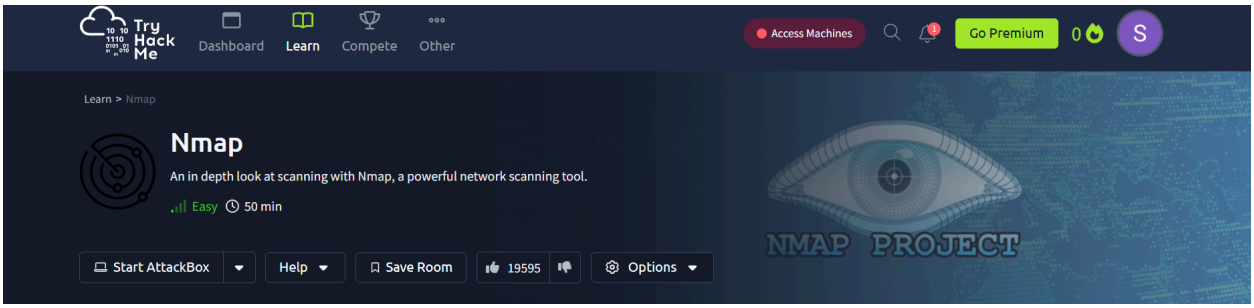
TryHackMe Write-up

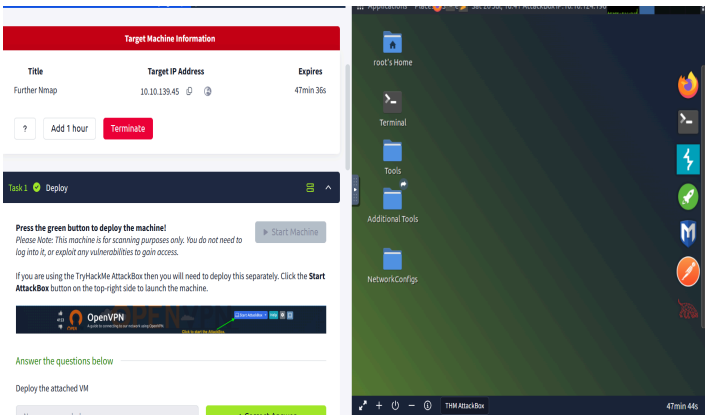
Room: Nmap
Prepared by: Shifna N.
Date: July 30, 2025

•Introduction

This report summarizes the completion of the "Nmap" room on TryHackMe. This room covered its different scan types, options, and capabilities, including how to use Nmap effectively in real-world penetration testing scenarios. Each task in the room included hands-on exercises and questions, which have been answered using screenshots for proof and are explained in this report.



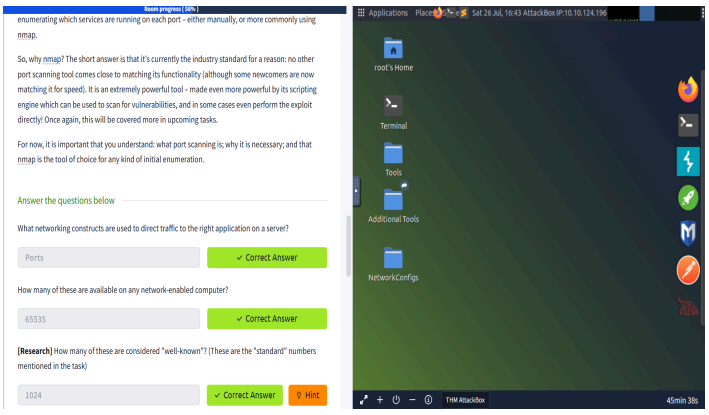
•Task 1: Deploy



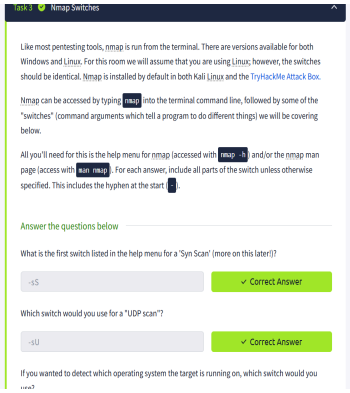
In this task, we deployed the target machine provided by TryHackMe. This step is essential as all the practical exercises depend on having an active target system. A green message indicated that the machine had been successfully deployed. After deployment, we waited for the IP address to be assigned and confirmed connectivity before moving on to the scanning tasks.

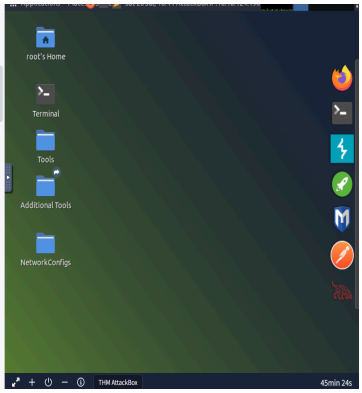
•Task 2: Introduction

This task gave a simple introduction to Nmap and how it is used in ethical hacking. It showed that Nmap helps scan open ports, find running services, and collect basic details about systems on a network.The task also introduced the room's structure, which includes multiple scan types and techniques that Nmap supports.



•Task 3: Nmap Switches

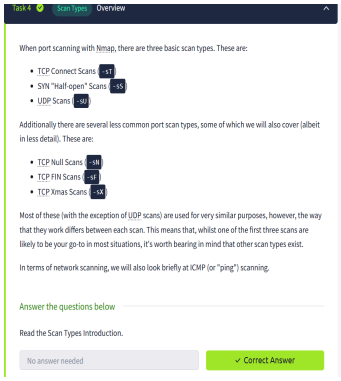


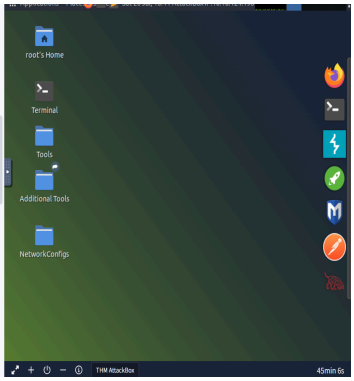


Here, we explored the different switches or command-line options that Nmap provides. We learned about commonly used switches like `-sS` for SYN scan, `-sT` for TCP Connect, and `-sU` for UDP scans. Other useful switches such as `-p` for specifying ports, `-A` for aggressive scan, and `-T` for timing templates were also covered. These switches help customize scans depending on the situation.

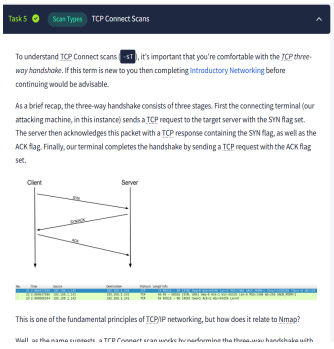
•Task 4: Scan Types Overview

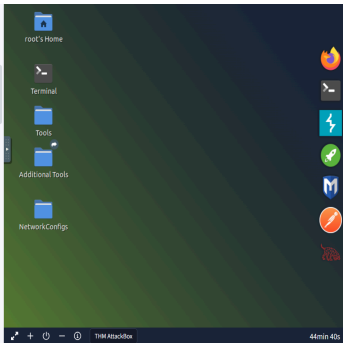
This task offered a classification of various scan types available in Nmap. This task explained the difference between TCP scans, UDP scans, and special types like NULL, FIN, and Xmas scans. It helped us understand which scans are more hidden and how they can avoid firewalls or detection systems.





•Task 5: TCP Connect Scans

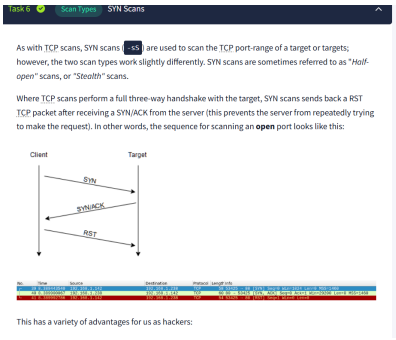


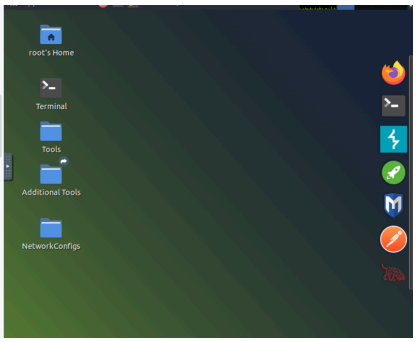


We learned that a TCP Connect scan uses the system's own networking stack to establish a full TCP connection. This scan is easy to spot because it finishes the full three-way handshake. It's mostly used when SYN scans can't be done due to limitations or lack of permission. Even though it's not hidden, it's reliable and helpful in some situations.

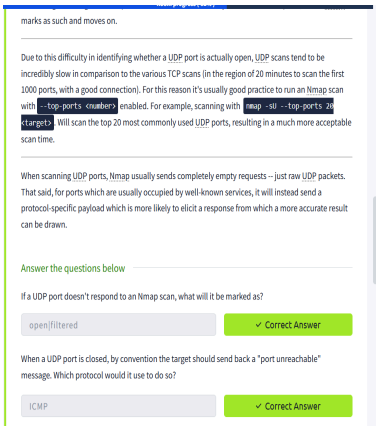
•Task 6: SYN Scans

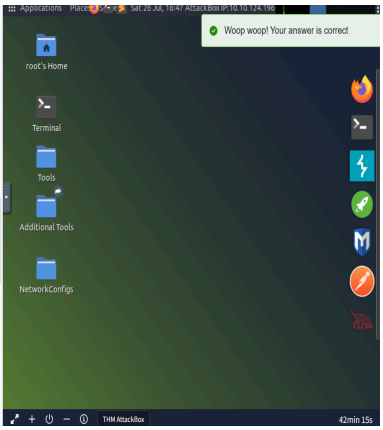
This task was about SYN scans, also known as "half-open scans." They send SYN packets and wait for SYN-ACK replies but don’t finish the connection. This makes the scan quicker and harder to detect than TCP Connect scans, so it's commonly used by penetration testers.. SYN scans require root privileges to operate.





•Task 7: UDP Scans

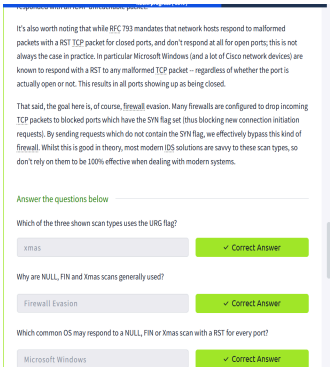


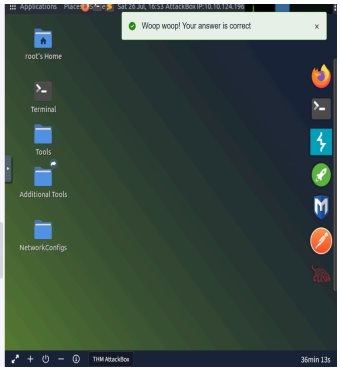


We learned about UDP scans, which help find services running on UDP ports. These scans are slower and less reliable because UDP doesn’t send acknowledgments. Still, Nmap checks for ICMP responses or no replies to find open ports, making it a useful method even with its drawbacks.

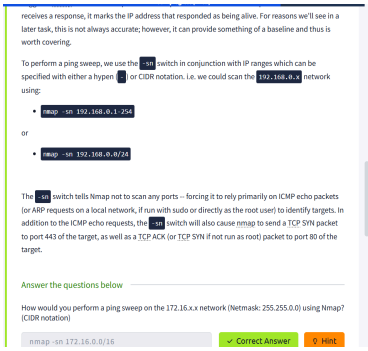
•Task 8: NULL, FIN, and Xmas Scans

In this task, we examined three advanced scan types: NULL, FIN, and Xmas scans. These scans change TCP flags to try and trick firewalls and avoid being detected. For example, NULL scans send packets with no flags, FIN scans send just a FIN flag, and Xmas scans use a mix of FIN, PSH, and URG flags . These are stealth scans often used when firewalls block more traditional scan types.





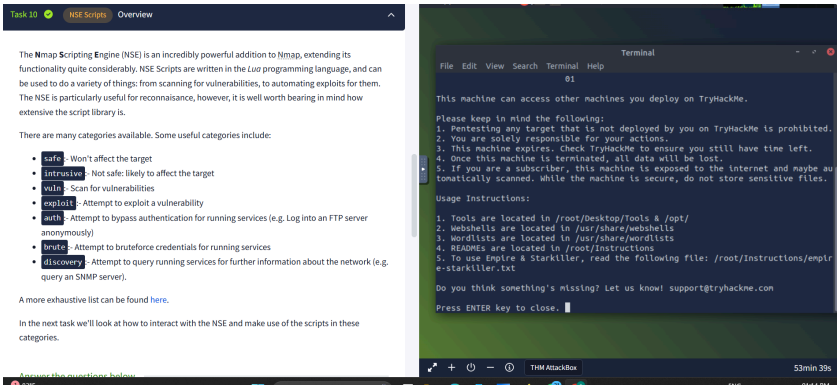
•Task 9: ICMP Network Scanning



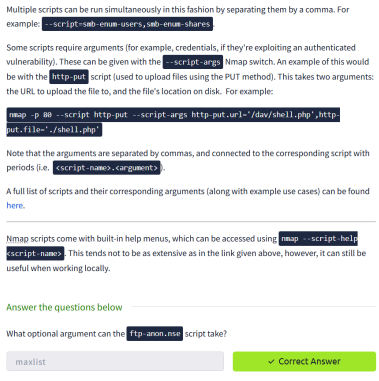
ICMP scanning is used for host discovery, determining which hosts are up without performing port scans. It sends echo requests (ping), timestamp requests, or address mask requests. This task explained how to use ICMP to quickly map live hosts in a network, especially when port scanning isn't possible.

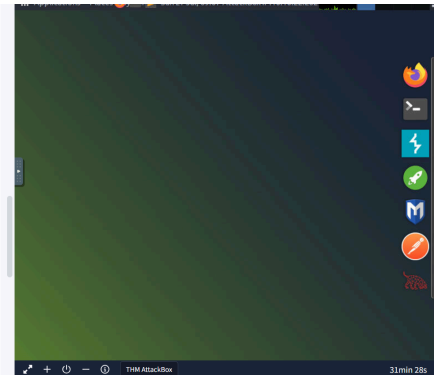
•Task 10: NSE Scripts Overview

In this task, we learned about the Nmap Scripting Engine (NSE), which helps with automating network tasks. NSE scripts are written in Lua and can check software versions, find security issues, and try password guessing. This showed us that Nmap can do more than just simple scanning.



•Task 11: Working with the NSE

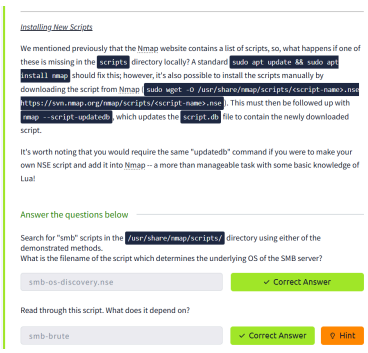


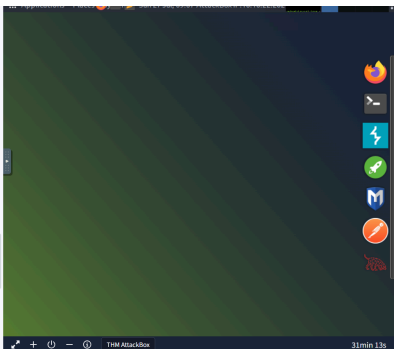


We explored how to use NSE scripts in scans by using the --script option. Examples included running default scripts with -sC, or specifying a category or individual script. We saw how NSE can add detailed information about services, vulnerabilities, and configurations when included in scans.

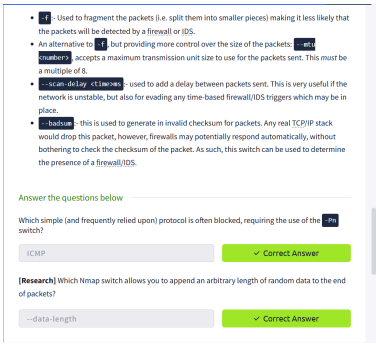
•Task 12: Searching for Scripts

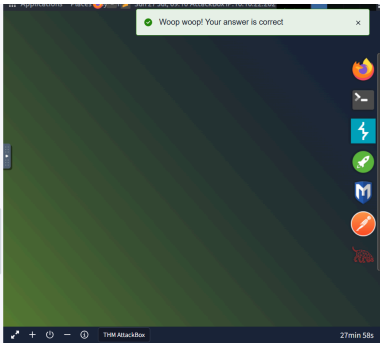
This task taught us how to find NSE scripts that match our needs. By navigating to the Nmap scripts directory or using command-line tools like `locate` or `grep`, we can search for specific keywords or categories. Understanding how to find and use the right script makes our scans more effective.





•Task 13: Firewall Evasion

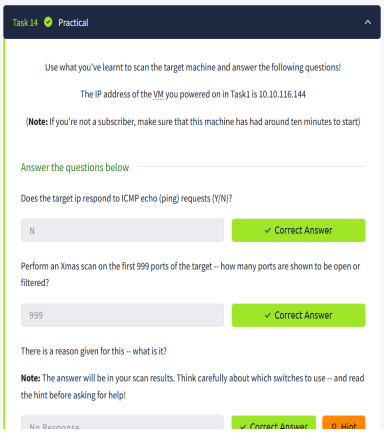


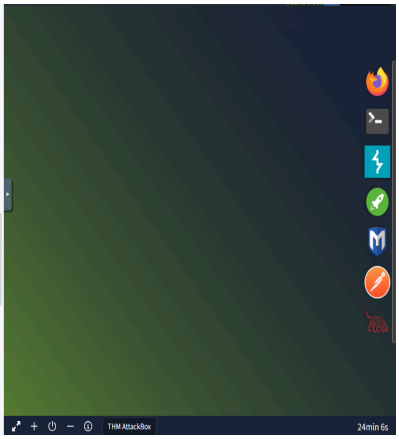


We learned techniques for evading firewalls and IDS during scans. Methods include fragmenting packets (-f), using decoys (--decoy), randomizing scan orders, and changing source ports. These techniques help avoid detection and gain access to more information when networks are actively monitored.

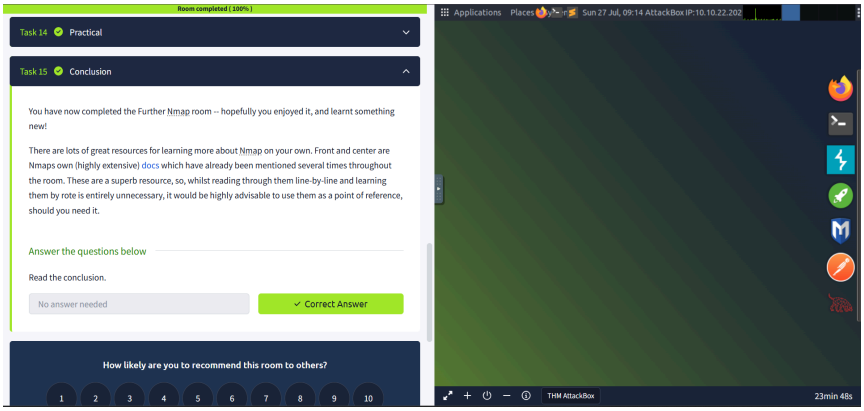
•Task 14: Practical

In the practical task, we applied what we had learned in the previous tasks by conducting various Nmap scans on the deployed target. We used different scan types and options, including NSE scripts, and interpreted the results. This hands-on section reinforced our understanding and helped us gain confidence in using Nmap effectively.





•Task 15: Conclusion



The final task summarized everything covered in the room. It showed how important Nmap is for finding and scanning targets during penetration testing. Learning about different scan types, NSE scripts, and ways to avoid detection is useful for both attacking and defending in cybersecurity.

•Conclusion

The "Further Nmap" room helped me learn advanced Nmap scanning techniques.I now understand how TCP, SYN, and UDP scans work, and I can use different ways to bypass firewalls and security tools. I also learned to use Nmap scripts to find security issues and create my own scripts when needed.These skills make it easier for me to scan networks and check for security issues.