

TD1: nmap

La room "Further Nmap" sur TryHackMe permet d'approfondir l'usage avancé de Nmap.

Voici les captures d'écrans des réponses à apporter sur la room :

Task 2 : introduction :

Answer the questions below

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

Ports

✓ Correct Answer

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

65535

✓ Correct Answer

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

1024

✓ Correct Answer

🔍 Hint

Task 3 : Nmap switches :

Answer the questions below

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

-sS

✓ Correct Answer

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

-sU

✓ Correct Answer

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

-O

✓ Correct Answer

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

-sV

✓ Correct Answer

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

-v

✓ Correct Answer

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

(Note: it's highly advisable to always use *at least* this option)

-vv

✓ Correct Answer

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?

-oA

✓ Correct Answer

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

-oN

✓ Correct Answer

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

-oG

✓ Correct Answer

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?

-A

✓ Correct Answer

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?

-T5

✓ Correct Answer

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

-p 80

✓ Correct Answer

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

-p 1000-1500

✓ Correct Answer

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

-p-

✓ Correct Answer

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

--script

✓ Correct Answer

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

--script=vuln

✓ Correct Answer

🔍 Hint

Task 5 : TCP connect scans :

Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 9293

✓ Correct Answer

🔍 Hint

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

RST

✓ Correct Answer

Task 6 : Syn scan :

Answer the questions below

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

Half-Open, Stealth

✓ Correct Answer

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

N

✓ Correct Answer

Task 7 : UDP scans :

Answer the questions below

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

open|filtered

✓ Correct Answer

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?

ICMP

✓ Correct Answer

Task 8 : NULL FIN XMAS

Answer the questions below

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

xmas

✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion

✓ Correct Answer

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

Microsoft Windows

✓ Correct Answer

Task 9 : ICMP network scanning

Answer the questions below

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

nmap -sn 172.16.0.0/16

✓ Correct Answer

🔍 Hint

Task 11 : working with the NSE

Answer the questions below

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

maxlist

✓ Correct Answer

Task 12 : Searching for scripts

Answer the questions below

Search for "smb" scripts in the `/usr/share/nmap/scripts/` directory using either of the demonstrated methods.
What is the filename of the script which determines the underlying OS of the SMB server?

smb-os-discovery.nse

✓ Correct Answer

Read through this script. What does it depend on?

smb-brute

✓ Correct Answer

🔍 Hint

Task 13 : Firewall Evasion

Answer the questions below

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

ICMP

✓ Correct Answer

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

--data-length

✓ Correct Answer

Task 14 : Practical :

Answer the questions below

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

N

✓ Correct Answer

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

999

✓ Correct Answer

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

Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

No Response

✓ Correct Answer

🔗 Hint

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

5

✓ Correct Answer

Open Wireshark (see [Cryillic's Wireshark Room](#) for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y

✓ Correct Answer

Explication des cas pratiques : task14 :

XMAS :

Avec la commande `nmap -sX -p1-999`, on a scanné les 999 premiers ports. Tous apparaissent comme "ouverts ou filtrés", ce qui signifie qu'aucune réponse claire n'est reçue.

TCP SYN :

En utilisant `nmap -sS -p1-5000`, on a détecté que 5 ports parmi les 5000 premiers sont ouverts. Ce scan rapide permet d'identifier les ports accessibles sans établir de connexion complète.

FTP PORT :

En utilisant le script `ftp-anon` avec la commande `nmap --script ftp-anon -p21`, on a vérifié l'accès FTP sur le port 21. Le serveur permet les connexions anonymes, ce qui signifie qu'il est possible de se connecter sans authentification.