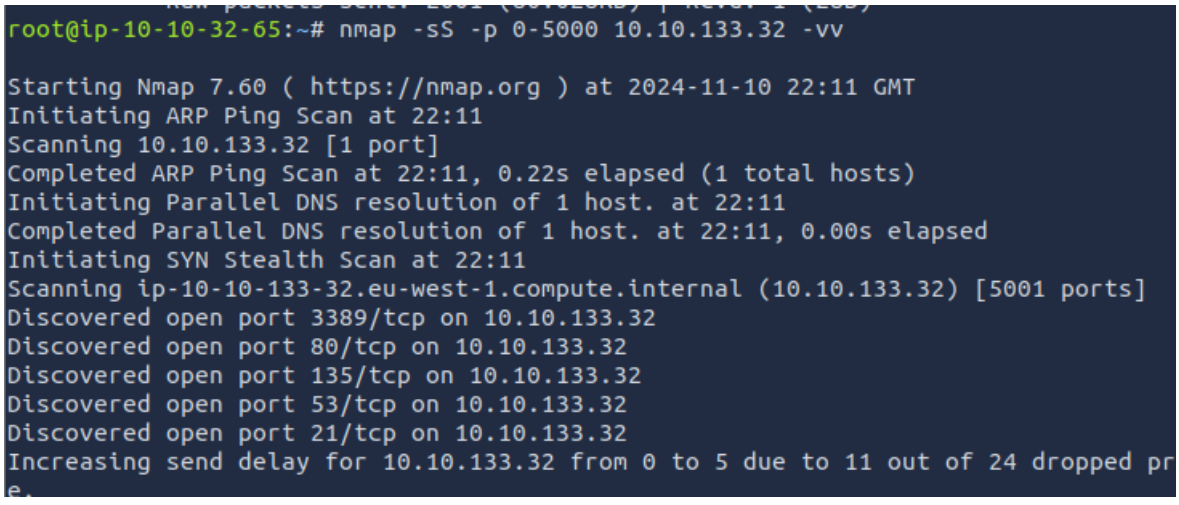


FIGURE 2.30 – Résultat scan des 5000 premiers ports nmap (scan SYN)

Après l'analyse TCP SYN sur les 5000 premiers ports de la cible, il y a 5 ports ouverts : 21 (FTP), 53 (DNS), 80 (HTTP), 135 (RPC) et 3389 (RDP).

Can Nmap login successfully to the FTP server on port 21 ? (Y/N)

$\Longrightarrow$ La réponse est **Y**.

```
Nmap done: 1 IP address (0 hosts up) scanned in 0.85 seconds
root@ip-10-10-32-65:~# nmap --script=ftp-anon -p 21 10.10.93.178

Starting Nmap 7.60 ( https://nmap.org ) at 2024-11-10 22:32 GMT
Nmap scan report for ip-10-10-93-178.eu-west-1.compute.internal (10.10.93.178)
Host is up (0.00038s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 02:4E:30:13:11:2D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
root@ip-10-10-32-65:~# ftp 10.10.93.178
Connected to 10.10.93.178.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (10.10.93.178:root): ^Croot@ip-10-10-32-65:~#
```

FIGURE 2.31 – Résultat scan avec script NSE ftp-anon

Remarque : @IP cible différente dans la capture car partie refaite.

2.15 Task 15 : Conclusion

Aucune réponse n'est demandée pour cette partie.

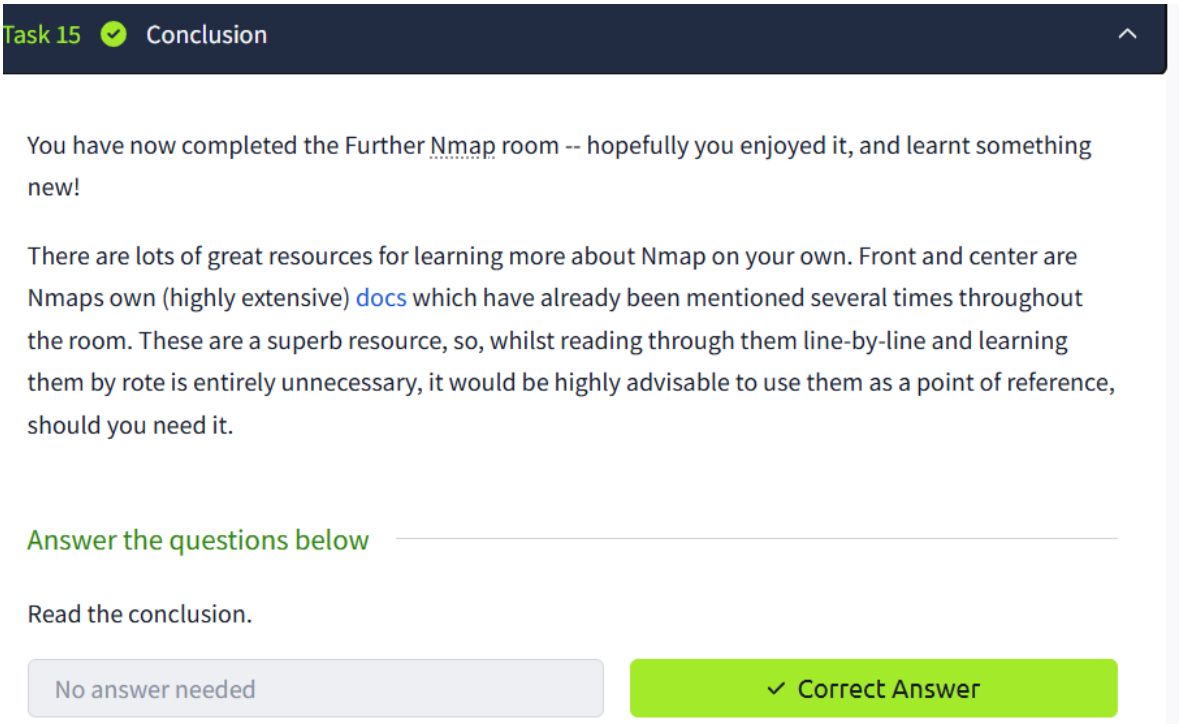


FIGURE 2.32 – Capture Task15

3 Conclusion :

Ce challenge TryHackMe a permis d'avoir des notions autour de l'outil nmap. J'ai pu découvrir/revoir les différents types de scans disponibles, tels que les SYN scans, UDP scans, NULL scans, FIN scans, Xmas scans, etc. Chaque scan a des objectifs et des techniques différentes pour l'analyse. J'ai également appris à utiliser les scripts NSE pour cibler une catégorie de scan et un service en particulier.

Fin du rapport.

Rapport écrit par Nathan Martel du 08/11/2024 au 11/11/2024.
Correction le 21/11/2024
Version : v1.1

Outils utilisés : VM TryHackMe et VM Kali Linux

Logiciel utilisé : Texworks
Langage et systèmes de composition : LaTeX
Console : MiKTeX
Format du document : PDF

Table des figures