

Nmap Room Tryhackme

1. Task 1

Firstly, I deployed the machine.

2. Task 2: **Introduction**

Introduction on networking constructs and three questions on it.

3. Task 3: **Nmap Switches**

Nmap can be accessed by typing `nmap` into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do different things) help menu for nmap (accessed with `nmap -h`) and/or the nmap man page (access with `man nmap`).

Room progress (11%)

Some of the switches (command arguments which tell a program to do different things) we will be covering below.

All you'll need for this is the help menu for `nmap` (accessed with `nmap -h`) and/or the `nmap` man page (access with `man nmap`). For each answer, include all parts of the switch unless otherwise specified. This includes the hyphen at the start (-).

Answer the questions below

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

✓ Correct Answer

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

Submit

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

Application Thu 7 Aug, 17:48 AttackBox IP:10.201.98.43

Woop woop! Your answer is correct

```
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-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
--spoof-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, sI<Ipt kIdd3, and Greppable 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)
```

Room progress (27%)

✓ Correct Answer

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

✓ 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?

Submit

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!

```
Options which take <time> are in seconds, or append 'ms' (milliseconds)
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-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
```

4. Task 4: Scan Types Overview

There are three basic scan types:

- TCP Connect Scans (-sT)
- SYN “Half-open” Scans (-sS)

- UDP Scans (-sU)

5. Task 5 : Scan Types TCP Connect Scans

The three-way handshake consists of three stages. First the connecting terminal (our attacking machine, in this instance) sends a TCP request to the target server with the SYN flag set. The server then acknowledges this packet with a TCP response containing the SYN flag, as well as the ACK flag. Finally, our terminal completes the handshake by sending a TCP request with the ACK flag set.

6. Task 6: Scan Types SYN Scans

SYN scans are sometimes referred to as "*Half-open*" scans, or "*Stealth*" scans. Where TCP scans perform a full three-way handshake with the target, SYN scans sends back a RST TCP packet after receiving a SYN/ACK from the server.

7. Task 7: Scan Types UDP Scans

tryhackme.com/room/furthernmap

Room progress (65%)

effective when dealing with modern systems.

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

Loading...

Application Thu 7 Aug, 17:56 AttackBox IP: 10.201.98.43

```
root@ip-10-201-98-43: ~
File Edit View Search Terminal Help
--resume <filename>: Resume an aborted scan
--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
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@ip-10-201-98-43:~# -iptables -I INPUT -p tcp --dport <port> -j REJECT --reject-with tcp-reset
bash: port: No such file or directory
root@ip-10-201-98-43:~#
```

tryhackme.com/room/furthernmap

Room progress (68%)

- `nmap -sn 192.168.0.1-254`

or

- `nmap -sn 192.168.0.0/24`

The `-sn` switch tells Nmap not to scan any ports -- forcing it to rely primarily on ICMP echo packets (or ARP requests on a local network, if run with sudo or directly as the root user) to identify targets. In addition to the ICMP echo requests, the `-sn` switch will also cause nmap to send a `TCP SYN` packet to port 443 of the target, as well as a `TCP ACK` (or `TCP SYN` if not run as root) packet to port 80 of the target.

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)

Submit Hint

Application Thu 7 Aug, 17:56 AttackBox IP: 10.201.98.43

```
root@ip-10-201-98-43: ~
File Edit View Search Terminal Help
--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
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@ip-10-201-98-43:~# -iptables -I INPUT -p tcp --dport <port> -j REJECT --reject-with tcp-reset
bash: port: No such file or directory
root@ip-10-201-98-43:~# nmap -sn 192.168.0.1-254
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-07 17:56 BST
```

Task 8: Scan Types NULL, FIN and Xmas

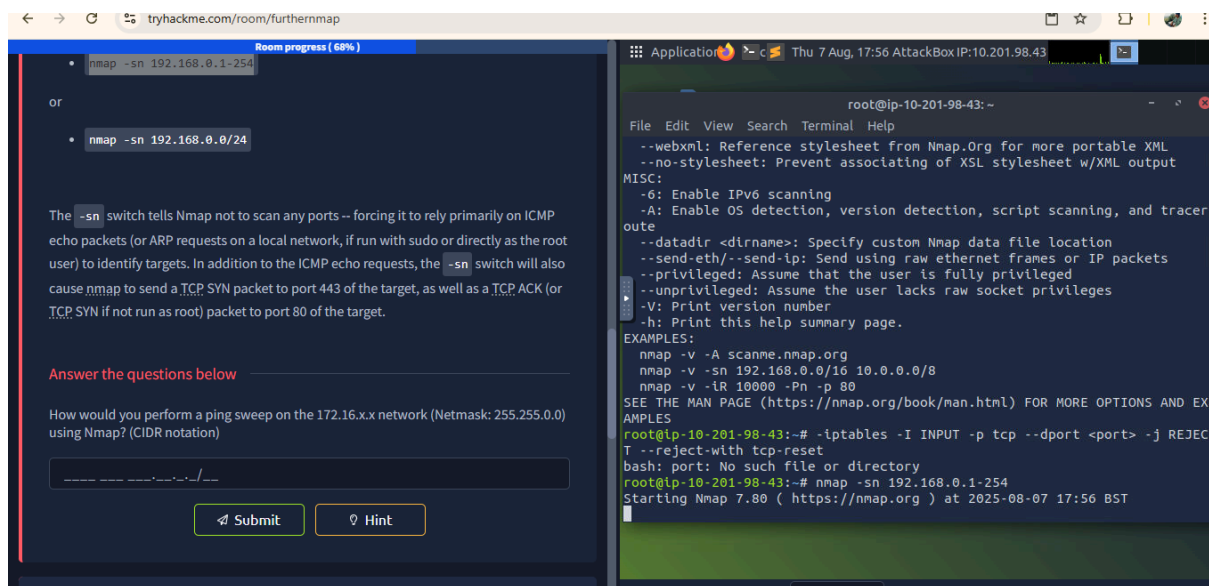
- FIN scans (`-sF`)

- NULL scans (`-sN`)

9. Task 9: Scan Types ICMP Network Scanning

Learned to perform ping sweep

`nmap -sn`

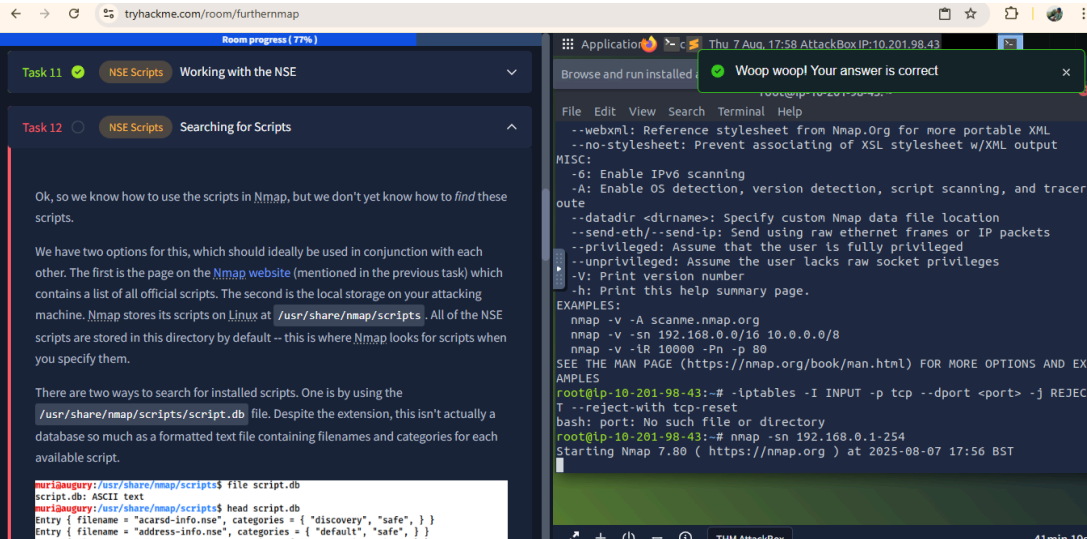


10. Task 10: NSE Scripts Overview

- `safe`:- Won't affect the target
- `intrusive`:- Not safe: likely to affect the target
- `vuln`:- Scan for vulnerabilities
- `exploit`:- Attempt to exploit a vulnerability

- **auth:-** Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)
- **brute:-** Attempt to bruteforce credentials for running services
- **discovery:-** Attempt to query running services for further information about the network (e.g. query an SNMP server).

11. Task 11: NSE Scripts



The screenshot shows a web browser window with the URL `tryhackme.com/room/furthernmap`. The page displays two tasks related to NSE scripts:

- Task 11: NSE Scripts - Working with the NSE** (Completed): This task explains how to use NSE scripts. It mentions that Nmap stores its scripts on Linux at `/usr/share/nmap/scripts`. It also describes two ways to search for installed scripts: using the `/usr/share/nmap/scripts/script.db` file or using the `file` command.
- Task 12: NSE Scripts - Searching for Scripts** (Not started): This task is currently inactive.

Below the task descriptions, a terminal window shows the following commands and output:

```

muri@augury:~$ cd /usr/share/nmap/scripts$ file script.db
script.db: ASCII text
muri@augury:~$ cd /usr/share/nmap/scripts$ head script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }

```

On the right side of the terminal, a green notification bubble says "Woop woop! Your answer is correct". The terminal also shows the Nmap version 7.80 help text and a successful scan of `192.168.0.1-254`.

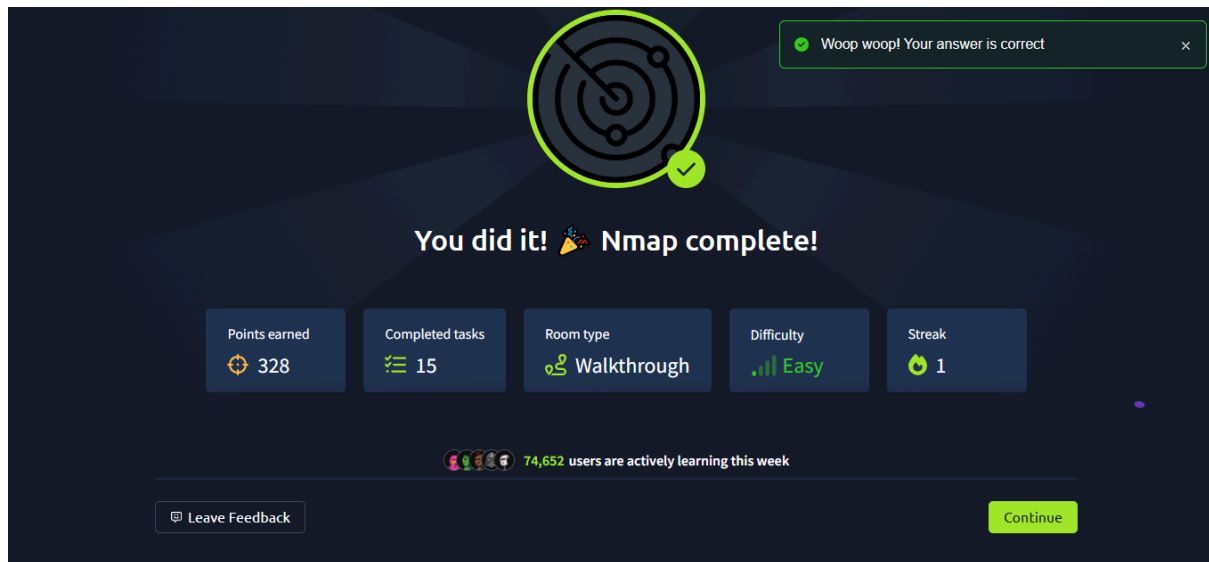
- *smb-brute*

12. Task 3: Firewall Evasion

- `-f:-` Used to fragment the packets
- `--scan-delay <time>ms:-` used to add a delay between packets sent
- `--badsum:-` this is used to generate in invalid checksum for packets.

And lastly, there was a practical one too.

I completed the room successfully.



– Abhinav V R

<https://tryhackme.com/p/lushfog>