

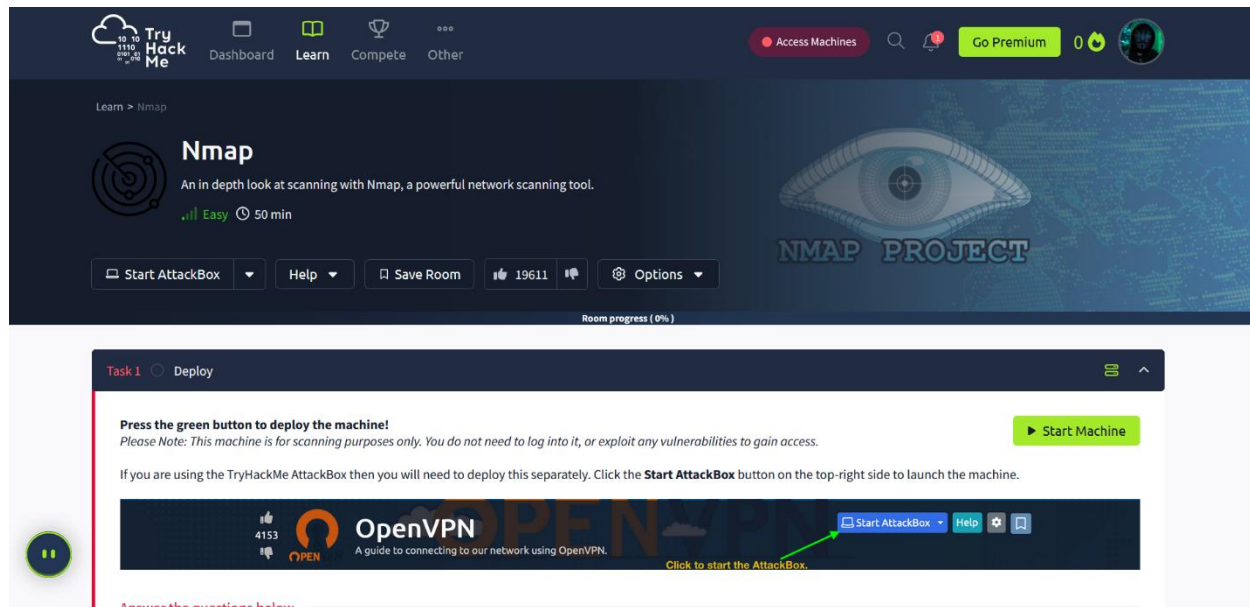
Task 3: Report on Further Nmap

Date: 08/08/2025

Prepared for: MuLearn Bootcamp

Prepared By: Atul H

This is my writeup for the further nmap room assigned as task 3 from Try Hack Me.

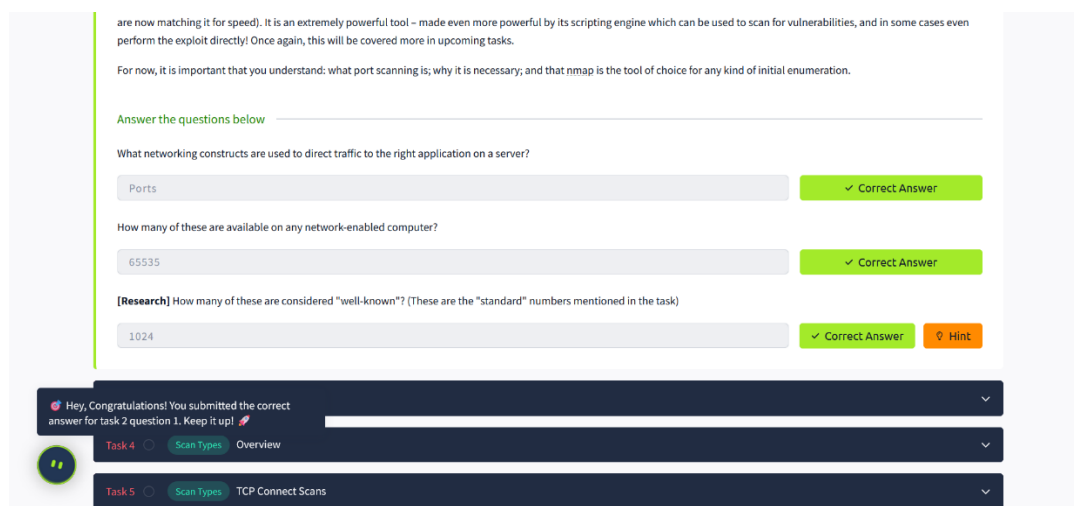
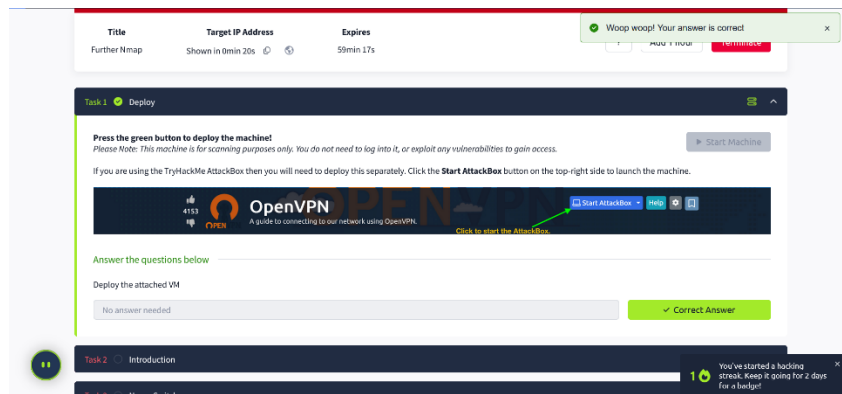


First we start this room and the attack-box of Try Hack Me.

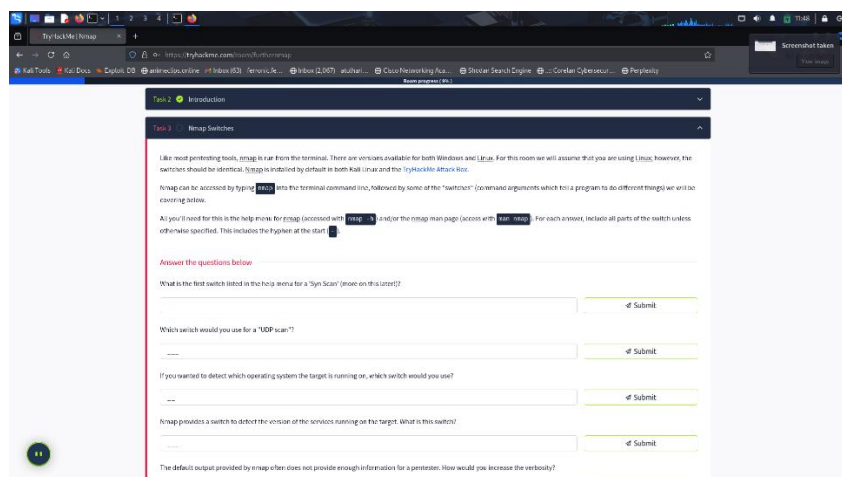
Introduction to nmap:

Nmap, short for Network Mapper, is a free and open-source network scanning tool used for network discovery and security auditing. It's primarily used to identify hosts, services, and open ports on a network, making it valuable for both security professionals and network administrators.

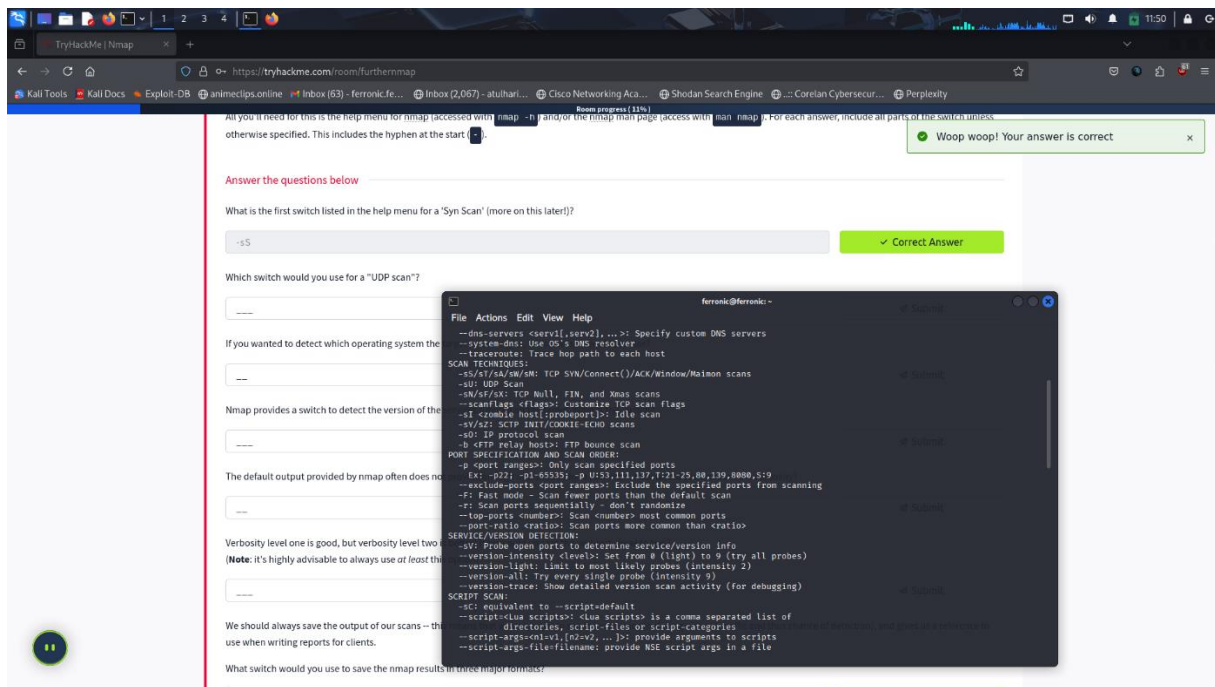
The first task mentioned is to deploy the machine. It will be completed after we deploy the machine and click completed.



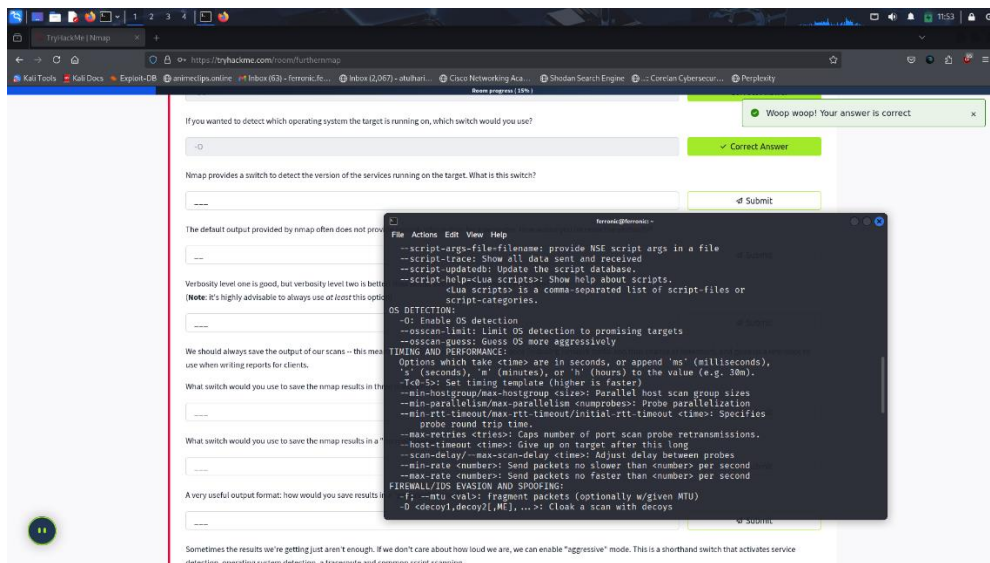
Task 2 of this room was an introduction, in which it clearly states all the answers to the questions asked. It introduces of Nmap and its uses, also hinting towards the port details.



Moving on to task 3, it describes about the switches of nmap. When we do the nmap -h we get:



From this we know the first 2 answers, for Syn Scan `-sS` and for a UDP scan it is `-sU`.



The next question describes the OS detection method. For that we use `-O` in nmap.

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 client.

Verbosity level one is good, but verbosity level two is better.

(Note: it's highly advisable to always use *at least* this option when writing reports for clients.)

We should always save the output of our scans -- this means 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 the terminal?

What switch would you use to save the nmap results in a file?

```
File Actions Edit View Help
How would you increase the verbosity?
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
  directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
```

-sV is used for version scan.

The default output provided by nmap often does not provide enough information for a client.

-v

Verbosity level one is good, but verbosity level two is better.

(Note: it's highly advisable to always use *at least* this option when writing reports for clients.)

-vv

We should always save the output of our scans -- this means 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 the terminal?

What switch would you use to save the nmap results in a file?

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

```
File Actions Edit View Help
How would you increase the verbosity?
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spooft-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|c|t|p|k|d|i|3,
  and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
```

-v is used for increasing the verbosity level. -vv for more greater effect.

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 the terminal?

-oA

What switch would you use to save the nmap results in a file?

-oN

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

Sometimes the results we're getting just aren't enough. If we want to see more information about the target, we can use the --script-args-file switch to provide arguments to scripts.

How would you activate this setting?

```
File Actions Edit View Help
How would you increase the verbosity?
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spooft-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|c|t|p|k|d|i|3,
  and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
```

-oA is used to get the outputs of nmap in 3 major formats at once. -oN is used for a normal scan.

-oN

Correct Answer

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

-oG

Sometimes the results we're getting just aren't enough. If we use the -oG option, we can get a more detailed output that includes host detection, operating system detection, a traceroute and a list of open ports.

How would you activate this setting?

-A

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?

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

```

File Actions Edit View Help
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
  
```

-oG is used to save the details in a greppable format. It is also considered to be very useful.

-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

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

How would you tell nmap to only scan port 80?

-p 80

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

A very useful option that should not be ignored:

How would you tell nmap to scan all ports?

```

File Actions Edit View Help
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sV/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
  
```

-p is used to define the ports for scanning the target. So if you had to scan port 1000-1500, we can use -p 1000-1500. To scan all ports, which is time consuming we use -p-.

To access the scripts from library we use --script.

TryHackMe | Nmap

https://tryhackme.com/room/furthernmap

Kali Tools | Kali Docs | Exploit-DB | online-ips.online | Inbox (63) - ferronic fe... | Inbox (2,067) - atulhari... | Cisco Networking Ac... | Shodan Search Engine | Correlation Cybersec... | Perplexity

Room progress (43%)

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 4 | Scan Types | Overview

Task 5 | Scan Types | TCP Connect Scans

Then we move on to task 4. In task 4 we are assigned to read about scan types.

Task 4 Scan Types Overview

When port scanning with Nmap, there are three basic scan types. These are:

- TCP Connect Scans (-sT)
- SYN "Half-open" Scans (-sS)
- UDP Scans (-sU)

Additionally there are several less common port scan types, some of which we will also cover (albeit in less detail). These are:

- TCP Null Scans (-sN)
- TCP FIN Scans (-sF)
- TCP Xmas Scans (-sX)

Most of these (with the exception of UDP scans) are used for very similar purposes, however, the way that they work differs between each scan. This means that, whilst one of the first three scans are likely to be your go-to in most situations, it's worth bearing in mind that other scan types exist.

In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Answer the questions below

Read the Scan Types Introduction.

No answer needed

✓ Correct Answer

Task 5 consist of reading TCP connect scans. We have answers to the questions asked in the following reading session which will briefly make us aware of the three way handshake. Introduce the SYN, ACK, SYN-ACK, RST requests.

Task 5 Scan Types SYN Scans

many firewalls are configured to simply **drop** incoming packets. nmap sends a TCP SYN request, and receives nothing back. This indicates (that the port is denied) protected by a firewall and thus the port is considered to be *filtered*.

That said, it is very easy to configure a firewall to respond with a RST TCP packet. For example, in IPTables for Linux, a simple version of the command would be as follows:

```
iptables -I INPUT -p tcp --dport <port> -j REJECT --reject-with tcp-reset
```

This can make it extremely difficult (if not impossible) to get an accurate reading of the target(s).

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

Now we completed task 5, lets move on to task 6, in which the details of SYN scan and its other names are mentioned.

Task 6 Scan Types SYN Scans

When using a SYN scan to identify closed and filtered ports, the exact same rules as with a TCP Connect scan apply.

If a port is closed then the server responds with a RST TCP packet. If the port is filtered by a firewall then the TCP SYN packet is either dropped, or spoofed with a TCP reset.

In this regard, the two scans are identical: the big difference is in how they handle open ports.

[1] SYN scans can also be made to work by giving Nmap the CAP_NET_RAW, CAP_NET_ADMIN and CAP_NET_BIND_SERVICE capabilities; however, this may not allow many of the NSE scripts to run properly.

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

Half open or stealth scan is the other terms used for SYN scan. Nmap require sudo permission for SYN scan.

When a packet is sent to an open UDP port, there should be no response. When this happens, Nmap refers to the port as being **open|filtered**. If the port is open, but it could be firewalled. If it gets a UDP response (which is very unusual), then the port is marked as **open**. More commonly there is sent a second time as a double-check. If there is still no response then the port is marked **open|filtered** and Nmap moves on.

When a packet is sent to a **closed** UDP port, the target should respond with an ICMP (ping) packet containing a message that the port is unreachable. This clearly identifies closed ports, which Nmap marks as such and moves on.

Due to this difficulty in identifying whether a UDP port is actually open, UDP scans tend to be incredibly slow in comparison to the various TCP scans (in the region of 20 minutes to scan the first 1000 ports, with a good connection). For this reason it's usually good practice to run an Nmap scan with `--top-ports <number>` enabled. For example, scanning with `nmap -sU --top-ports 20 <target>`. Will scan the top 20 most commonly used UDP ports, resulting in a much more acceptable scan time.

When scanning UDP ports, Nmap usually sends completely empty requests -- just raw UDP packets. That said, for ports which are usually occupied by well-known services, it will instead send a protocol-specific payload which is more likely to elicit a response from which a more accurate result can be drawn.

Answer the questions below

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

✓ 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?

✓ Correct Answer

Task 8 Scan Types NULL, FIN and Xmas

Task 7 consist of reading session about UDP. If a UDP port doesn't respond to Nmap scan it usually shows open|filtered. The protocols used are ICMP for the host to receive port unreachable message from the target.

The expected response for **open** ports with these scans is also identical, and is very similar to that of a UDP scan. If the port is open then the response is identical. Unfortunately (as with open UDP ports), that is also an expected behaviour if the port is protected by a firewall, so NULL, FIN and Xmas scans can be **filtered**, **closed**, or **filtered**. If a port is identified as filtered with one of these scans then it is usually because the target has responded with an ICMP unreachable packet.

It's also worth noting that while RFC 793 mandates that network hosts respond to malformed packets with a RST TCP packet for closed ports, and don't respond at all for open ports; this is not always the case in practice. In particular Microsoft Windows (and a lot of Cisco network devices) are known to respond with a RST to any malformed TCP packet -- regardless of whether the port is actually open or not. This results in all ports showing up as being closed.

That said, the goal here is, of course, firewall evasion. Many firewalls are configured to drop incoming TCP packets to blocked ports which have the SYN flag set (thus blocking new connection initiation requests). By sending requests which do not contain the SYN flag, we effectively bypass this kind of firewall. Whilst this is good in theory, most modern IDS solutions are savvy to these scan types, so don't rely on them to be 100% effective when dealing with modern systems.

Answer the questions below

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

✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

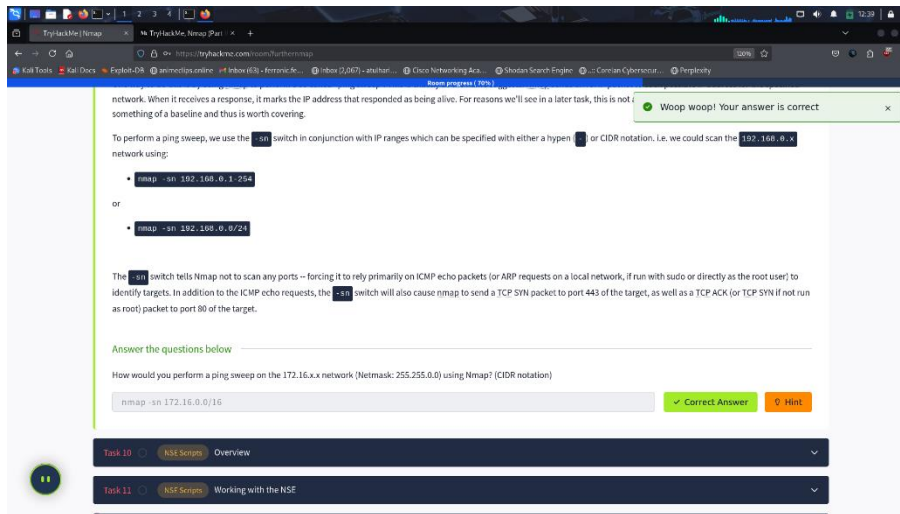
✓ Correct Answer

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

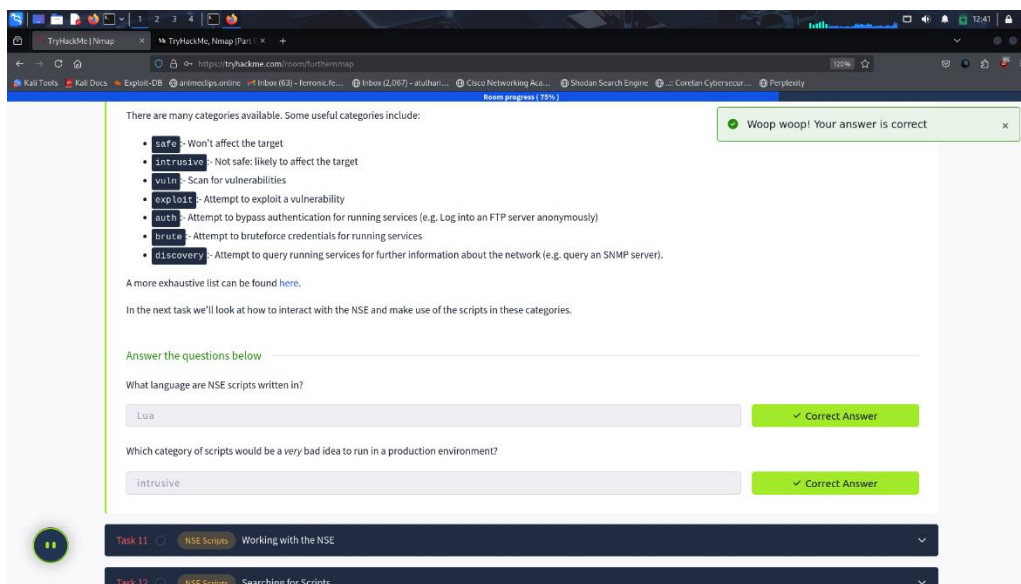
✓ Correct Answer

Task 9 Scan Types ICMP Network Scanning

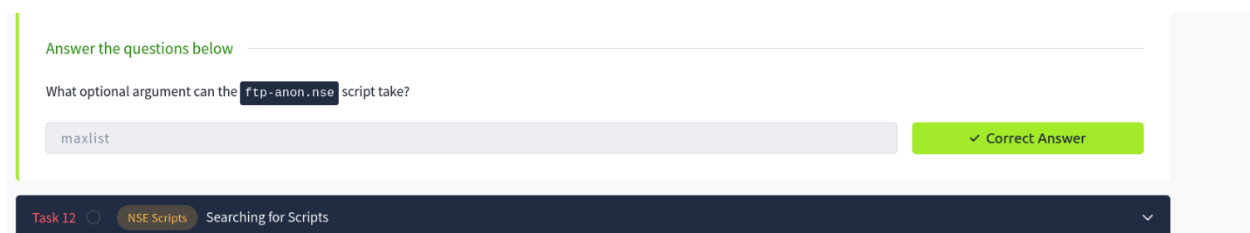
Task 8 consist of reading part of NULL, FIN and XMAS. The URG flag is used by XMAS scan . PSH,URG and FIN are used in xmas scan (-sX).



From the above example we can use a similar ping method to extract the answers for this question using nmap.



Task 10 is an overview of NSE. Lua is a programming language used for NSE scripts. Intrinsive script is not safe and is likely to affect the target.



Task 11 includes the topic 'Working with NSE'. It explains about the NSE scripts.

The screenshot shows a THM AttackBox interface. On the left, a web browser displays a tutorial titled 'Room progress (77%)' about NSE scripts. The tutorial explains how to install NSE scripts manually using `sudo apt update` and `sudo apt install nmap`, and how to download scripts from the Nmap SVN repository. It also mentions the `nmap --script-updatedb` command. Below the tutorial, there are two questions: '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?' and 'Read through this script. What does it depend on?'. The first question has a text input field with 'smb-os-discovery.nse' and a 'Correct Answer' button. The second question has a text input field with '-----' and a 'Submit' button. On the right, a terminal window shows the command `ls *smb*` being executed in the directory `/usr/share/nmap/scripts`, listing various NSE scripts including `info.nse`, `ip-forwarding.nse`, `root@ip-10-201-58-187:~# cd /usr/share/nmap/scripts`, `root@ip-10-201-58-187:/usr/share/nmap/scripts# ls *smb*`, `smb2-capabilities.nse`, `smb2-security-mode.nse`, `smb2-tlsh.nse`, `smb2-vuln-uptime.nse`, `smb-brute.nse`, `smb-double-pulsar-backdoor.nse`, `smb-enum-domains.nse`, `smb-enum-groups.nse`, `smb-enum-processes.nse`, `smb-enum-services.nse`, `smb-enum-sessions.nse`, `smb-enum-shares.nse`, `smb-enum-users.nse`, `smb-flood.nse`, `smb-ls.nse`, `smb-nmap.nse`, `smb-os-discovery.nse`, `smb-print-text.nse`, `smb-vuln-conficker.nse`, `smb-vuln-cve2009-3103.nse`, `smb-vuln-cve-2017-7494.nse`, `smb-vuln-ms06-025.nse`, `smb-vuln-ms07-029.nse`, `smb-vuln-ms08-067.nse`, `smb-vuln-ms10-054.nse`, `smb-vuln-ms10-061.nse`, `smb-vuln-ms17-010.nse`, `smb-vuln-regsvcs-dos.nse`, `smb-vuln-webexec.nse`, and `smb-webexec-exploit.nse`. A notification bubble at the top right says 'Woop woop! Your answer is correct'.

In task 12, we had to access the script library and then find the smb script from it.

The screenshot shows a THM AttackBox interface. On the left, a web browser displays a tutorial titled 'Room progress (79%)' about NSE scripts. The tutorial explains how to install NSE scripts manually using `sudo apt update` and `sudo apt install nmap`, and how to download scripts from the Nmap SVN repository. It also mentions the `nmap --script-updatedb` command. Below the tutorial, there are two questions: '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?' and 'Read through this script. What does it depend on?'. The first question has a text input field with 'smb-os-discovery.nse' and a 'Correct Answer' button. The second question has a text input field with 'smb-brute' and a 'Loading...' button. On the right, a terminal window shows the command `cat smb-brute.nse` being executed, displaying the content of the `smb-brute` script. The script includes a header with the author 'Ron Bowes', a license, categories, and dependencies. It also includes a function `hostrule` that checks if the script should be run based on the host's OS strings. A notification bubble at the top right says 'Woop woop! Your answer is correct'.

After we open the smb file using grep command which is mentioned in this.

Then we have task 13 which is firewall evasion, ICMP protocol is most necessary. The option for -pn switch is mentioned.

The screenshot shows the TryHackMe interface for the 'Nmap' room. On the left, the 'Room progress (88%)' section lists tasks 1 through 14. Task 13 is 'Practical' and Task 14 is 'Conclusion'. The main content area displays the 'Answer the questions below' section for Task 13. The questions are:

- Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-pn` switch?
Answer: ICMP (Correct Answer)
- [Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?
Answer: `--data-length` (Correct Answer)

On the right, a terminal window shows the following commands and output:

```
root@ip-10-201-58-187:~# nmap --help | grep -i data
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--datadir <dirname>: Specify custom Nmap data file location

root@ip-10-201-58-187:~#
```

The screenshot shows the TryHackMe interface for the 'Nmap' room. On the left, the 'Room progress (90%)' section lists tasks 1 through 14. Task 14 is 'Practical'. The main content area displays the 'Answer the questions below' section for Task 14. The questions are:

- Does the target ip respond to ICMP echo (ping) requests (Y/N)?
Answer: 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?
Answer: 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!
Answer: `-sX` (Correct Answer)
- Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?
Answer: `-sS` (Correct Answer)
- Open Wireshark (see [Cryllie'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?
Answer: 217 (Y/N) (Correct Answer)

On the right, a terminal window shows the following commands and output:

```
root@ip-10-201-58-187:~# nmap --help | grep -i data
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--datadir <dirname>: Specify custom Nmap data file location

root@ip-10-201-58-187:~# ping 10.201.43.168
PING 10.201.43.168 (10.201.43.168) 56(84) bytes of data.
^C
--- 10.201.43.168 ping statistics ---
Add 77 packets transmitted, 0 received, 100% packet loss, time 77805ms

root@ip-10-201-58-187:~# nmap --help | grep -i xmas
-sX/sf/sX: TCP Null, FIN, and Xmas scans

root@ip-10-201-58-187:~# nmap -sX 10.201.43.168
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-02 08:44 BST
Nmap scan report for ip-10-201-43-168.ec2.internal (10.201.43.168)
Host is up (0.000054s latency).
All 1000 scanned ports on ip-10-201-43-168.ec2.internal (10.201.43.168) are open
|filtered
MAC Address: 16:FF:F1:C6:FA:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds
```

We had our task 14, in which it tested our practical skills using nmap to scan and gather info after we have been given a target IP (which we get after initial starting of the machine).

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?

- Submit

Open Wireshark (see [Cryllinc'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 by playing the [ftp-anon](#) script against the box. Can Nmap login successfully to the FTP server 21? (Y/N)

✓ Correct Answer Submit

The screenshot shows a web browser at <https://tryhackme.com/room/furthermap>. The left sidebar lists various tools like Kali Tools, Kali Docs, Exploit-DB, and others. The main area displays two challenge cards:

- Challenge 1:** "Does the target ip respond to icmp - echo request (ping)?"
Answer: N
Status: Correct Answer
- Challenge 2:** "Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?"
Answer: 999
Status: Correct Answer

Below the second challenge, there is a hint section:

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!

Answer: No Response
Status: Correct Answer Hint

A third challenge card is partially visible:

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

Answer: 5
Status: Correct Answer

At the bottom, there is a Wireshark instruction: "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)"

On the right side of the screen, a terminal window titled "root@ip-10-201-58-187:" shows the output of several nmap commands:

```
File Edit View Search Terminal Help
Initiating ARP Ping Scan at 08:59
Scanning 10.201.43.168 [1 port]
Completed ARP Ping Scan at 08:59, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:59
Completed Parallel DNS resolution of 1 host. at 08:59, 0.00s elapsed
Initiating SYN Stealth Scan at 08:59
Scanning ip-10-201-43-168.ec2.internal (10.201.43.168) [5000 ports]
Discovered open port 80/tcp on 10.201.43.168
Discovered open port 21/tcp on 10.201.43.168
Discovered open port 135/tcp on 10.201.43.168
Discovered open port 53/tcp on 10.201.43.168
Add: Discovered open port 3389/tcp on 10.201.43.168
Completed SYN Stealth Scan at 08:59, 14.26s elapsed (5000 total ports)
Nmap scan report for ip-10-201-43-168.ec2.internal (10.201.43.168)
Host is up, received arp-response (0.00028s latency).
Scanned at 2025-08-02 08:59:11 BST for 15s
Not shown: 4995 filtered ports
NetReason: 4995 no-responses
PORT      STATE SERVICE        REASON
21/tcp    open  ftp            syn-ack ttl 128
53/tcp    open  domain         syn-ack ttl 128
80/tcp    open  http           syn-ack ttl 128
135/tcp   open  msrpc          syn-ack ttl 128
3389/tcp  open  ms-wbt-server  syn-ack ttl 128
```

A green notification bubble says: "Woop woop! Your answer is correct"

We got a total of 5 responses for TCP SYN scan on the first 5000 ports.

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

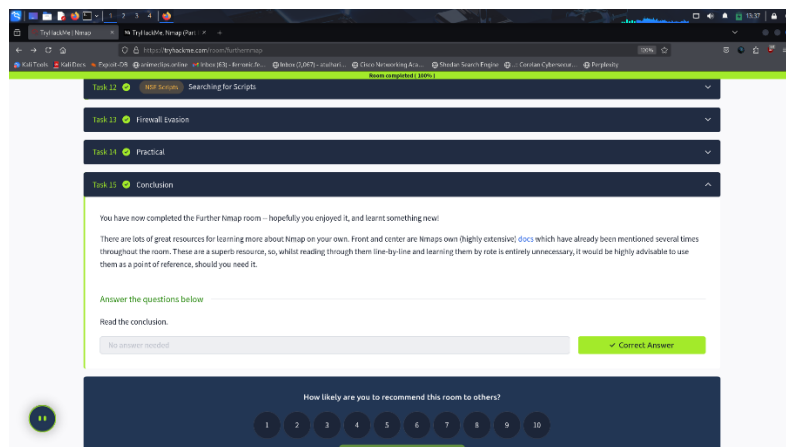
✓ Correct Answer

Open Wireshark (see [Cryllic'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)

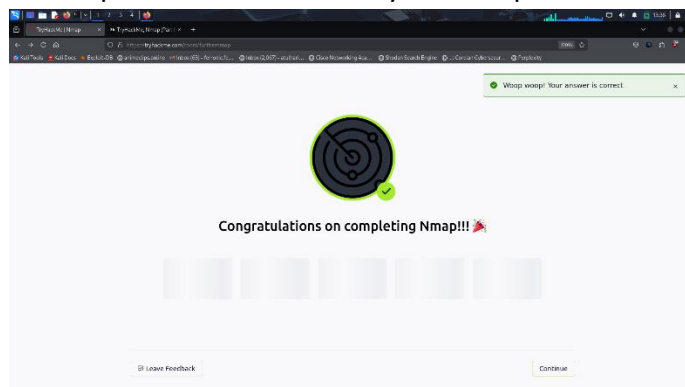
Y

✓ Correct Answer

Task 15 Conclusion



With that we have completed our room or further Nmap. Which focused on the use and types of nmap and the different ways to find ports and scan them accordingly.



We have successfully completed this Nmap room on THM.