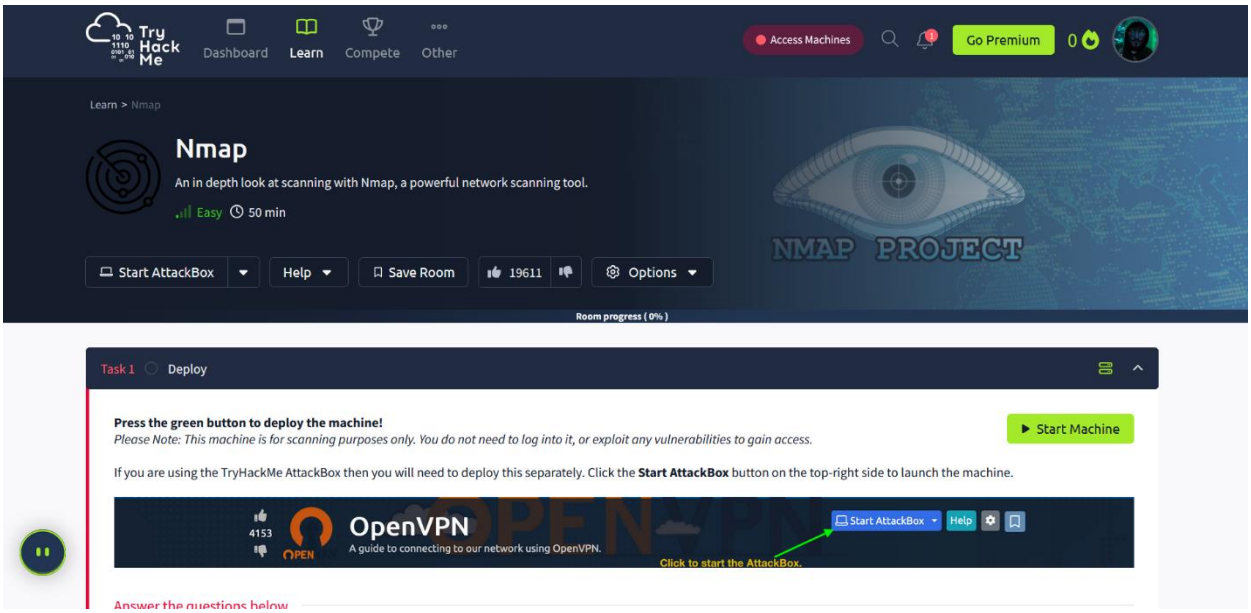
Task 3: Report on Further Nmap

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.

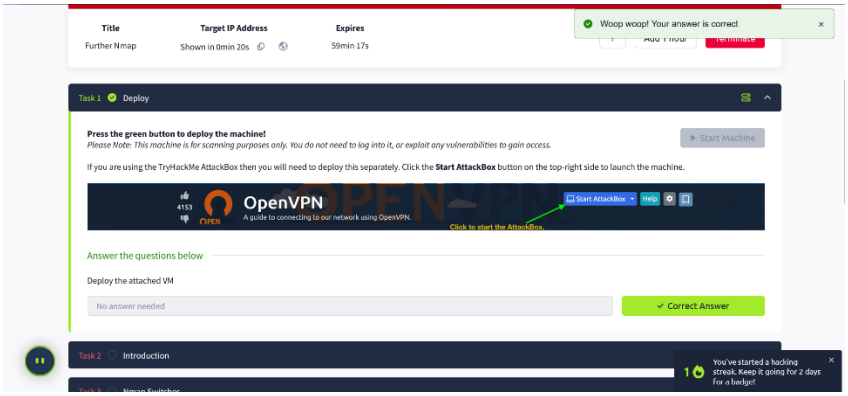


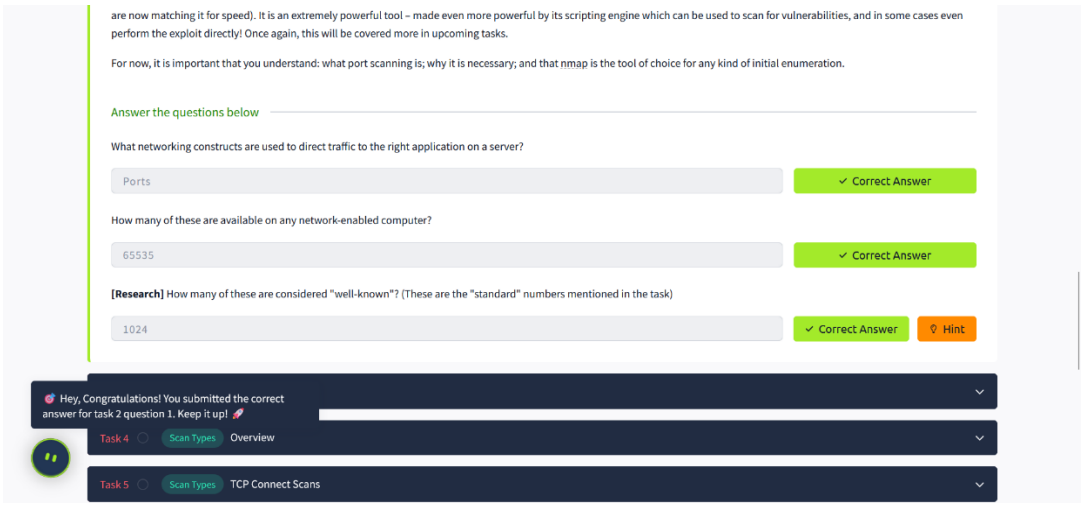
First we start this room and the attack-box of Try Hack Me.

Introduction to nmap:

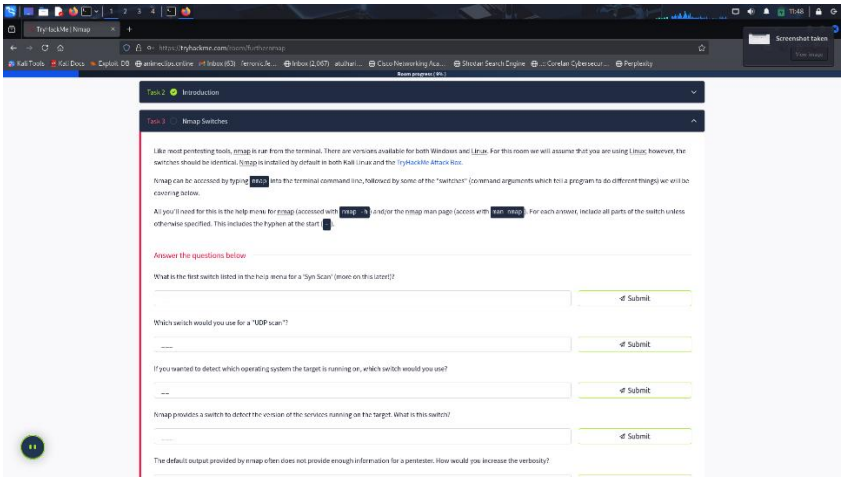
Nmap, short for Network Mapper, is a free and open-source network scanning tool used for network discovery and security auditing. It's primarily used to identify hosts, services, and open ports on a network, making it valuable for both security professionals and network administrators.

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

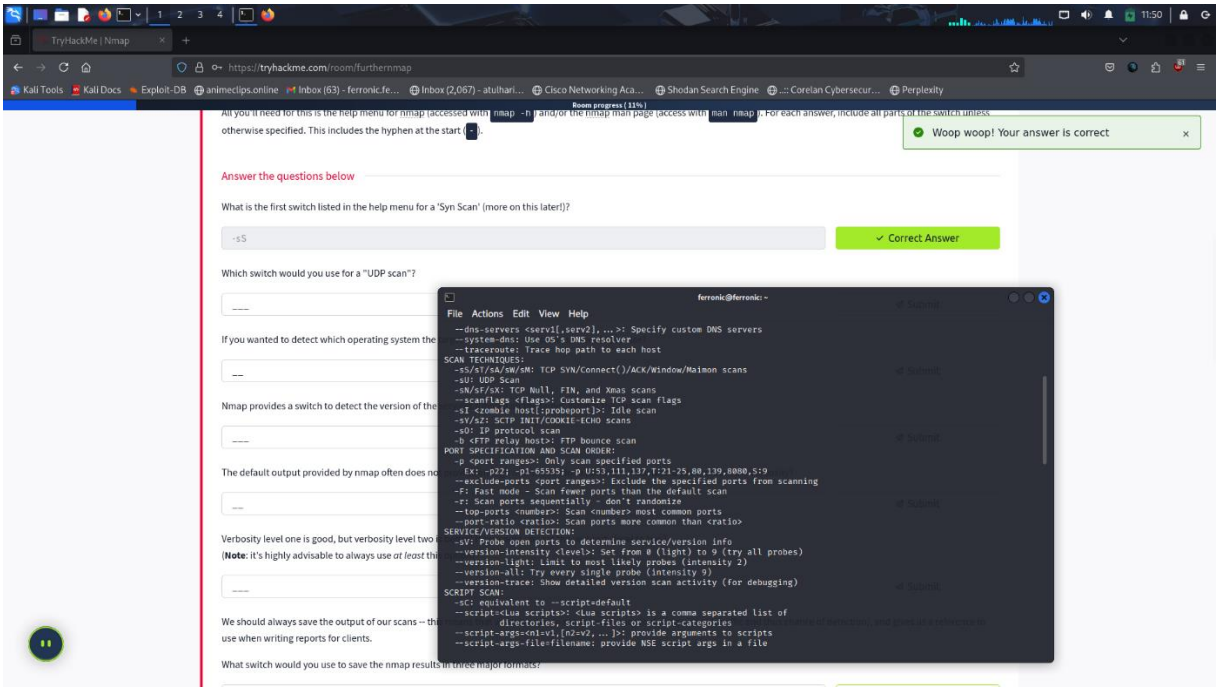




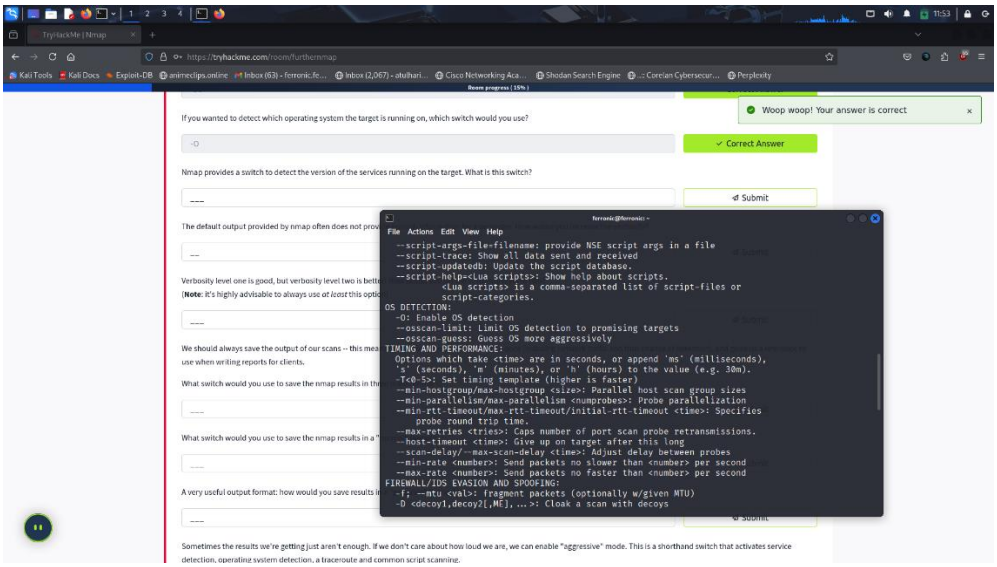
Task 2 of this room was an introduction, in which it clearly states all the answers to the questions asked. It introduces of Nmap and its uses, also hinting towards the port details.



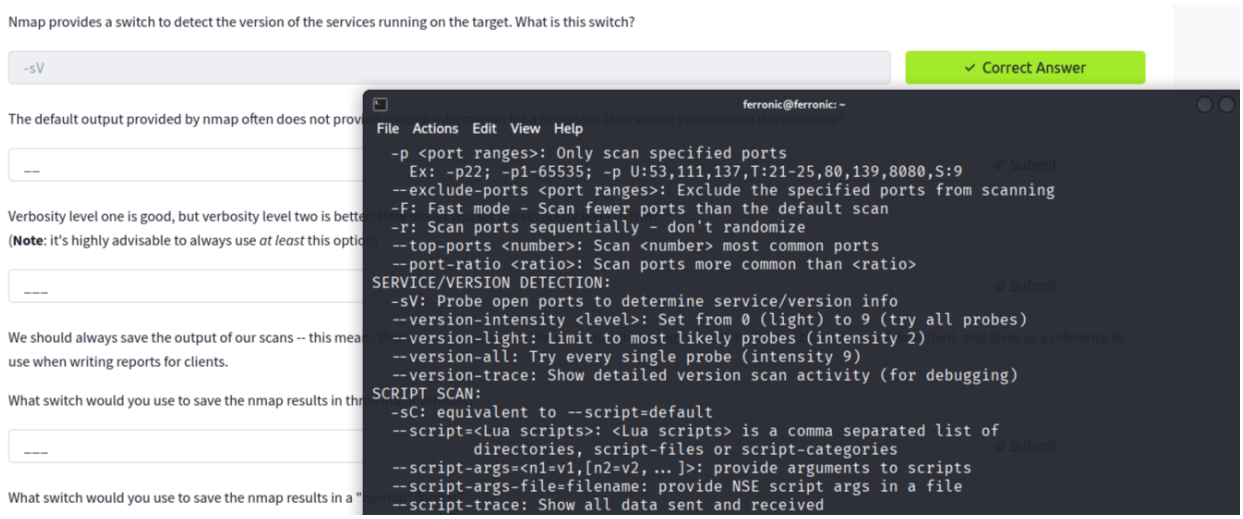
Moving on to task 3, it describes about the switches of nmap. When we do the nmap -h we get:



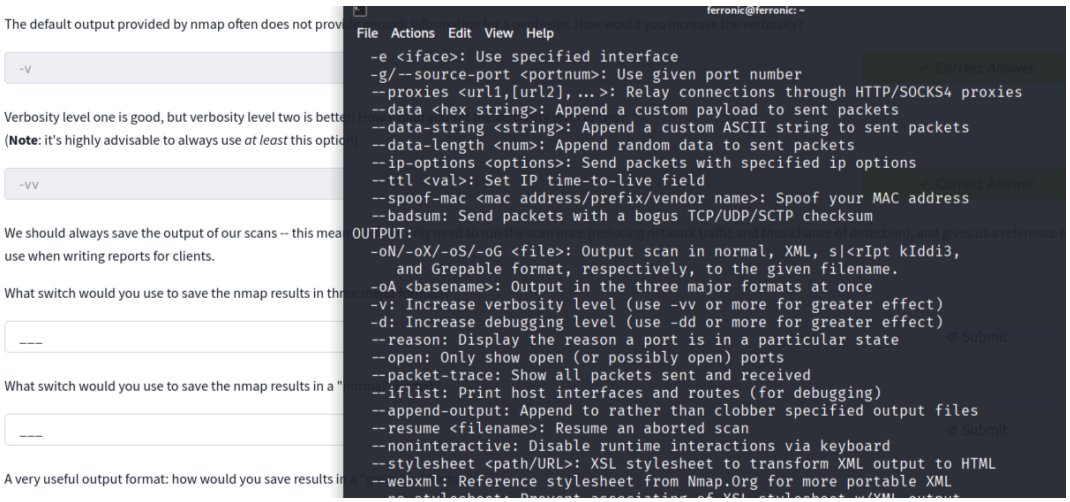
From this we know the first 2 answers, for Syn Scan -sS and for a UDP scan it is -sU.



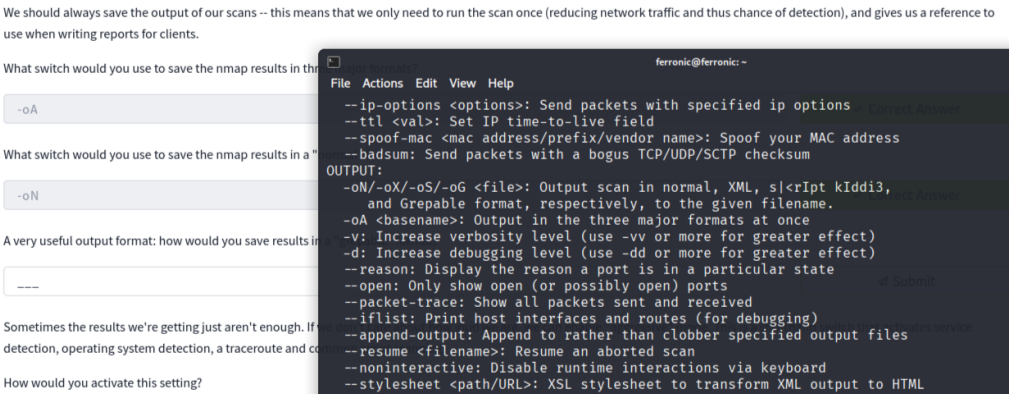
The next question describes the OS detection method. For that we use -O in nmap.



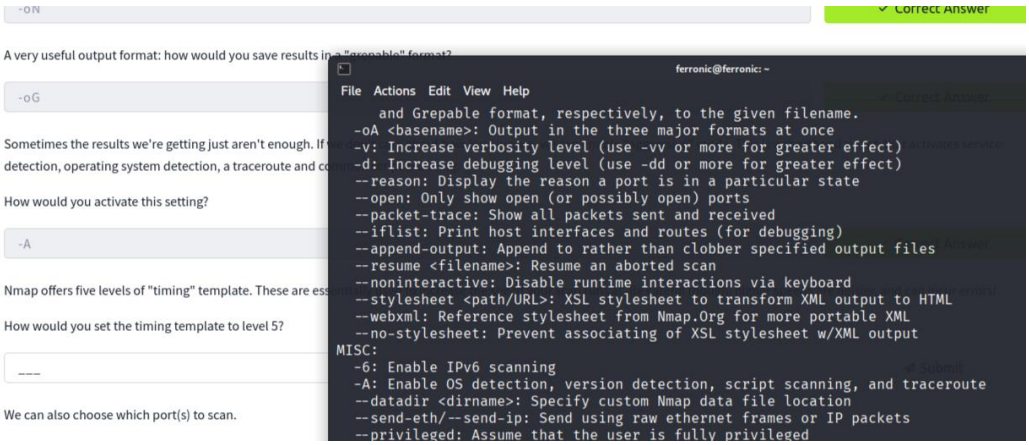
-sV is used for version scan.



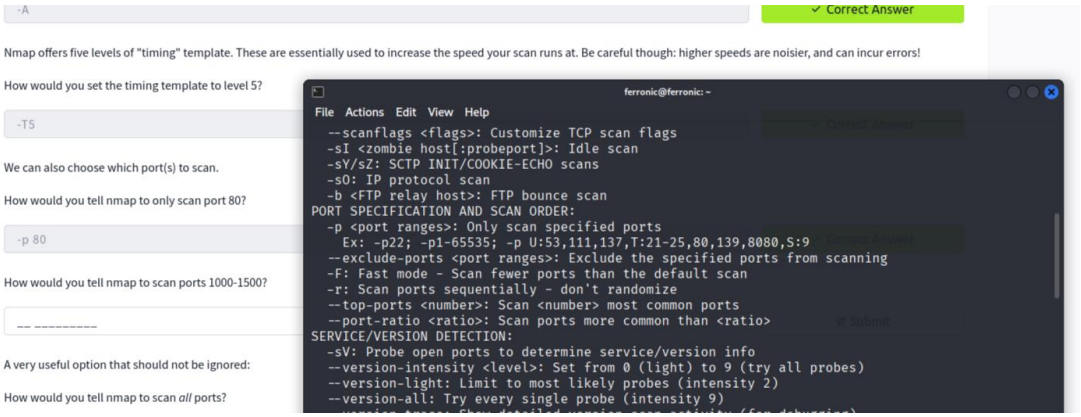
-v is used for increasing the verbosity level. -vv for more greater effect.



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

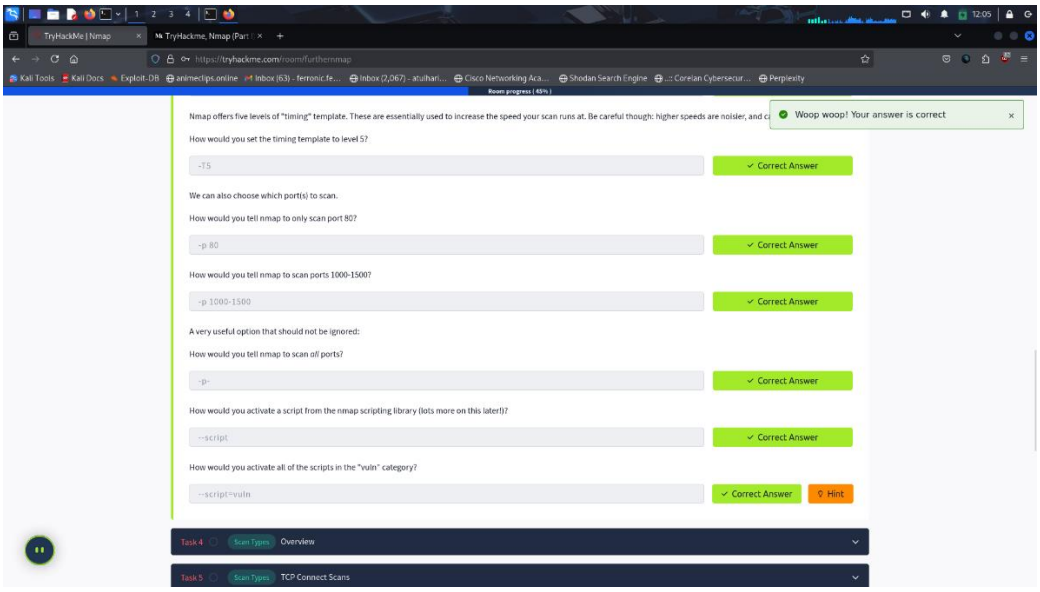


-oG is used to save the details in a grepable format. It is also considered to be very useful.

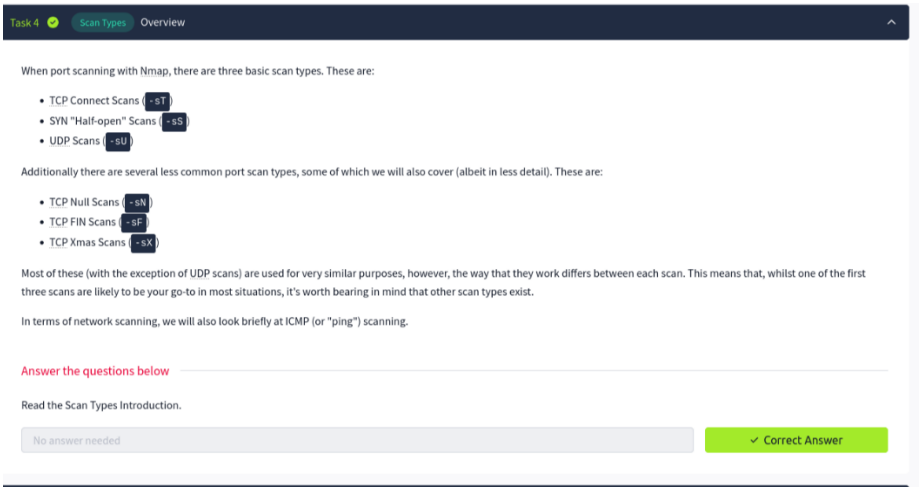


-p is used to define the ports for scanning the target. So if you had to scan port 1000-1500, we can use -p 1000-1500. To scan all ports, which is time consuming we use -p-.

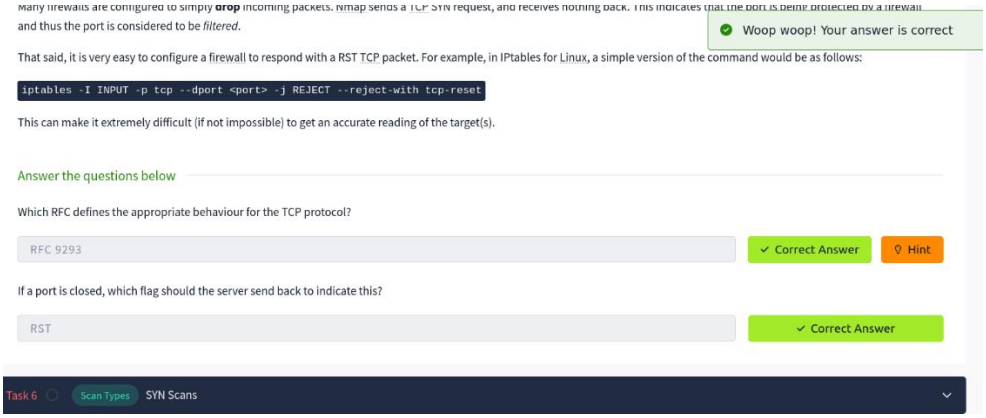
To access the scripts from library we use –script.



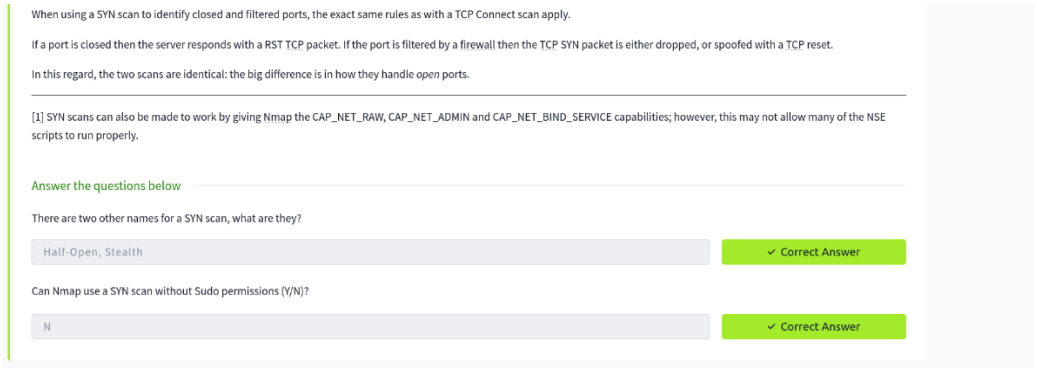
Then we move on to task 4. In task 4 we are assigned to read about scan types.



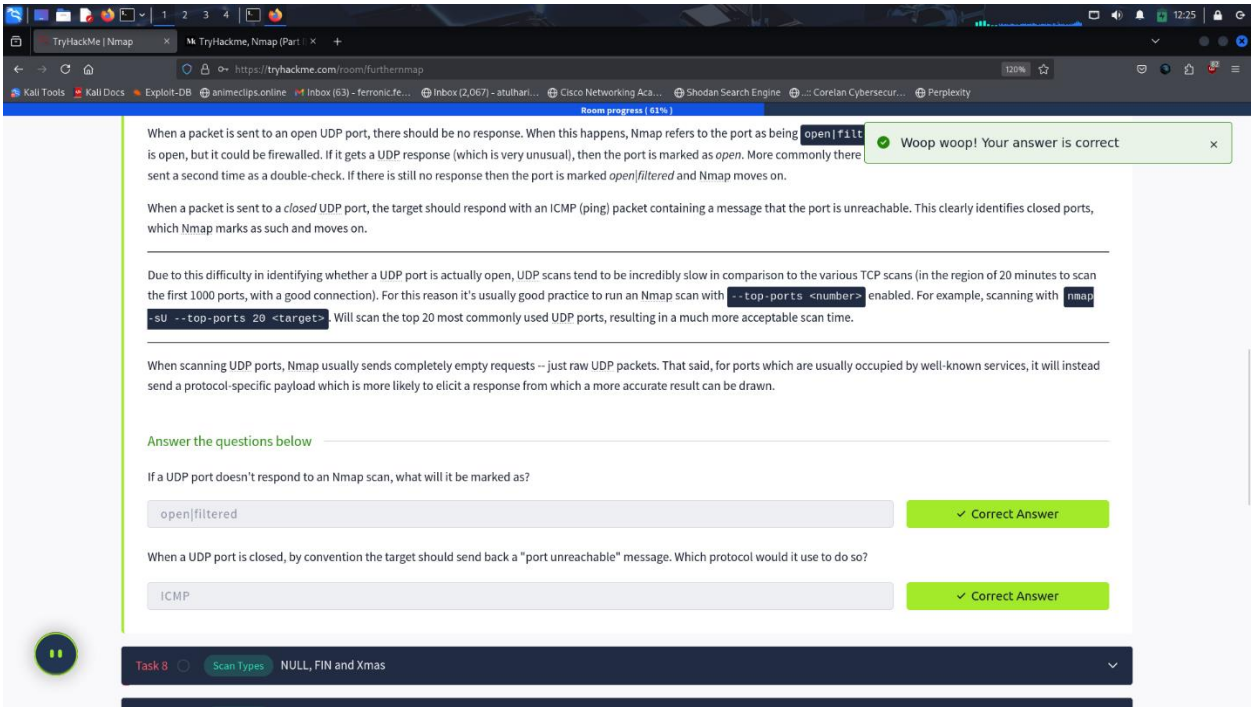
Task 5 consist of reading TCP connect scans. We have answers to the questions asked in the following reading session which will briefly make us aware of the three way handshake. Introduce the SYN, ACK, SYN-ACK, RST requests.



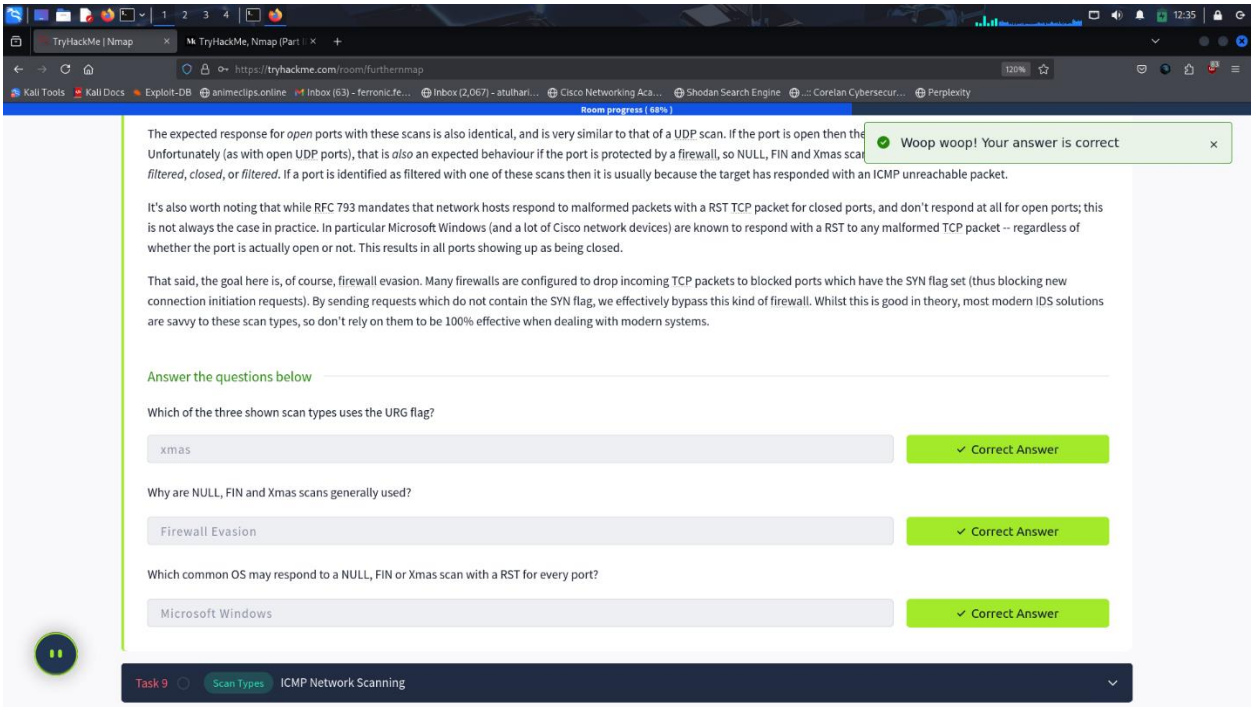
Now we completed task 5, lets move on to task 6, in which the details of SYN scan and its other names are mentioned.



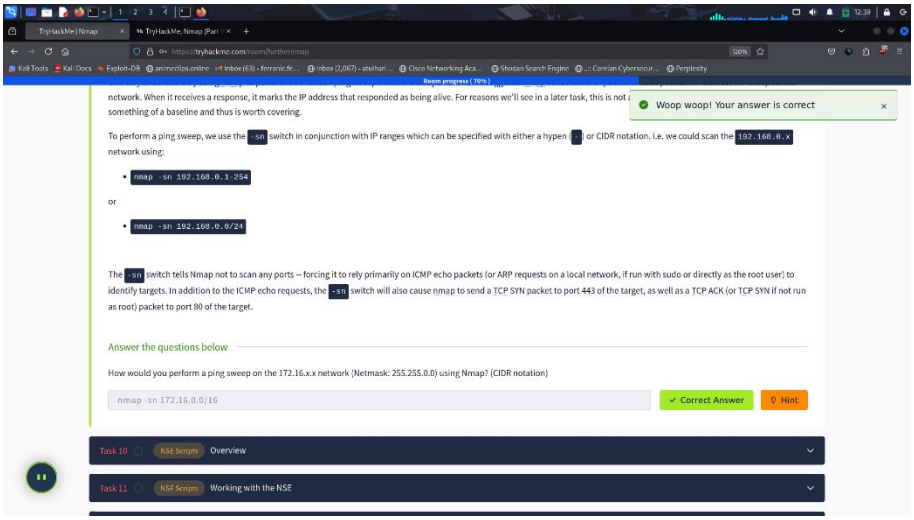
Half open or stealth scan is the other terms used for SYN scan. Nmap require sudo permission for SYN scan.



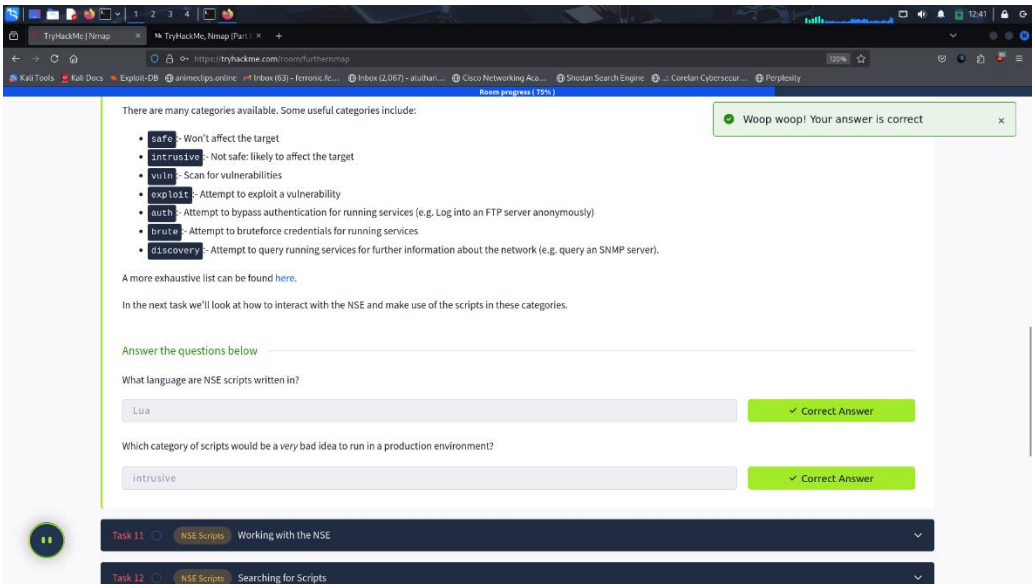
Task 7 consist of reading session about UDP. If a UDP port doesn’t respond to Nmap scan it usually shows open|filtered. The protocols used are ICMP for the host to receive port unreachable message from the target.



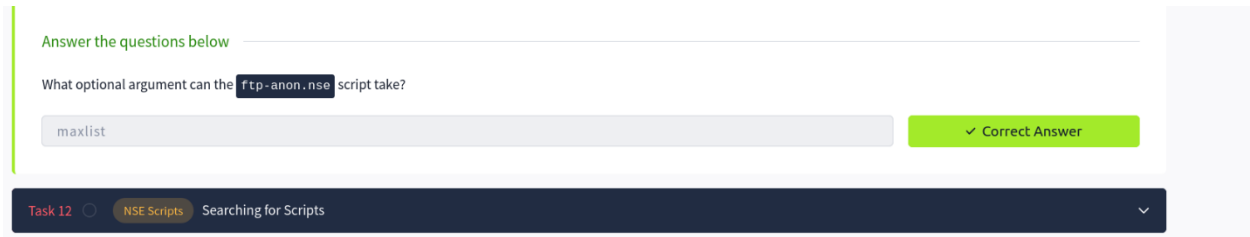
Task 8 consist of reading part of NULL, FIN and XMAS. The URG flag is used by XMAS scan . PSH,URG and FIN are used in xmas scan (-sX).



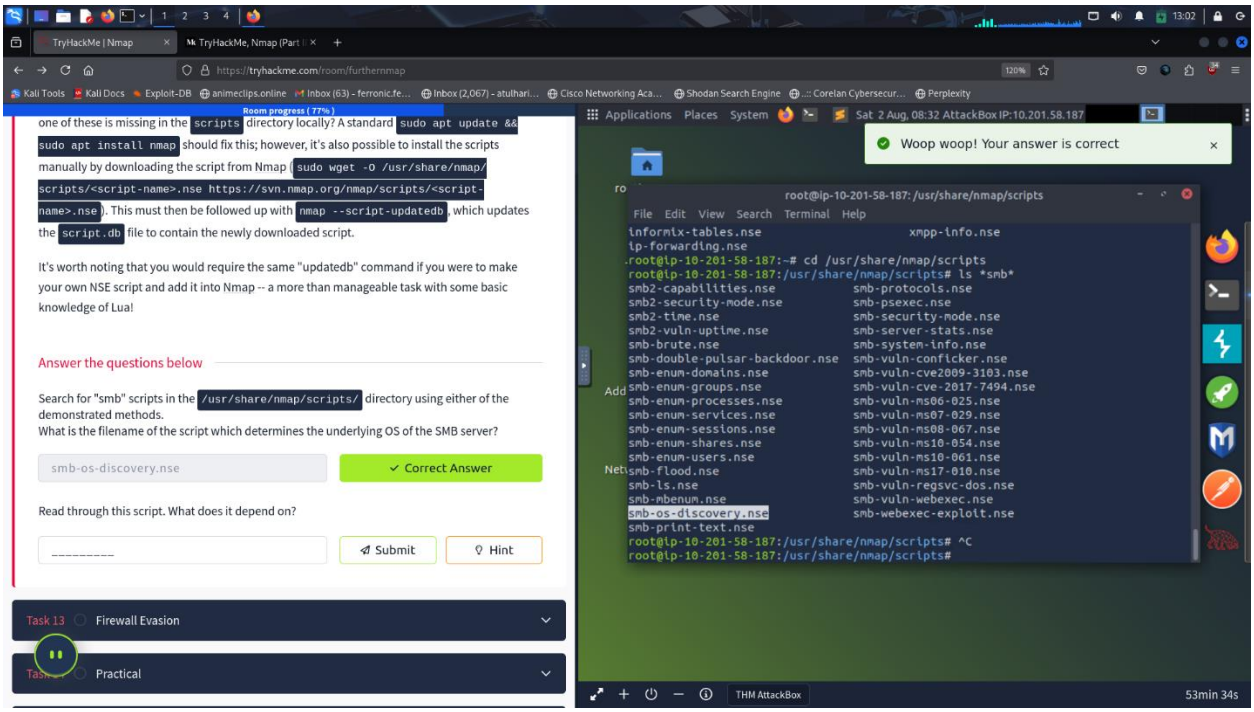
From the above example we can use a similar ping method to extract the answers for this question using nmap.



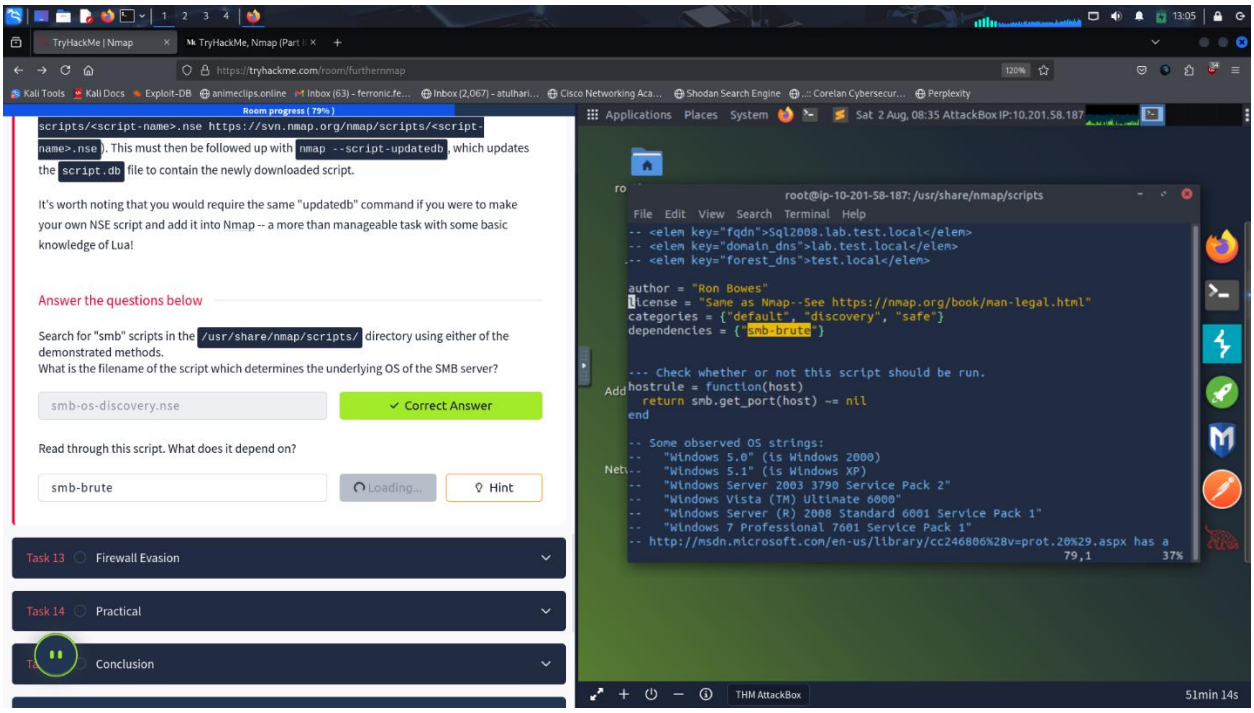
Task 10 is an overview of NSE. Lua is a programming language used for NSE scripts. Intrinsive script is not safe and is likely to affect the target.



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

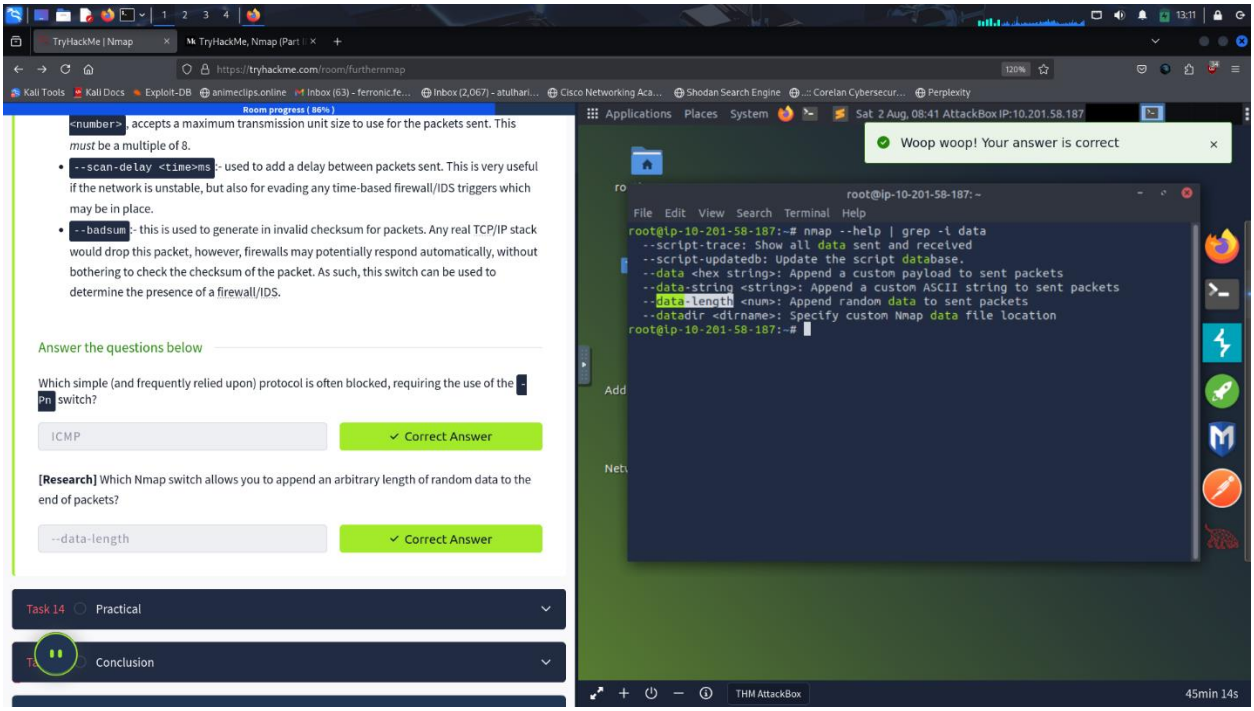


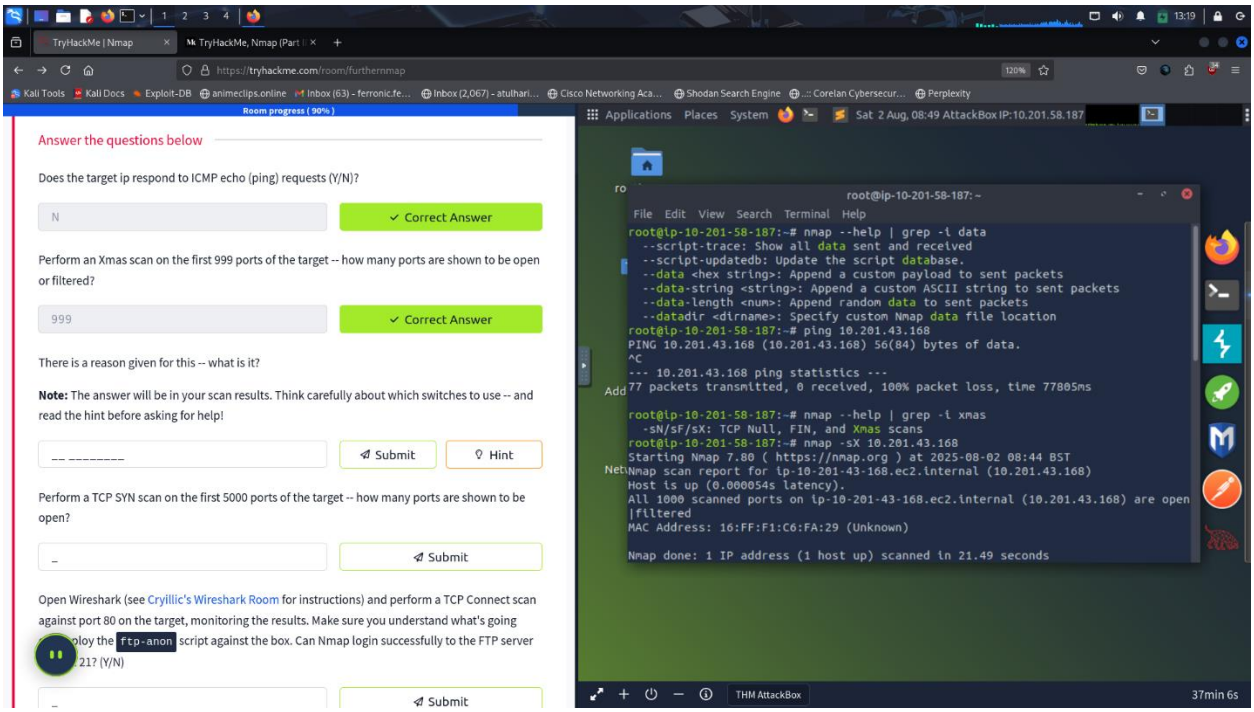
In task 12 , we had to access the script library and then find the smb script from it.



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

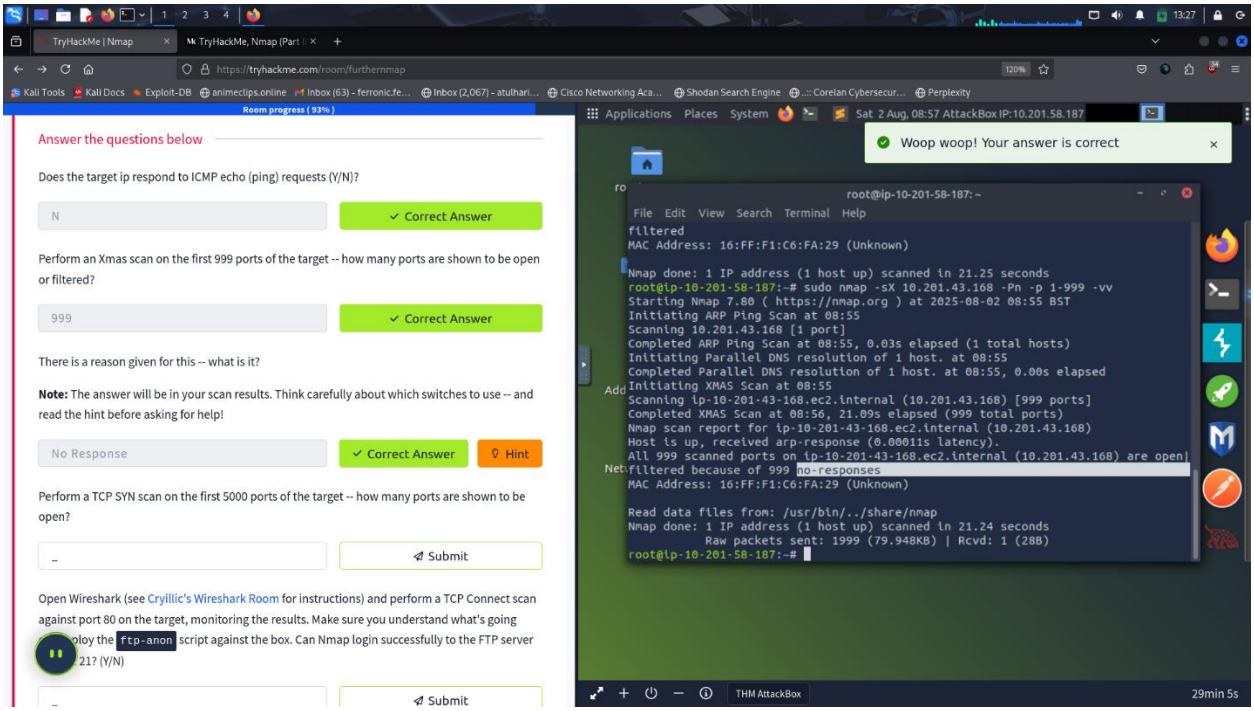
Then we have task 13 which is firewall evation, ICMP protocol is most necessary. The option for -pn switch is mentioned.

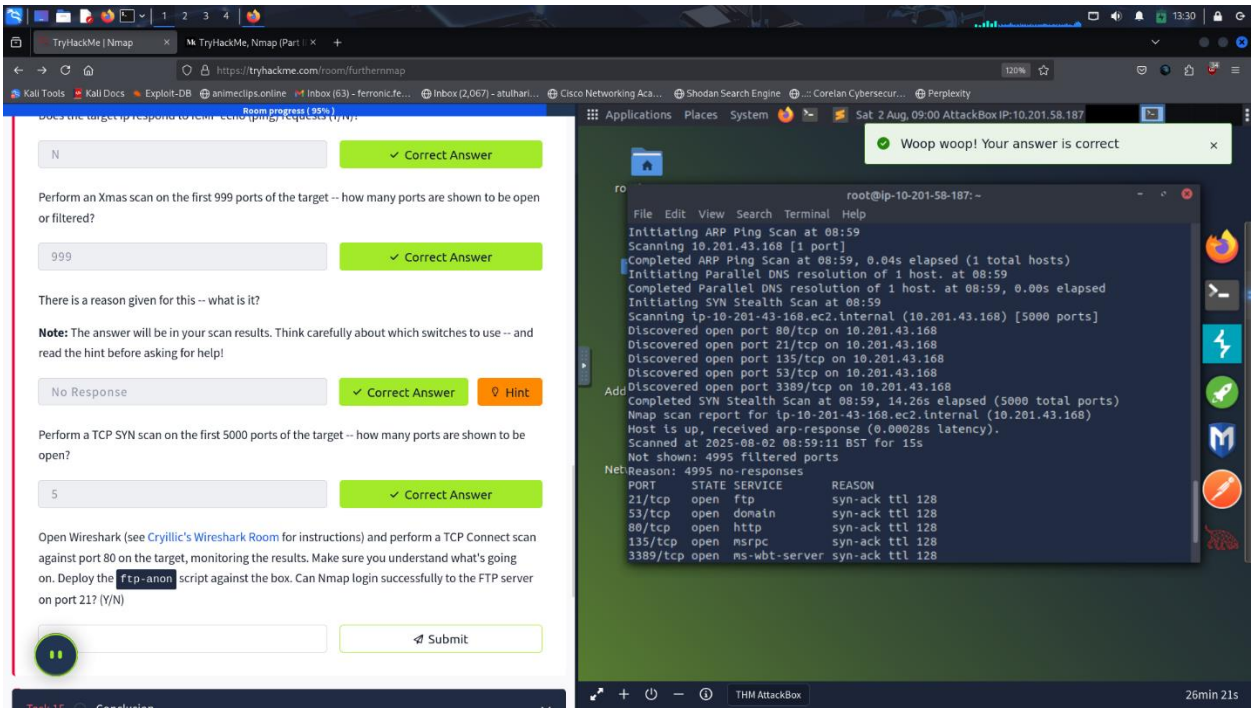




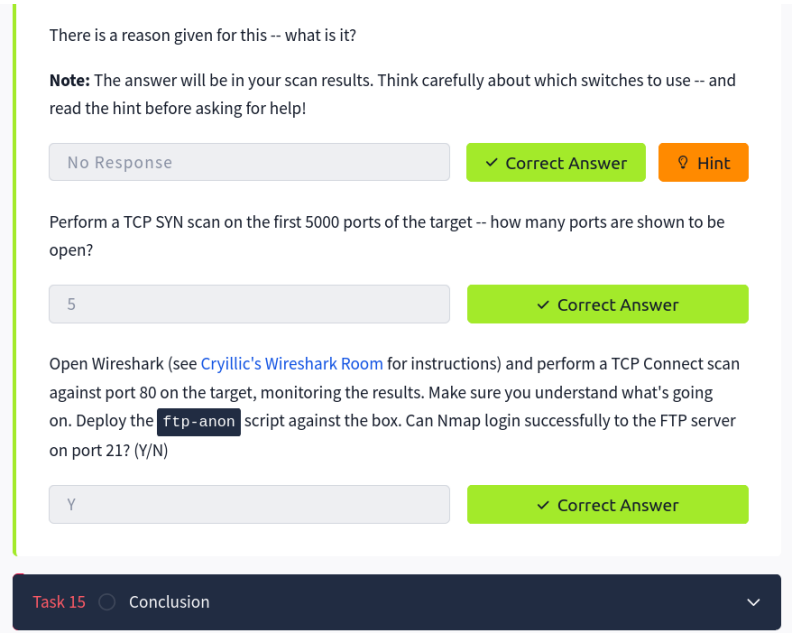
We had our task 14, in which it tested our practical skills using nmap to scan and gather info after we have been given a target IP (which we get after initial starting of the machine).

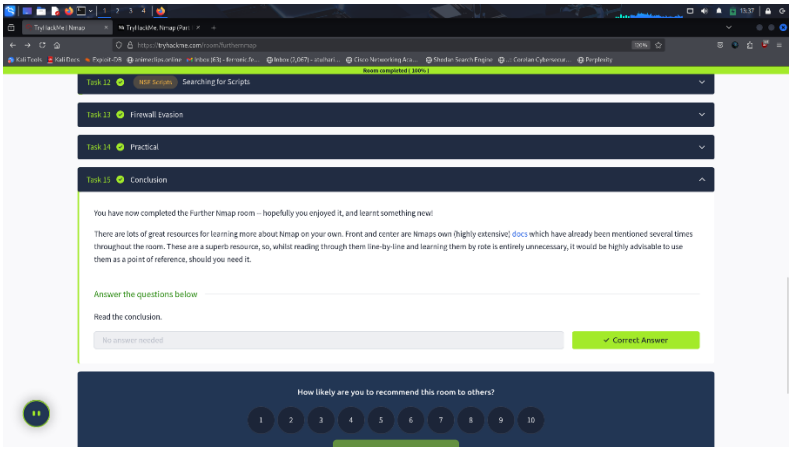
We didn’t receive any ping response form the target IP. Using Xmas scan all 999 ports were open.



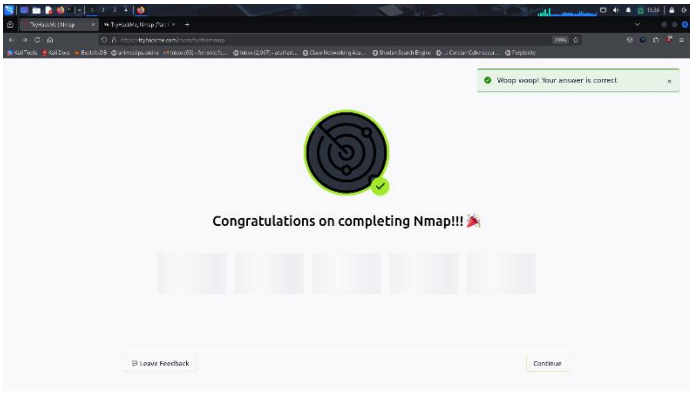


We got a total of 5 responses for TCP SYN scan on the first 5000 ports.





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.