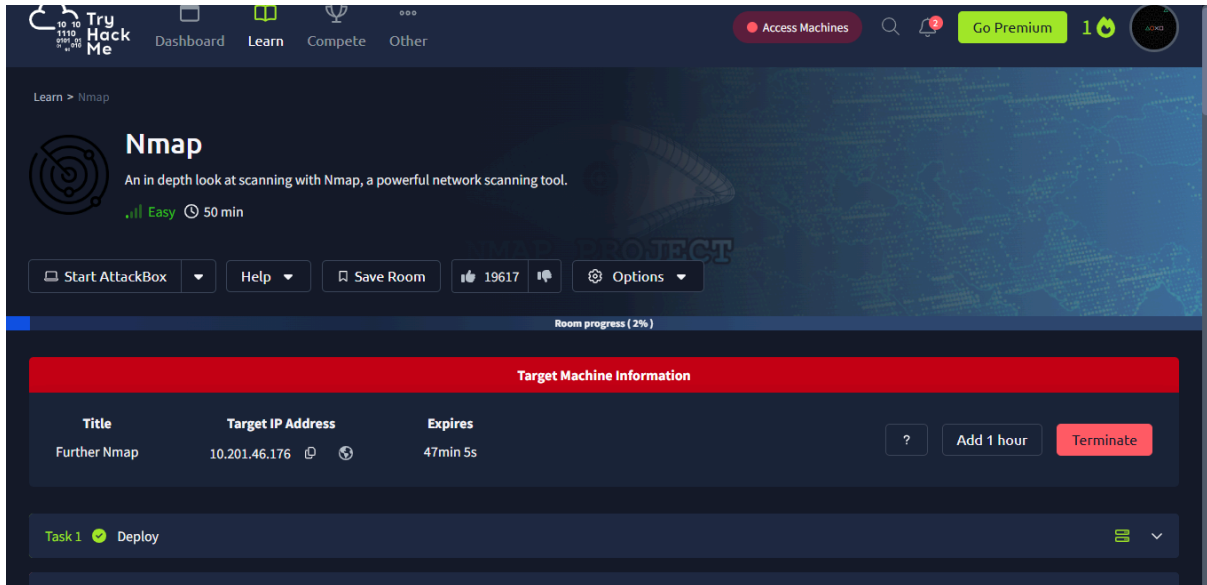


TryHackMe: Nmap CTF Walkthrough

- Nobin Sijo

Challenge: Nmap - An in-depth look at scanning with Nmap, a powerful network scanning tool. **Target IP Address:** 10.201.46.176

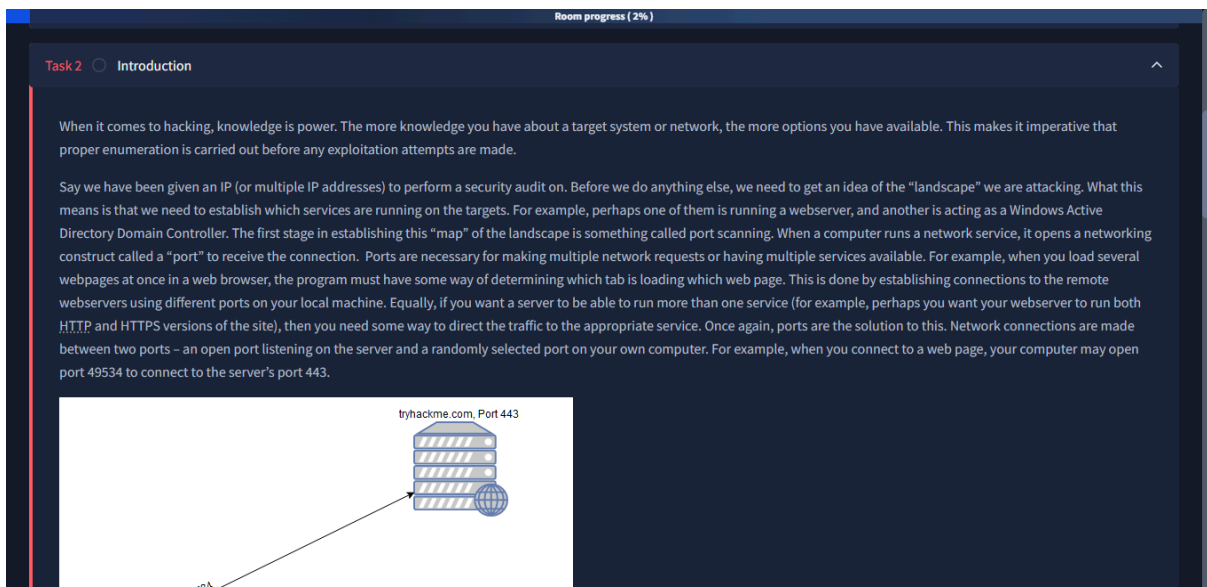
Task 1: Deploy



The screenshot shows the TryHackMe interface for the 'Nmap' challenge. The top navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other'. The challenge title 'Nmap' is prominently displayed, along with a difficulty level of 'Easy' and a duration of '50 min'. Below the title, there are buttons for 'Start AttackBox', 'Help', 'Save Room', and 'Options'. A 'Room progress (2%)' indicator is visible. The 'Target Machine Information' section shows the title 'Further Nmap', the target IP address '10.201.46.176', and an expiration time of '47min 5s'. At the bottom, the task list shows 'Task 1' as 'Deploy'.

- **Objective:** First things first, we need to power on our target. This task is all about deploying the virtual machine we'll be scanning, giving us a live system to practice on.
- **Action:** The virtual machine for the challenge was deployed.

Task 2: Introduction



The screenshot shows the 'Task 2: Introduction' section of the Nmap challenge. The text explains the importance of knowledge in hacking and the process of port scanning. It states that port scanning is the first stage in establishing a 'map' of the target system. The text describes how a computer runs a network service, opening a networking construct called a 'port' to receive connections. It explains that ports are necessary for making multiple network requests or having multiple services available. For example, when loading webpages, the program must determine which tab is loading which web page by establishing connections to the remote webserver using different ports. It also mentions that a server can run more than one service, and ports are the solution to this. Network connections are made between two ports: an open port listening on the server and a randomly selected port on the user's computer. For example, when connecting to a web page, the user's computer may open port 49534 to connect to the server's port 443.

tryhackme.com, Port 443

49534

muitandoradle.co.uk Port 443

- **Objective:** Before we start scanning, it's crucial to understand the 'why'. This task covers the basics of network reconnaissance and the role of ports. Our goal is to grasp the core concepts that make tools like Nmap so powerful.
- **Question:** What networking constructs are used to direct traffic to the right application on a server?
 - **Answer:** Ports

Room progress (9%)

So, why `nmap`? The short answer is that it's currently the industry standard for a reason: no other port scanning tool comes close to matching its functionality (although some newcomers are now matching it for speed). It is an extremely powerful tool - made even more powerful by its scripting engine which can be used to scan for vulnerabilities, and in some cases even perform the exploit directly! Once again, this will be covered more in upcoming tasks.

For now, it is important that you understand: what port scanning is; why it is necessary; and that `nmap` is the tool of choice for any kind of initial enumeration.

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

Task 4 ○ Scan Types Overview

- **Question:** How many of these are available on any network-enabled computer?
 - **Answer:** 65535
- **Question:** How many of these are considered "well-known"?
 - **Answer:** 1024

Task 3: Nmap Switches

Room progress (11%)

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) 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)?

-sS ✓ 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: Sun 3 Aug, 13:25 AttackBox IP: 10.201.112.138

Woop woop! Your answer is correct

```

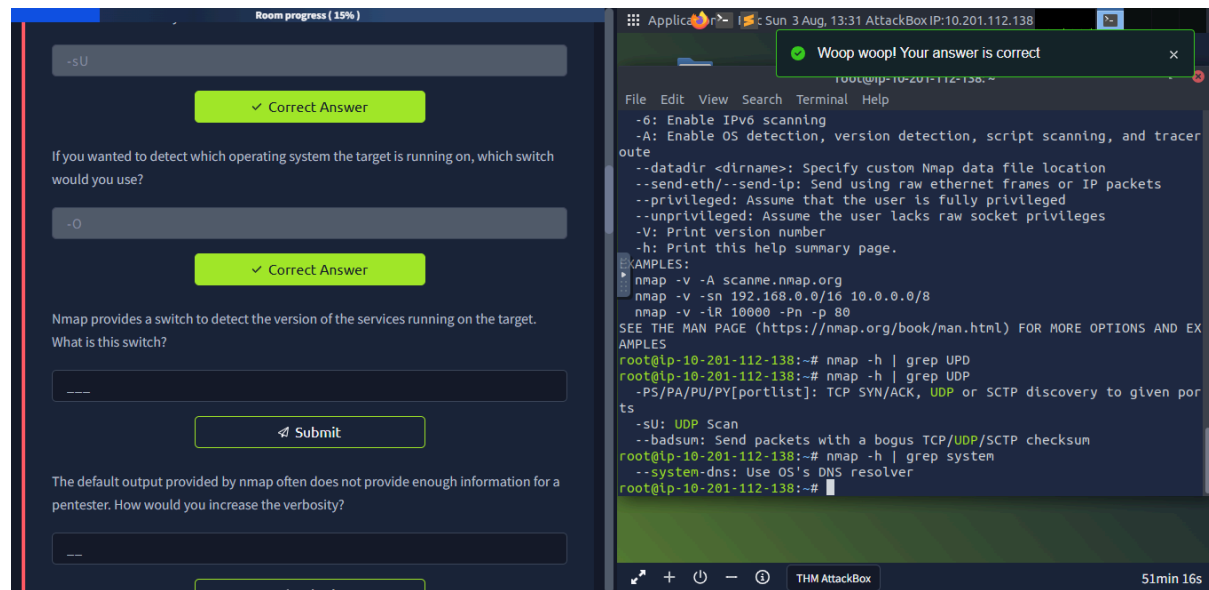
File Edit View Search Terminal Help
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to 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:
-o: 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 -lR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@tp-10-201-112-138:~#
  
```

THM AttackBox 57min 5s

- **Objective:** Time to learn the language of Nmap. This task is about getting comfortable with the command-line switches that control our scans. We'll use the

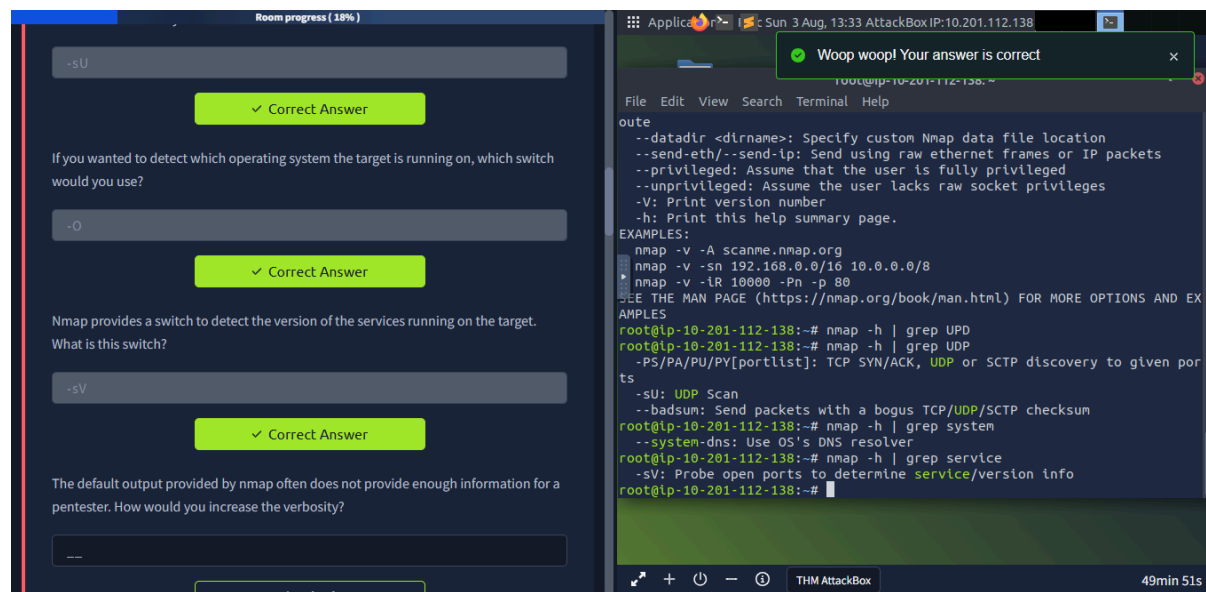
help menu to look up different options for everything from scan types to output formats.

- **Question:** What is the first switch listed in the help menu for a "Syn Scan"?
 - **Answer:** `-sS`
 - **Nmap Command Used:** `nmap -h` (to view the help menu)
- **Question:** Which switch would you use for a "UDP scan"?
 - **Answer:** `-sU`
 - **Nmap Command Used:** `nmap -h | grep UDP`
- **Question:** If you wanted to detect which operating system the target is running on, which switch would you use?
 - **Answer:** `-O`

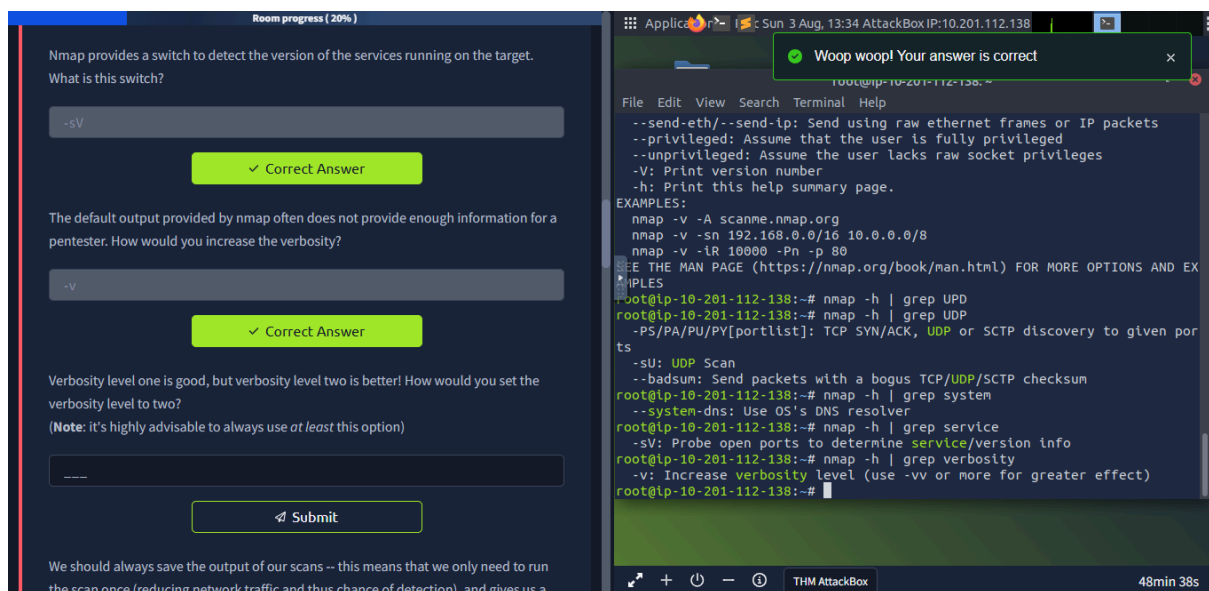


- **Nmap Command Used:** `nmap -h | grep "OS detection"`
- **Question:** Nmap provides a switch to detect the version of the services running on the target. What is this switch?
 - **Answer:** `-sV`

- **Nmap Command Used:** `nmap -h | grep "version detection"`



- **Question:** How would you increase the verbosity?



- **Answer:** `-v`
- **Nmap Command Used:** `nmap -h | grep "verbosity"`

- **Question:** How would you set the verbosity level to two?

Room progress (20%)

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

✓ Correct Answer

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

✓ 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)

Submit

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

THM AttackBox

```

root@ip-10-201-112-138:~
File Edit View Search Terminal Help
--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 EX
MPLES
root@ip-10-201-112-138:~# nmap -h | grep UDP
root@ip-10-201-112-138:~# nmap -h | grep UDP
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given por
ts
-sU: UDP Scan
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
root@ip-10-201-112-138:~# nmap -h | grep system
--system-dns: Use OS's DNS resolver
root@ip-10-201-112-138:~# nmap -h | grep service
-sV: Probe open ports to determine service/version info
root@ip-10-201-112-138:~# nmap -h | grep verbosity
-v: Increase verbosity level (use -vv or more for greater effect)
root@ip-10-201-112-138:~# nmap -h | grep verbose
root@ip-10-201-112-138:~#

```

47min 24s

- **Answer:** -vv

- **Question:** What switch would you use to save the nmap results in three major formats?

Room progress (25%)

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)

✓ 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?

✓ Correct Answer

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

Submit

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

THM AttackBox

```

root@ip-10-201-112-138:~
File Edit View Search Terminal Help
root@ip-10-201-112-138:~# nmap -h | grep UDP
root@ip-10-201-112-138:~# nmap -h | grep UDP
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given por
ts
-sU: UDP Scan
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
root@ip-10-201-112-138:~# nmap -h | grep system
--system-dns: Use OS's DNS resolver
root@ip-10-201-112-138:~# nmap -h | grep service
-sV: Probe open ports to determine service/version info
root@ip-10-201-112-138:~# nmap -h | grep verbosity
-v: Increase verbosity level (use -vv or more for greater effect)
root@ip-10-201-112-138:~# nmap -h | grep verbose
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-03 13:36 BST
Read data files from: /usr/bin/./share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~#

```

45min 55s

- **Answer:** -oA
- **Nmap Command Used:** nmap -h | grep "major formats"

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

The screenshot shows a THM AttackBox interface. On the left, a quiz question asks: "What switch would you use to save the nmap results in a 'normal' format?". The input field contains "-oN", which is marked as a "Correct Answer". Below this, another question asks: "What switch would you use to save the nmap results in a 'greppable' format?". The input field is empty. A "Submit" button is visible. On the right, a terminal window shows the command `root@ip-10-201-112-138:~# nmap -h | grep normal` being executed, resulting in the output: `-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdId3,`. A notification bubble at the top of the terminal says "Woop woop! Your answer is correct".

- **Answer:** -oN
- **Nmap Command Used:** `nmap -h | grep "normal"`

- **Question:** How would you save results in a "greppable" format?

- **Answer:** -oG

- **Question:** How would you activate "aggressive" mode?

The screenshot shows a THM AttackBox interface. On the left, a quiz question asks: "How would you activate this setting?". The input field contains "-A", which is marked as a "Correct Answer". Below this, another question asks: "How would you set the timing template to level 5?". The input field is empty. A "Submit" button is visible. On the right, a terminal window shows the command `root@ip-10-201-112-138:~# nmap -h | grep aggressive` being executed, resulting in the output: `-A: Enable OS detection, version detection, script scanning, and traceroute`. A notification bubble at the top of the terminal says "Woop woop! Your answer is correct".

- **Answer:** -A
- **Nmap Command Used:** `nmap -h | grep "aggressive"`

- **Question:** How would you set the timing template to level 5?

Room progress (34%)

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?

✓ 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?

✓ Correct Answer

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

How would you tell nmap to only scan port 80?

```

root@ip-10-201-112-138:~
File Edit View Search Terminal Help
-sV: Probe open ports to determine service/version info
root@ip-10-201-112-138:~# nmap -h | grep verbosity
-v: Increase verbosity level (use -vv or more for greater effect)
root@ip-10-201-112-138:~# nmap -h | grep verbose
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-03 13:36 BST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -h | grep normal
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|c|ri|pt kId|d|3,
root@ip-10-201-112-138:~# nmap -h | grep traceroute
--traceroute: Trace hop path to each host
-A: Enable OS detection, version detection, script scanning, and traceroute
root@ip-10-201-112-138:~# http
root@ip-10-201-112-138:~# nmap -h | grep timing
-T<0-5>: Set timing template (higher is faster)
root@ip-10-201-112-138:~# !!

```

- **Answer:** -T5
- **Nmap Command Used:** nmap -h | grep "timing template"

- **Question:** How would you tell nmap to only scan port 80?

Room progress (38%)

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?

✓ Correct Answer

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

How would you tell nmap to only scan port 80?

✓ Correct Answer

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

✓ Correct Answer

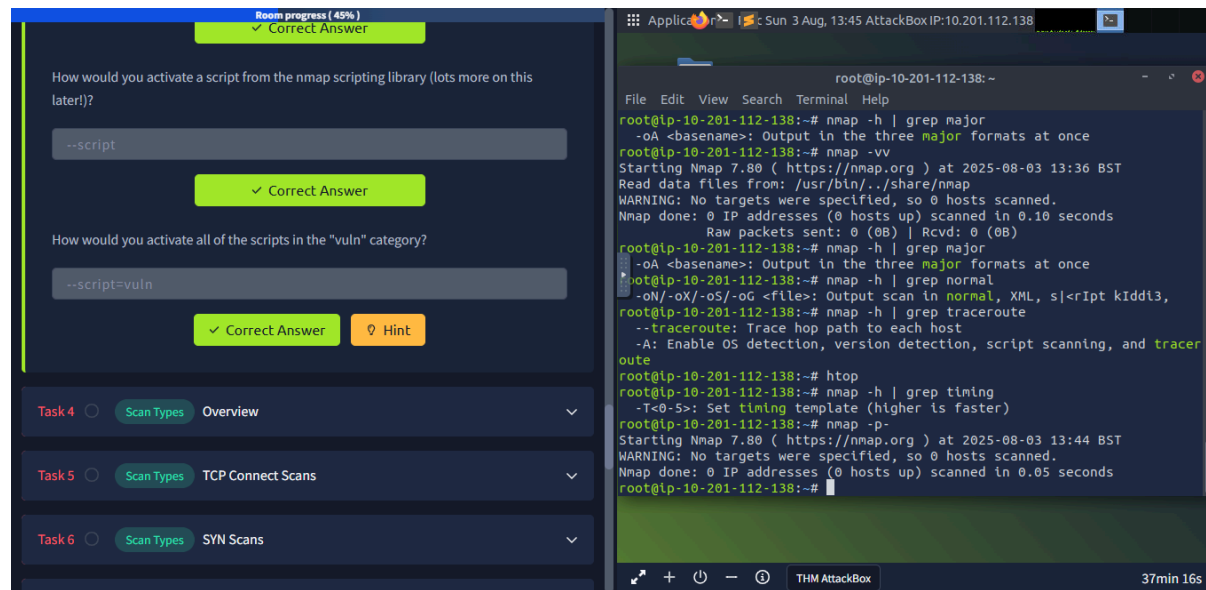
Woop woop! Your answer is correct

```

root@ip-10-201-112-138:~
File Edit View Search Terminal Help
-sV: Probe open ports to determine service/version info
root@ip-10-201-112-138:~# nmap -h | grep verbosity
-v: Increase verbosity level (use -vv or more for greater effect)
root@ip-10-201-112-138:~# nmap -h | grep verbose
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-03 13:36 BST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -h | grep normal
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|c|ri|pt kId|d|3,
root@ip-10-201-112-138:~# nmap -h | grep traceroute
--traceroute: Trace hop path to each host
-A: Enable OS detection, version detection, script scanning, and traceroute
root@ip-10-201-112-138:~# http
root@ip-10-201-112-138:~# nmap -h | grep timing
-T<0-5>: Set timing template (higher is faster)
root@ip-10-201-112-138:~# !!

```

- **Answer:** -p 80
- **Question:** How would you tell nmap to scan ports 1000-1500?
 - **Answer:** -p 1000-1500
- **Question:** How would you activate a script from the nmap scripting library?
 - **Answer:** --script



- **Question:** How would you activate all of the scripts in the "vuln" category?
 - **Answer:** `--script=vuln`

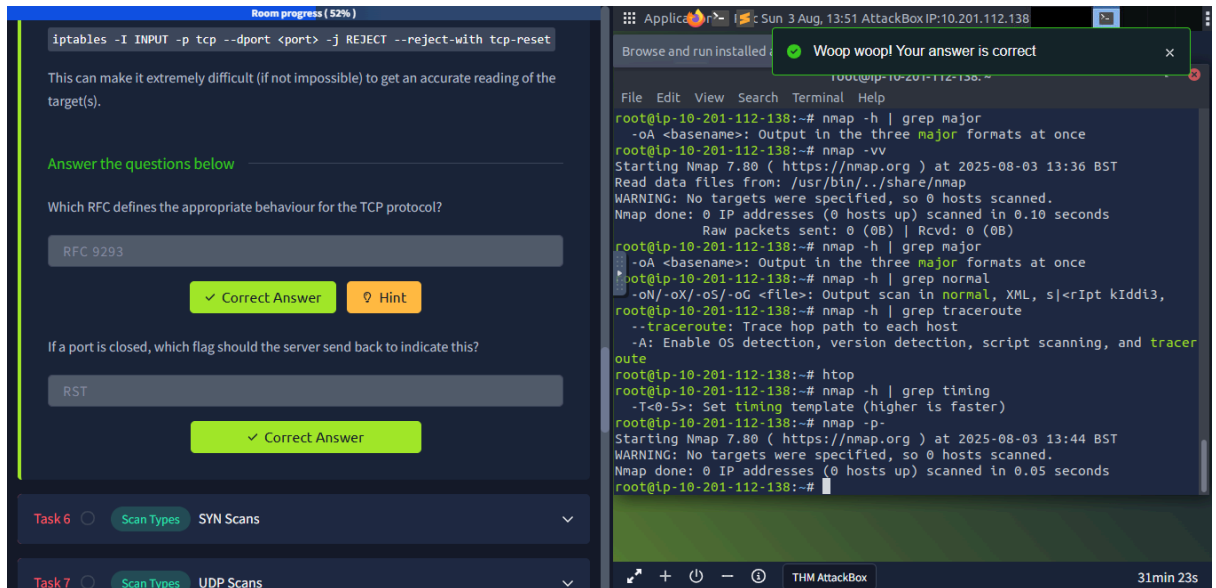
Task 4 & 5: Scan Types - TCP Connect Scans

- **Objective:** Let's start with the most fundamental scan type. Here, we'll explore the TCP Connect scan, which completes a full three-way handshake. The objective is to understand how this basic scan works and how to interpret its results based on standard TCP behavior.
- **Question:** Which RFC defines the appropriate behaviour for the TCP protocol?
 - **Answer:** `RFC 9293`
- **Question:** If a port is closed, which flag should the server send back to indicate this?
 - **Answer:** `RST`

Task 6: Scan Types - SYN Scans

- **Objective:** Now for a more subtle approach. This task introduces the SYN 'stealth' scan. Our goal is to see how this 'half-open' scan differs from a full connect scan,

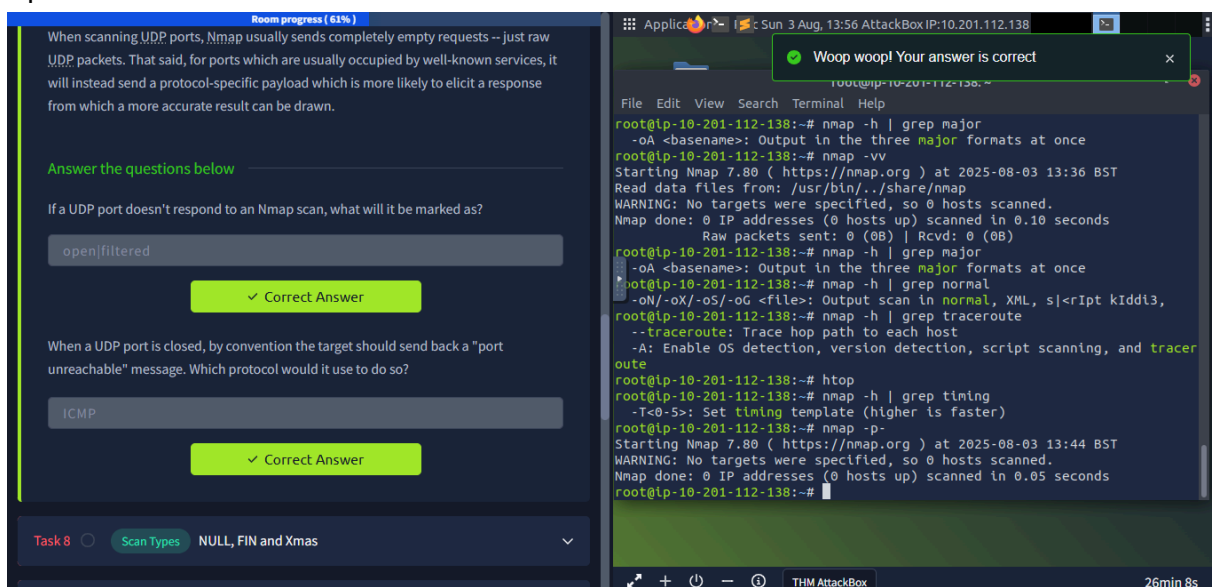
making it faster and less conspicuous on the network.



- **Question:** There are two other names for a SYN scan, what are they?
 - **Answer:** Half-Open, Stealth
- **Question:** Can Nmap use a SYN scan without Sudo permissions (Y/N)?
 - **Answer:** N

Task 7: Scan Types - UDP Scans

- **Objective:** Scanning UDP ports presents a unique challenge because it's a 'connectionless' protocol. The objective here is to understand the difficulties of UDP scanning and learn how Nmap interprets the responses (or lack thereof) to determine a port's state.



- **Question:** If a UDP port doesn't respond to an Nmap scan, what will it be marked as?
 - **Answer:** open|filtered

- **Question:** 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?
 - **Answer:** ICMP

Task 8: Scan Types - NULL, FIN, and Xmas

- **Objective:** Let's get even stealthier. This section is about using NULL, FIN, and Xmas scans to evade firewalls. The goal is to understand the theory behind sending these non-standard packets and how they can sometimes bypass security measures that are only watching for typical SYN packets.

The screenshot shows a THM AttackBox interface. On the left, a quiz titled "Room progress (60%)" is displayed. It contains three questions with input fields and "Correct Answer" buttons. The questions are:

- Which of the three shown scan types uses the URG flag? (Answer: xmas)
- Why are NULL, FIN and Xmas scans generally used? (Answer: Firewall Evasion)
- Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port? (Answer: Microsoft Windows)

On the right, a terminal window shows the output of several nmap commands. A green notification bubble at the top of the terminal says "Woop woop! Your answer is correct". The terminal output includes:

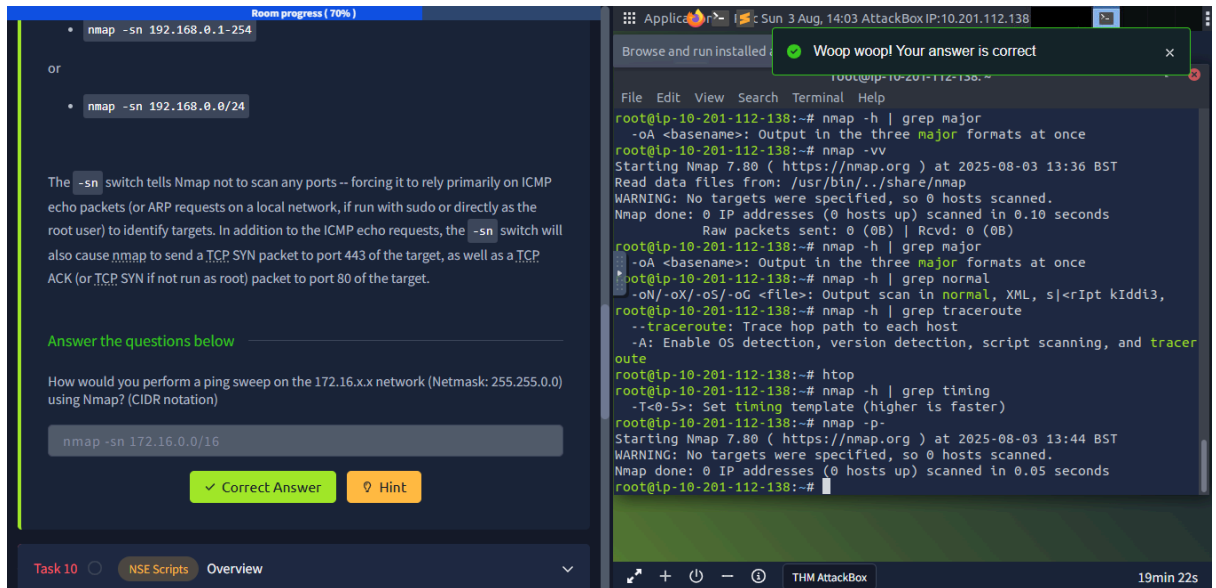
```
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-03 13:36 BST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@ip-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@ip-10-201-112-138:~# nmap -h | grep normal
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdId3,
--traceroute: Trace hop path to each host
-A: Enable OS detection, version detection, script scanning, and traceroute
root@ip-10-201-112-138:~# http
root@ip-10-201-112-138:~# nmap -h | grep timing
-T<0-5>: Set timing template (higher is faster)
root@ip-10-201-112-138:~# nmap -p-
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-03 13:44 BST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
root@ip-10-201-112-138:~#
```

- **Question:** Which of the three shown scan types uses the URG flag?
 - **Answer:** Xmas
- **Question:** Why are NULL, FIN, and Xmas scans generally used?
 - **Answer:** Firewall Evasion
- **Question:** Which common OS may respond to a NULL, FIN, or Xmas scan with a RST for every port?
 - **Answer:** Microsoft Windows

Task 9: Scan Types - ICMP Network Scanning

- **Objective:** Before we scan for open ports, we need to know which hosts are even online. This task focuses on host discovery using a 'ping sweep'. Our objective is to

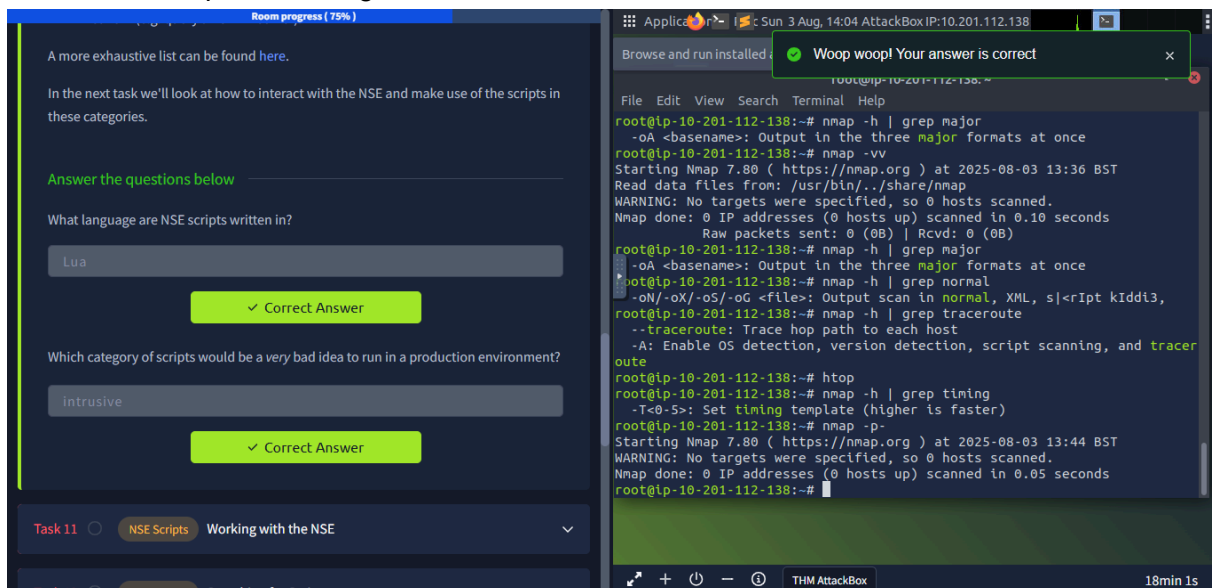
learn how to map out a network and identify live targets.



- **Question:** How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)
 - **Answer:** `nmap -sn 172.16.0.0/16`

Task 10 & 11: NSE Scripts

- **Objective:** Nmap is more than just a port scanner. Here, we'll dive into the Nmap Scripting Engine (NSE), a feature that lets us automate tasks from vulnerability scanning to advanced reconnaissance. The goal is to get a handle on what NSE is and how its scripts are categorized.



- **Question:** What language are NSE scripts written in?
 - **Answer:** `Lua`
- **Question:** Which category of scripts would be a very bad idea to run in a production environment?
 - **Answer:** `intrusive`

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

Script Output

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 verbosity is enabled. Use a negative number to disable the limit, or 0 to disable the listing entirely.

Example Usage

```
nmap -sV -sC <target>
```

Script Output

```
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--  1 1170  924      31 Mar 28  2001 .banner
| d--x--x--x  2 root    root      1024 Jan 14  2002 bin
| d--x--x--x  2 root    root      1024 Aug 10  1999 etc
```

firewall-bypass	Detects a vulnerability in netfilter and other firewalls that use helpers to dynamically open ports for protocols such as ftp and sip.
flume-master-info	Retrieves information from Flume master HTTP pages.
fox-info	Tridium Niagara Fox is a protocol used within Building Automation Systems. Based off Billy Rios and Terry McCorkle's work this Nmap NSE will collect information from A Tridium Niagara system.
freelancer-info	Detects the Freelancer game server (FLServer.exe) service by sending a status query UDP probe.
ftp-anon	Checks if an FTP server allows anonymous logins.
ftp-bounce	Checks to see if an FTP server allows port scanning using the FTP bounce method.
ftp-brute	Performs brute force password auditing against FTP servers.
ftp-libopie	Checks if an FTPd is prone to CVE-2010-1938 (OPIE off-by-one stack overflow), a vulnerability discovered by Maksymilian Arciemowicz and Adam "pi3" Zabrocki. See the advisory at https://nmap.org/r/fbsd-sa-opie . Be advised that, if launched against a vulnerable host, this script will crash the FTPd.
ftp-proftpd-backdoor	

Room progress (77%)

Note that the arguments are separated by commas, and connected to the corresponding script with periods (i.e. `<script-name>.<argument>`).

A full list of scripts and their corresponding arguments (along with example use cases) can be found [here](#).

Nmap scripts come with built-in help menus, which can be accessed using `nmap --script-help <script-name>`. This tends not to be as extensive as in the link given above, however, it can still be useful when working locally.

Answer the questions below

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

maxlist

✓ Correct Answer

Task 12 ☐ NSE Scripts Searching for Scripts

Task 13 ☐ Firewall Evasion

Application

Sun 3 Aug, 14:08 AttackBox IP:10.201.112.138

Woop woop! Your answer is correct

File Edit View Search Terminal Help

root@lp-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@lp-10-201-112-138:~# nmap -vv
Starting Nmap 7.80 (https://nmap.org) at 2025-08-03 13:36 BST
Read data files from: /usr/bin/./share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@lp-10-201-112-138:~# nmap -h | grep major
-oA <basename>: Output in the three major formats at once
root@lp-10-201-112-138:~# nmap -h | grep normal
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, sI<rIpt kiddi3,
root@lp-10-201-112-138:~# nmap -h | grep traceroute
--traceroute: Trace hop path to each host
-A: Enable OS detection, version detection, script scanning, and traceroute
root@lp-10-201-112-138:~# htop
root@lp-10-201-112-138:~# nmap -h | grep timing
-T<0-5>: Set timing template (higher is faster)
root@lp-10-201-112-138:~# nmap -p-
Starting Nmap 7.80 (https://nmap.org) at 2025-08-03 13:44 BST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
root@lp-10-201-112-138:~#

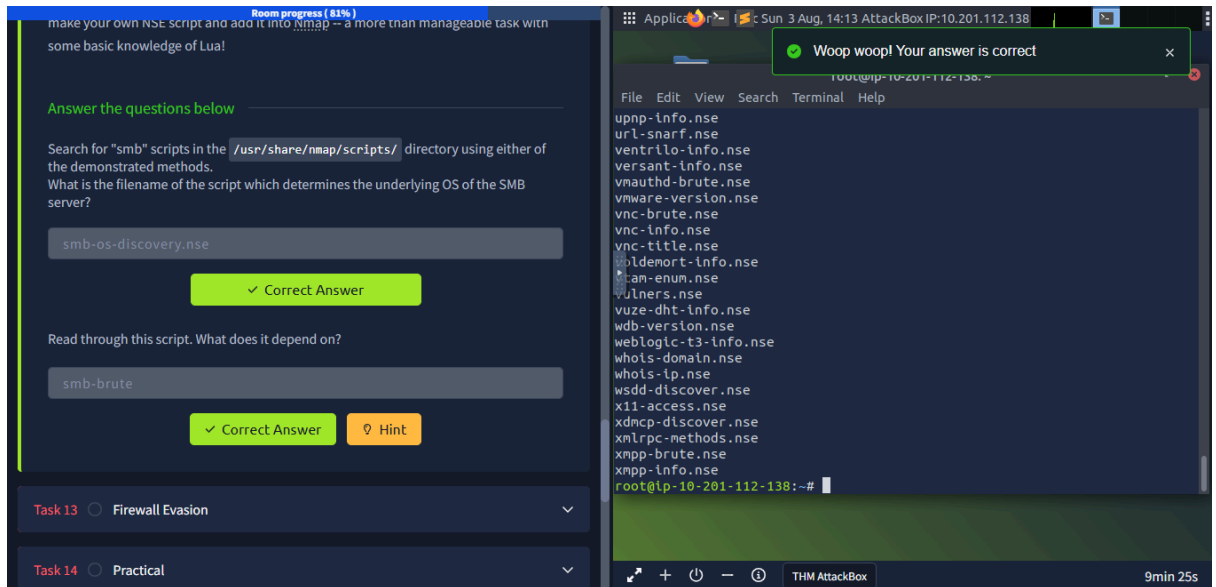
THM AttackBox

14min 4s

- **Answer:** `maxlist`

Task 12: NSE Scripts - Searching for Scripts

- **Objective:** With a massive library of scripts available, knowing how to find the right one is key. This task is focused on searching for NSE scripts locally, so we can find the perfect tool for any given situation.

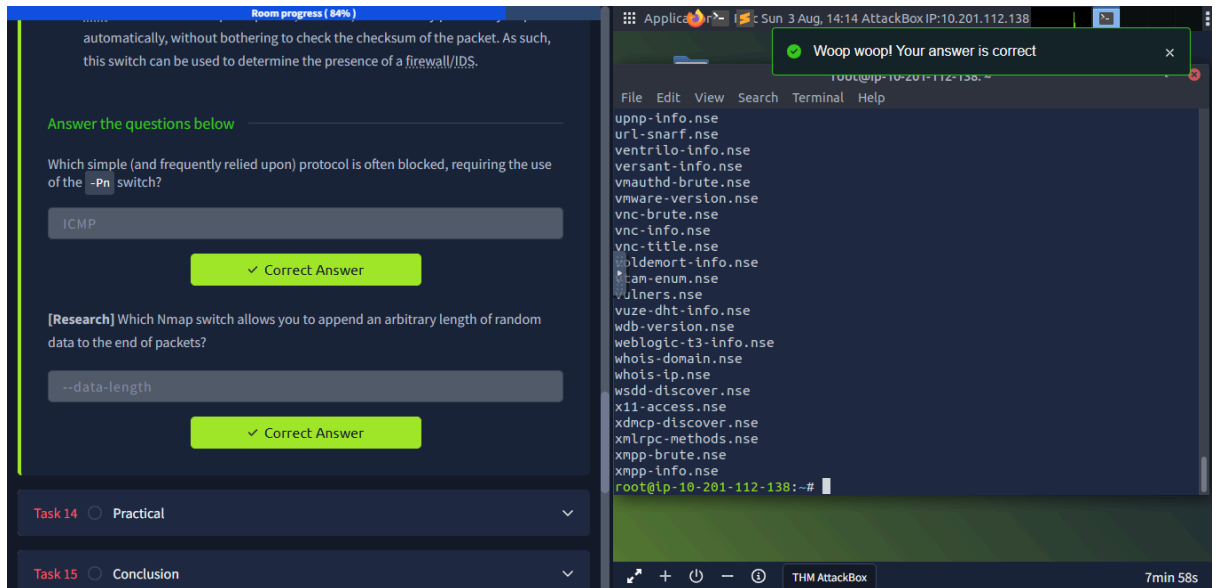


- **Question:** What is the filename of the script which determines the underlying OS of the SMB server?
 - **Answer:** `smb-os-discovery.nse`
 - **Command Used:** `ls /usr/share/nmap/scripts/smb*` or `grep "smb" /usr/share/nmap/scripts/script.db`
- **Question:** Read through this script. What does it depend on?
 - **Answer:** `smb-brute`

Task 13: Firewall Evasion

- **Objective:** Firewalls are a common obstacle. This task reinforces our firewall evasion skills, focusing on the essential `-Pn` switch. The objective is to understand why we need it and how it helps us scan targets that would otherwise appear to be

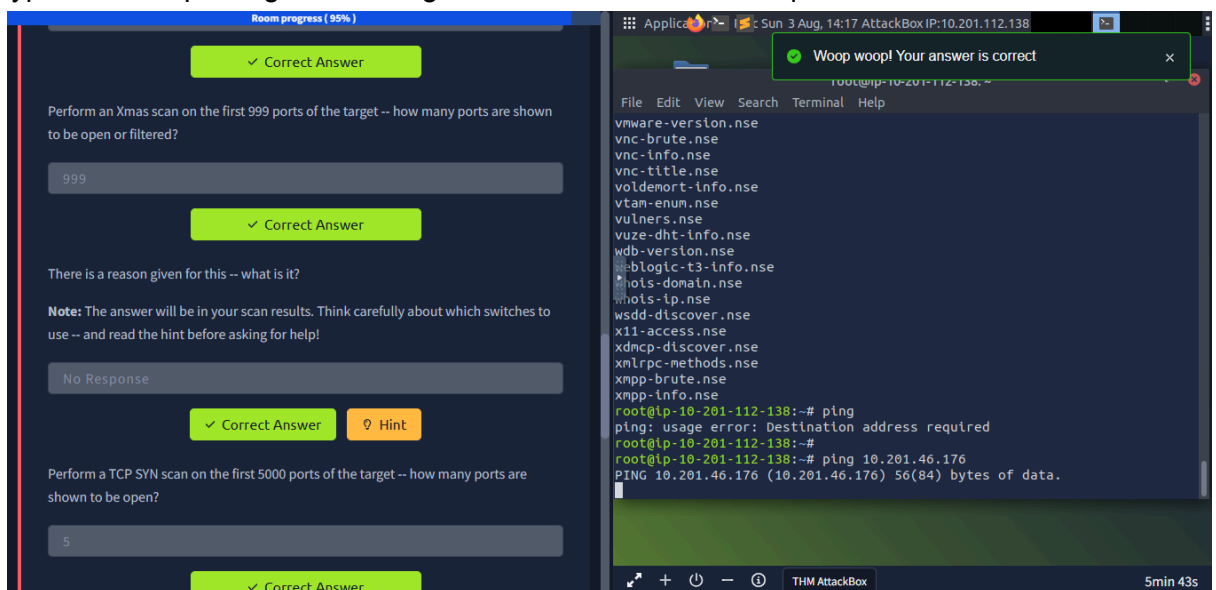
offline.



- **Question:** Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?
 - **Answer:** ICMP
- **Question:** Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?
 - **Answer:** --data-length

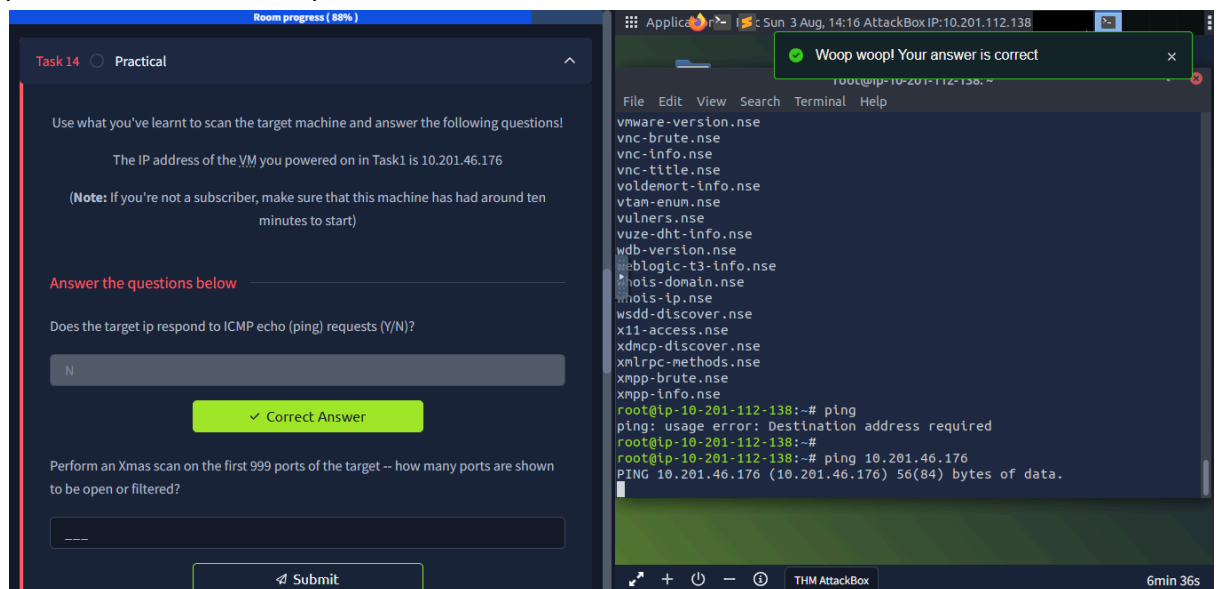
Task 14: Practical

- **Objective:** Time to put theory into practice. In this hands-on section, our goal is to use everything we've learned to scan the live target. We'll combine different scan types and scripts to gather intelligence and answer the final questions.



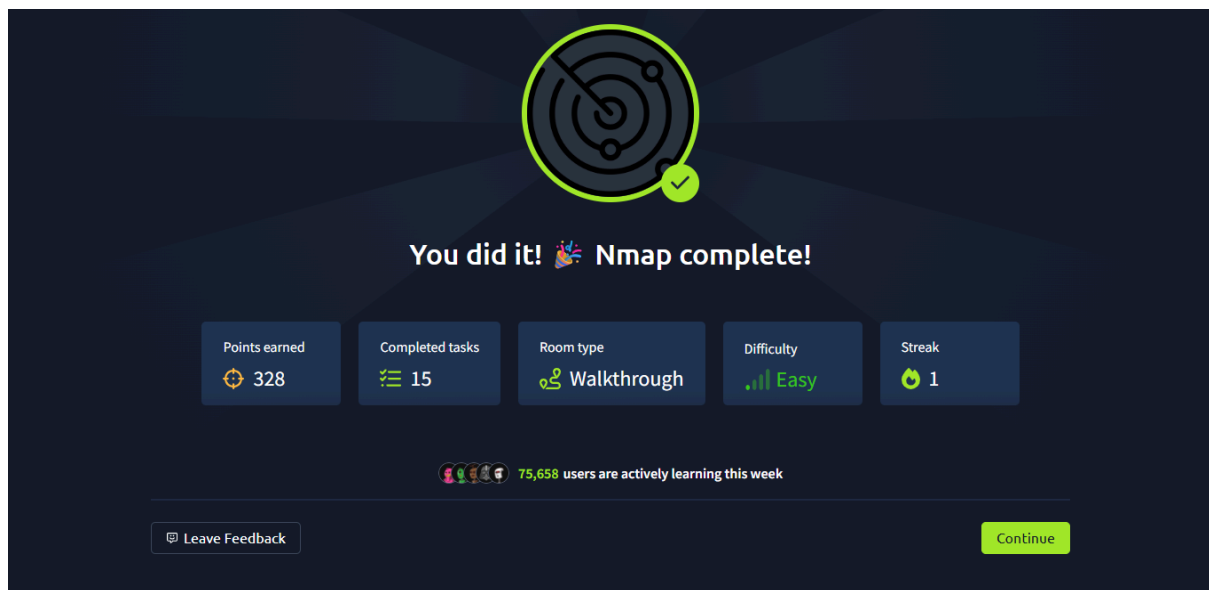
- **Question:** Does the target IP respond to ICMP echo (ping) requests (Y/N)?
 - **Answer:** N
 - **Command Used:** ping 10.201.46.176

- **Question:** Perform an Xmas scan on the first 999 ports of the target- how many ports are shown to be open or filtered?
 - **Answer:** 999
 - **Nmap Command Used:** `nmap -sX -p 1-999 10.201.46.176`
- **Question:** There is a reason given for this- what is it?
 - **Answer:** No Response
- **Question:** Perform a TCP SYN scan on the first 5000 ports of the target- how many ports are shown to be open?



- **Answer:** 5
- **Nmap Command Used:** `nmap -sS -p 1-5000 10.201.46.176`
- **Question:** Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)
 - **Answer:** Y
 - **Nmap Command Used:** `nmap -sC -p 21 10.201.46.176` or `nmap --script ftp-anon -p 21 10.201.46.176`

Task 15: Conclusion



- **Objective:** We've reached the end! This final step signifies the completion of the Nmap challenge, marking a solid milestone in our understanding of network scanning with this essential tool.
- **Result:** The Nmap room was successfully complete.