INTRODUCTION

Task 3: TryHackMe Further Nmap Report

Keshav S S

09/08/2025

Link to the room: TryHackMe Further Nmap

This report includes a tutorial for a beginner level TryHackMe room called FurtherNmap. The goal of this task was to learn advanced scanning techniques using Nmap, understand different scan types and apply them to identify vulnerabilities and services on a target machine.

TOOLS

Nmap

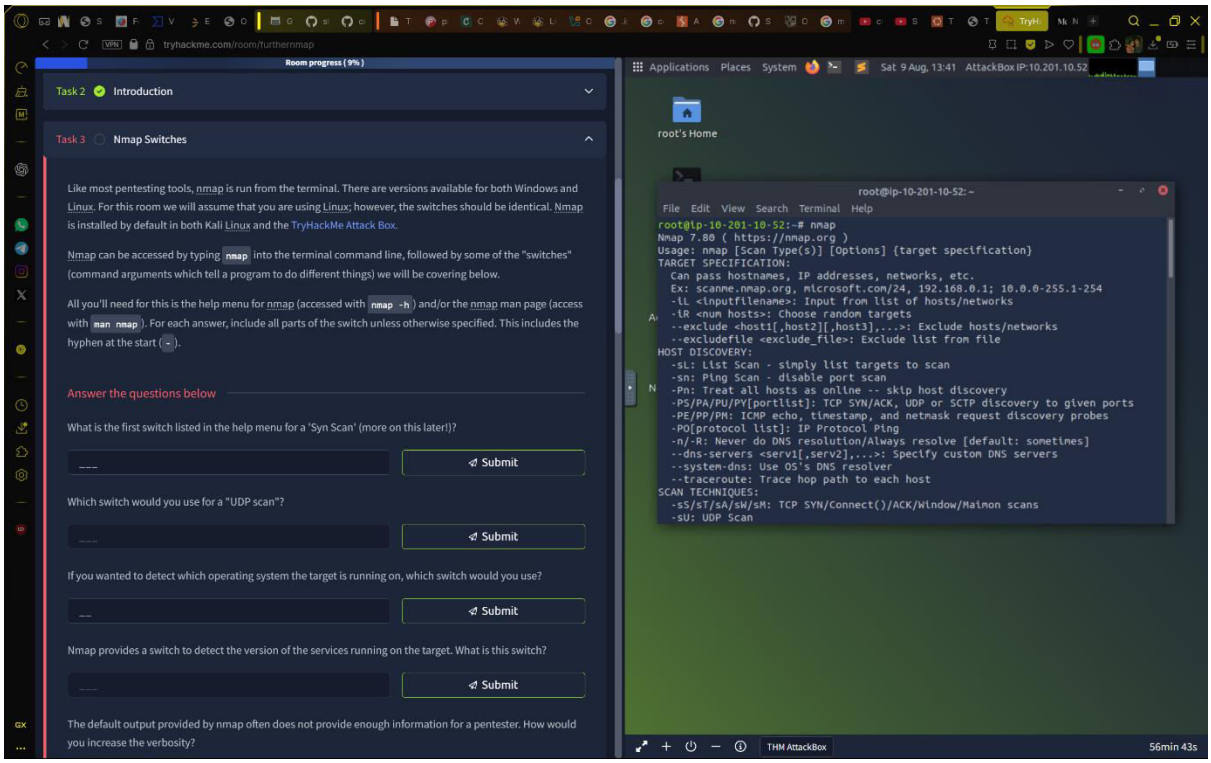
Linux VM provided inbuilt with the TryHackMe room (IP: 10.201.10.52)

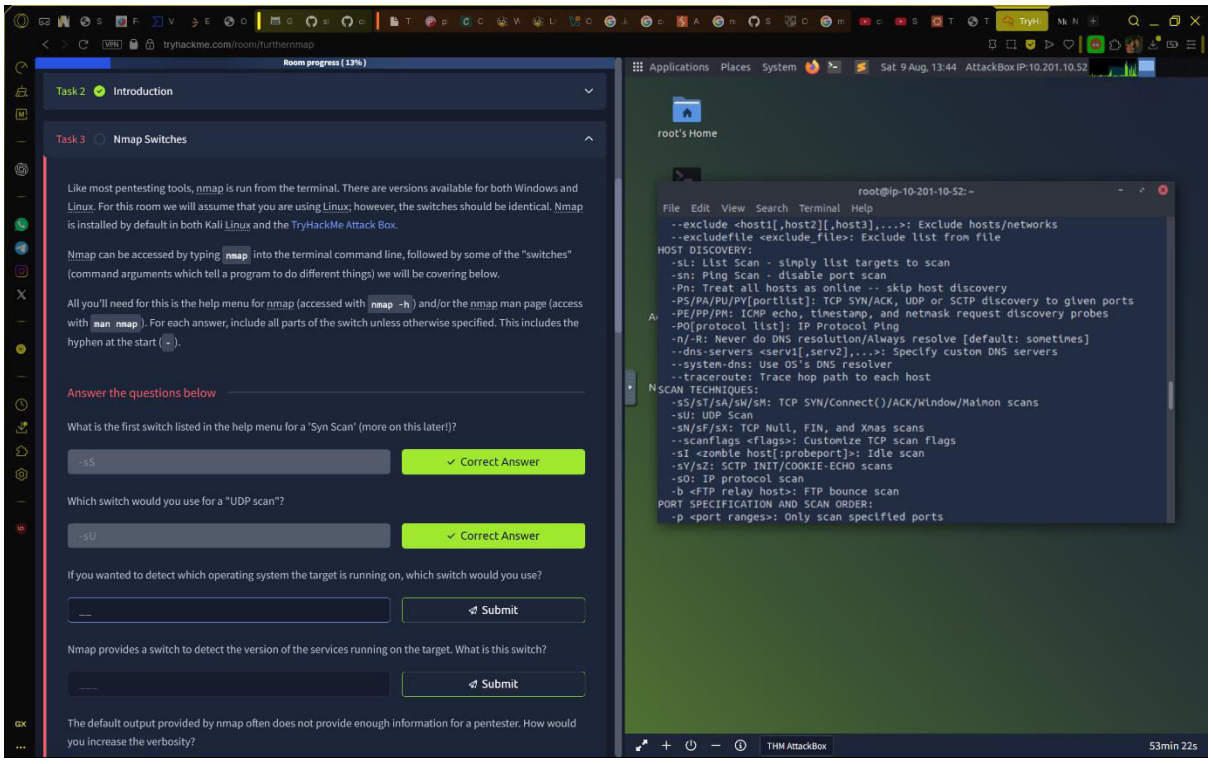
Attackbox provided inbuilt with the TryHackMe room (IP: 10.201.111.1)

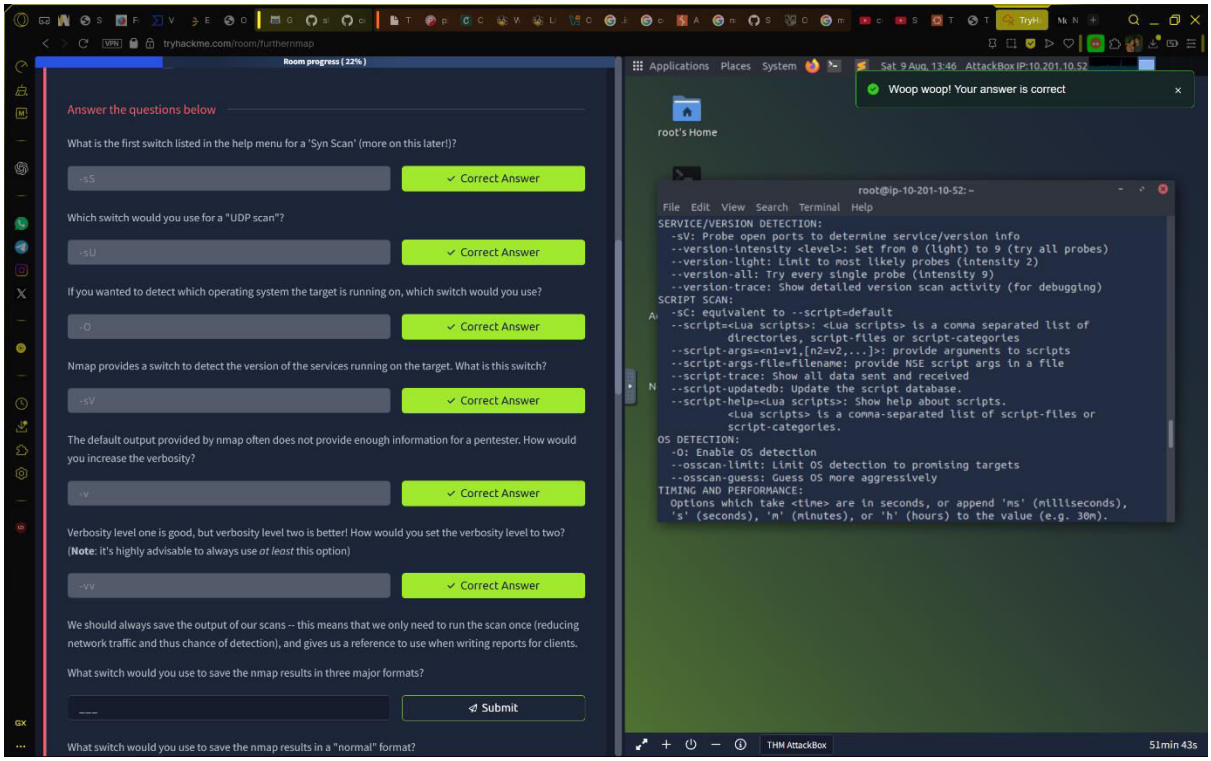
TASK

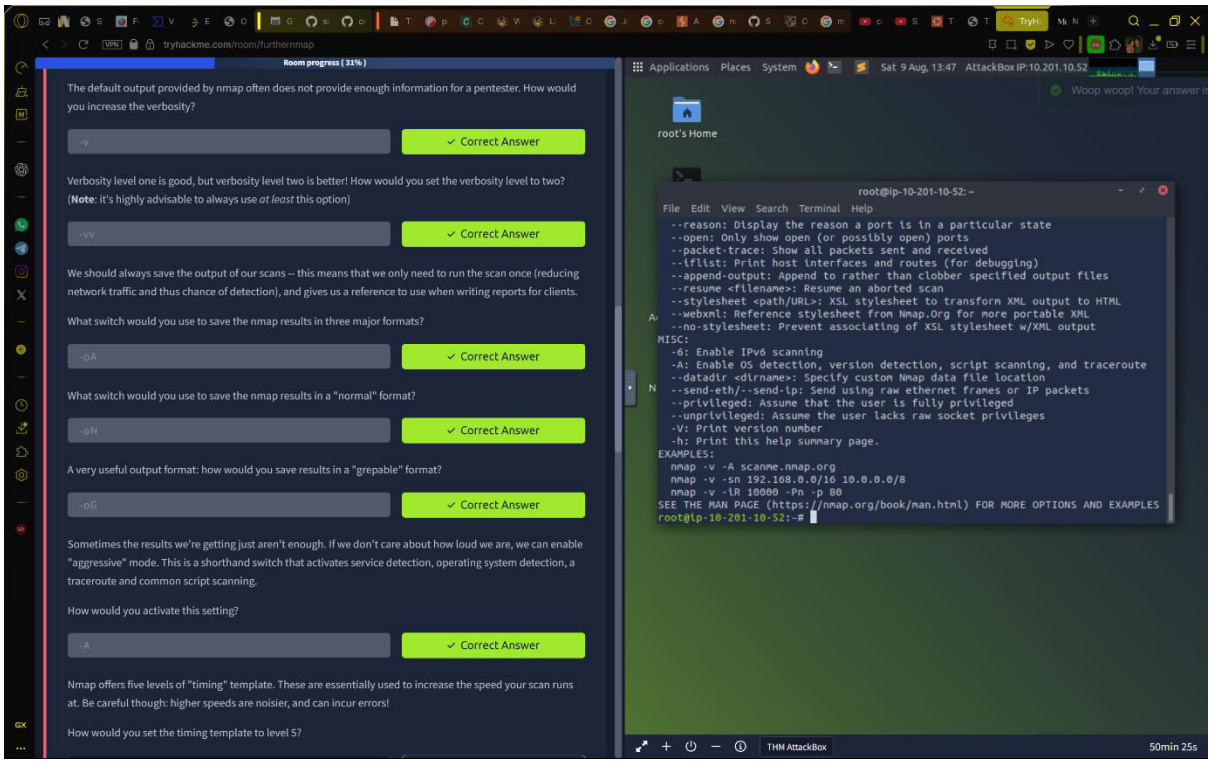
The task 5, task 6, task 7, task 10, task 11, task 13 answers could be easily found out by just reading the description part of the task. So, descriptions about them are not provided as it could be directly read out from the descriptions of the tasks.

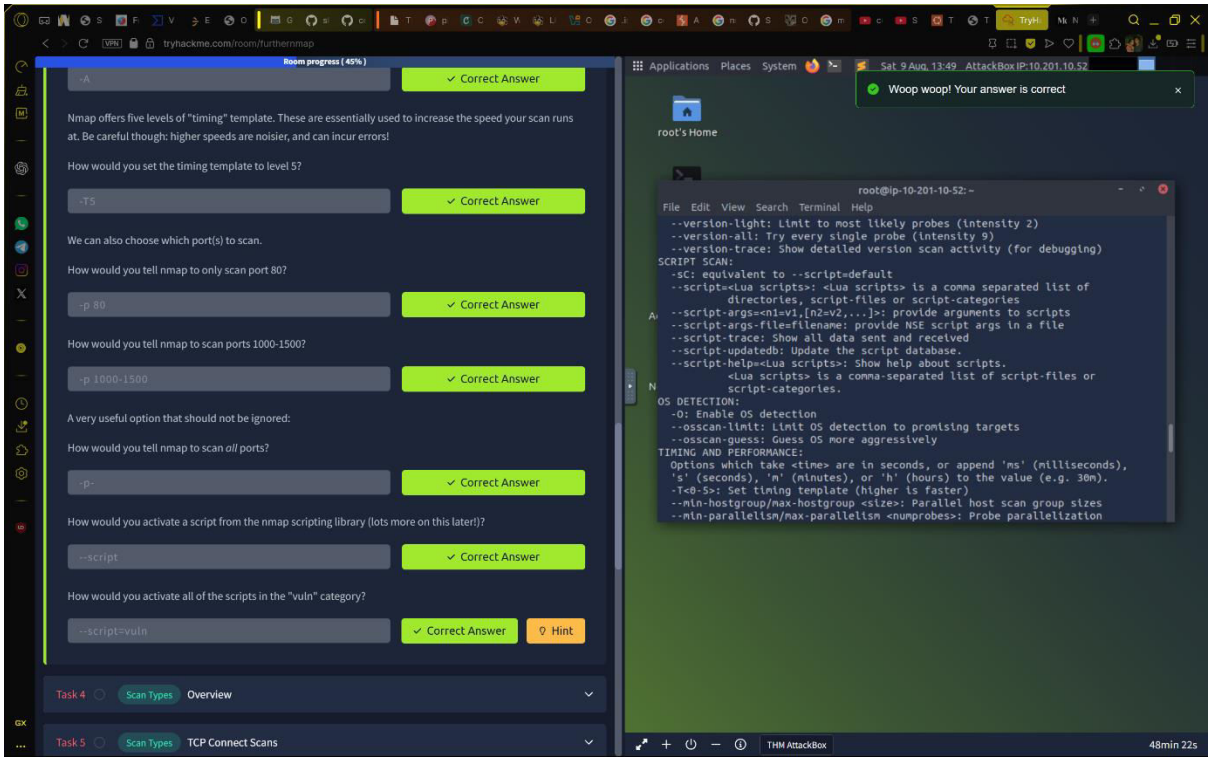
In task 3 I was able to get a knowledge on what Nmap does and how to look up the commands used in Nmap. There were a few questions to check our understanding of Nmap at the end of the task whose answers could be easily be found out using the command nmap -h.





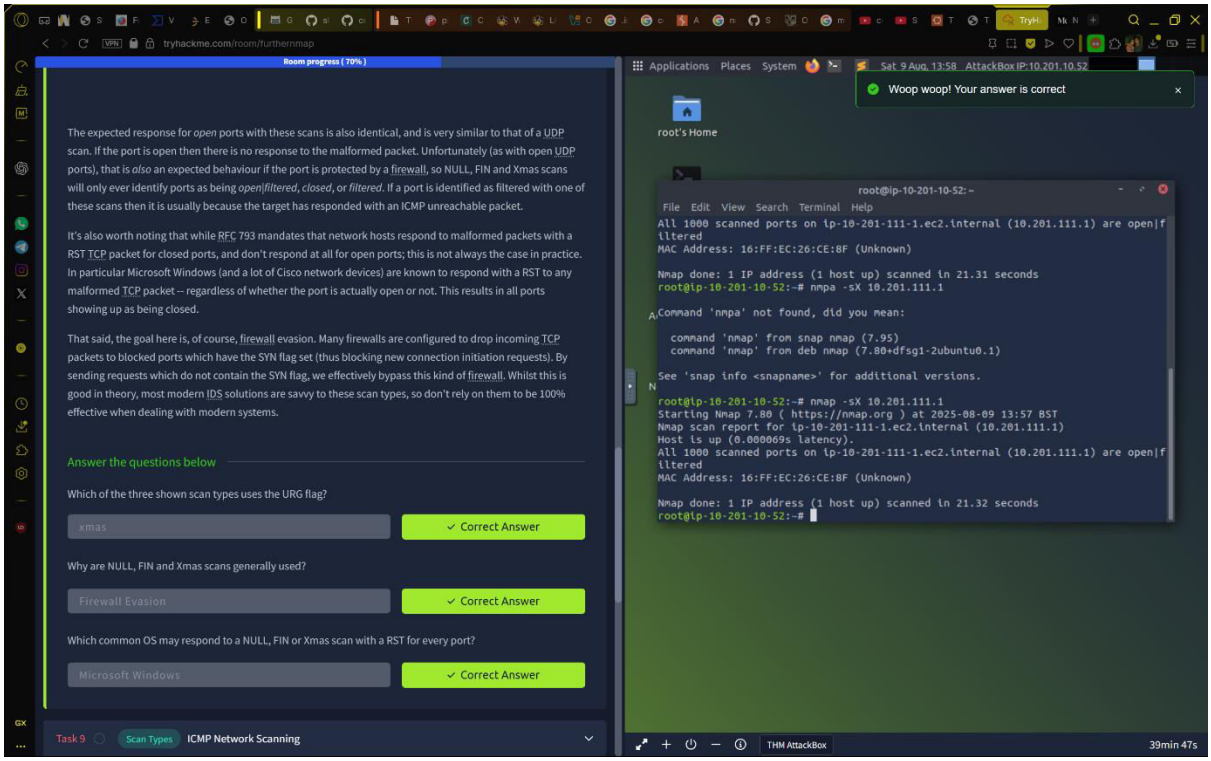

Room progress (22%)
Answer the questions below
What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?
-sS
Correct Answer
Which switch would you use for a "UDP scan"?
-sU
Correct Answer
If you wanted to detect which operating system the target is running on, which switch 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?
Submit
What switch would you use to save the nmap results in a "normal" format?
Applications Places System
Sat 9 Aug, 13:46 AttackBox IP:10.201.10.52
Woop woop! Your answer is correct
root's Home
root@ip-10-201-10-52: ~
File Edit View Search Terminal Help
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
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
<Lua scripts> is a comma-separated list of script-files or
script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
THM AttackBox
51min 43s


Room progress (31%)
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?
Applications Places System
Sat 9 Aug, 13:47 AttackBox IP:10.201.10.52
root's Home
root@ip-10-201-10-52: ~
File Edit View Search Terminal Help
--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
--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-10-201-10-52:~#
THM AttackBox
50min 25s

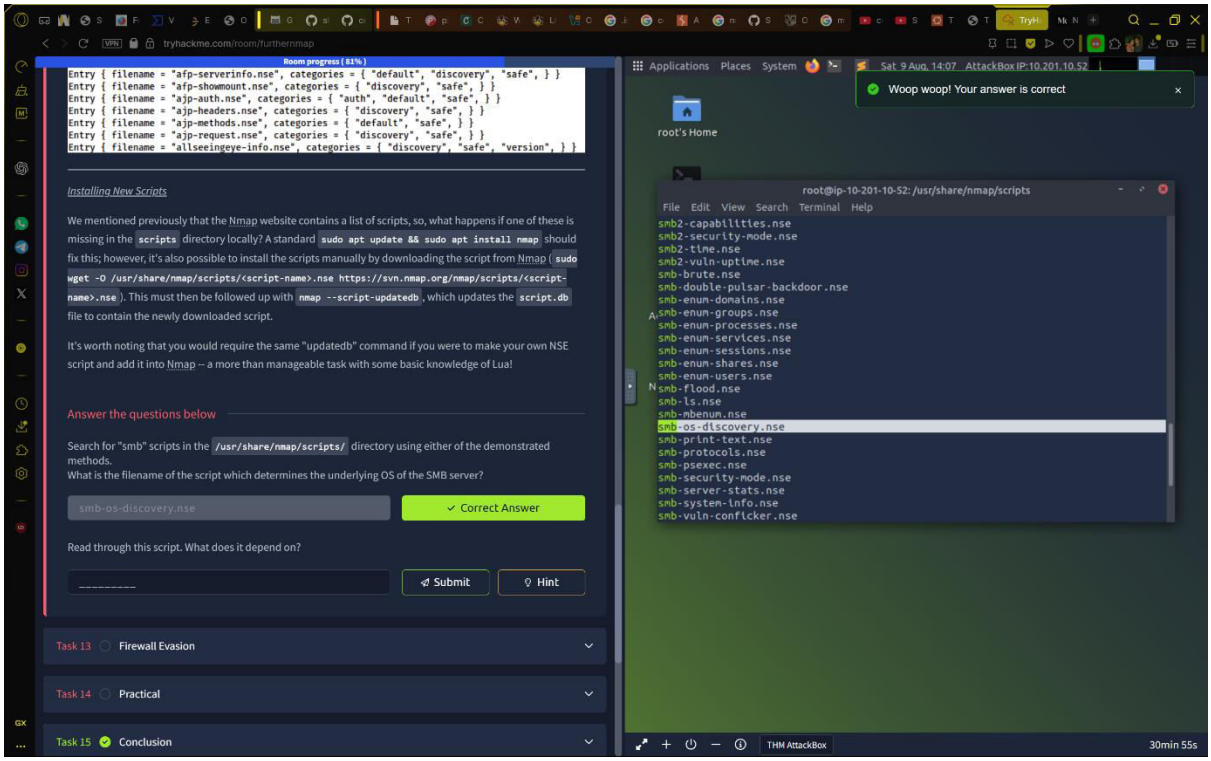


In task 8 I had to provide the command nmap -sX 10.201.111.1 to obtain the answer.

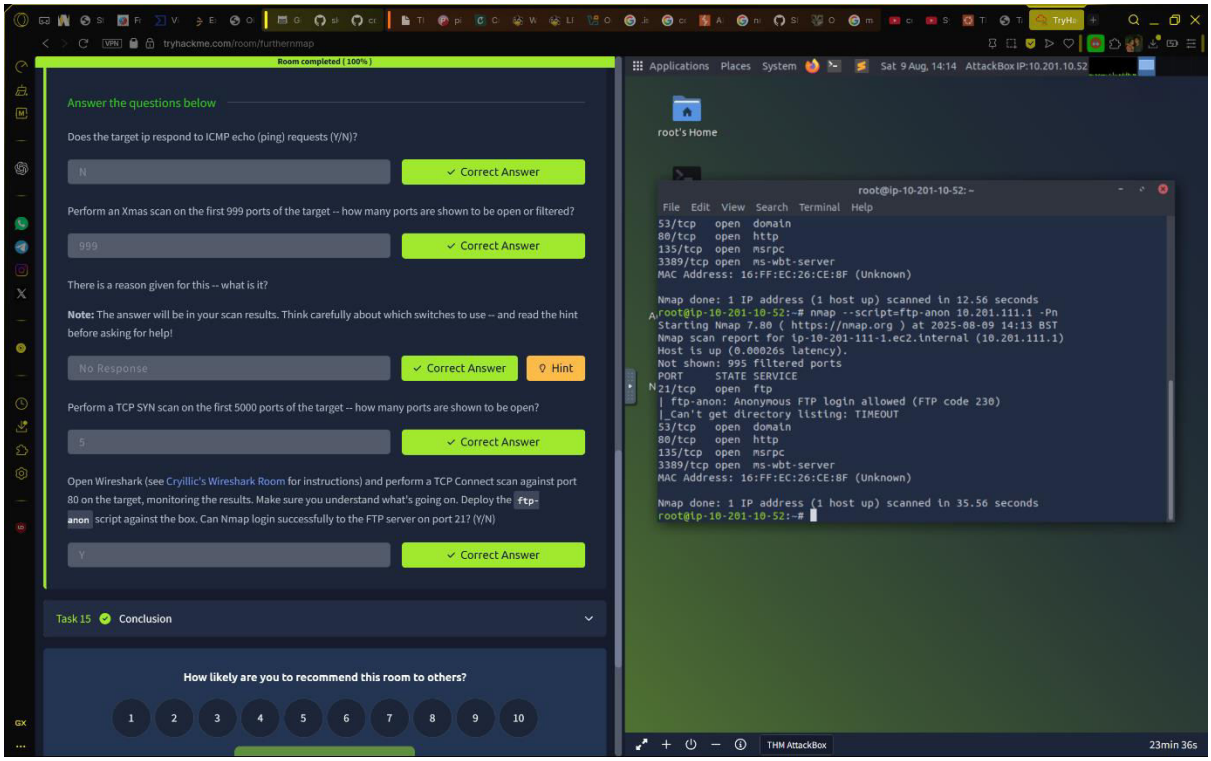
In task 9 I had to do the -sn scan to obtain the answer to the question provided.



In task 12 first I had to go into the [/usr/share/nmap/scripts/] directory and then had to run ls | grep smb in the terminal to obtain the answer.



In task 14 I had to run nmap -p1-999 -sX 10.201.111.1 -vv to identify how many ports are open, the reason for them to be open etc. I also had to run nmap -sS -Pn 10.201.111.1 to perform a TCP SYN scan. Another command nmap –script=ftp-anon 10.201.111.1 -Pn to check whether Nmap can successfully login to FTP server on port 21.


tryhackme.com/room/furthernmap
Room completed (100%)
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
Task 15 Conclusion
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Applications Places System Sat 9 Aug, 14:14 AttackBox IP:10.201.10.52
root's Home
root@ip-10-201-10-52: ~
File Edit View Search Terminal Help
53/tcp open domain
80/tcp open http
135/tcp open msrpc
3389/tcp open ms-wbt-server
MAC Address: 16:FF:EC:26:CE:8F (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds
root@ip-10-201-10-52:~# nmap --script=ftp-anon 10.201.111.1 -Pn
Starting Nmap 7.80 (https://nmap.org) at 2025-08-09 14:13 BST
Nmap scan report for ip-10-201-111-1.ec2.internal (10.201.111.1)
Host is up (0.00026s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
21/tcp open ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
53/tcp open domain
80/tcp open http
135/tcp open msrpc
3389/tcp open ms-wbt-server
MAC Address: 16:FF:EC:26:CE:8F (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 35.56 seconds
root@ip-10-201-10-52:~#
THM AttackBox
23min 36s