TryHackMe Write-up - Nmap

Room: Nmap

Prepared by: Adhithyan KJ

Date: July 31, 2025

Further Nmap Room

The Further Nmap room helps to learn advanced Nmap scanning techniques. It covers different scan types, switches, output formats, and NSE scripts. This room improves skills in network enumeration and firewall evasion using Nmap.

Task 1 - Deploy

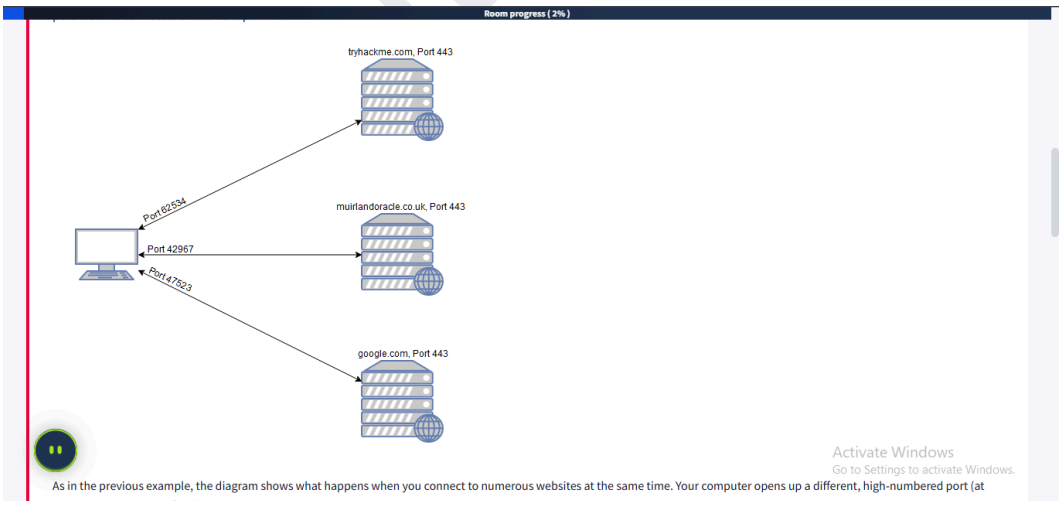
Objective: Deploy the attached VM
Answer: Deployed via TryHackMe - no response needed

Task 2 - Introduction

Nmap is used to scan open ports and identify vulnerabilities.

Task 3 - Nmap Switches

Nmap uses switches to control scan behavior such as -sS, -sU, -A, -T5, etc.



Task 4 - Scan Types Overview

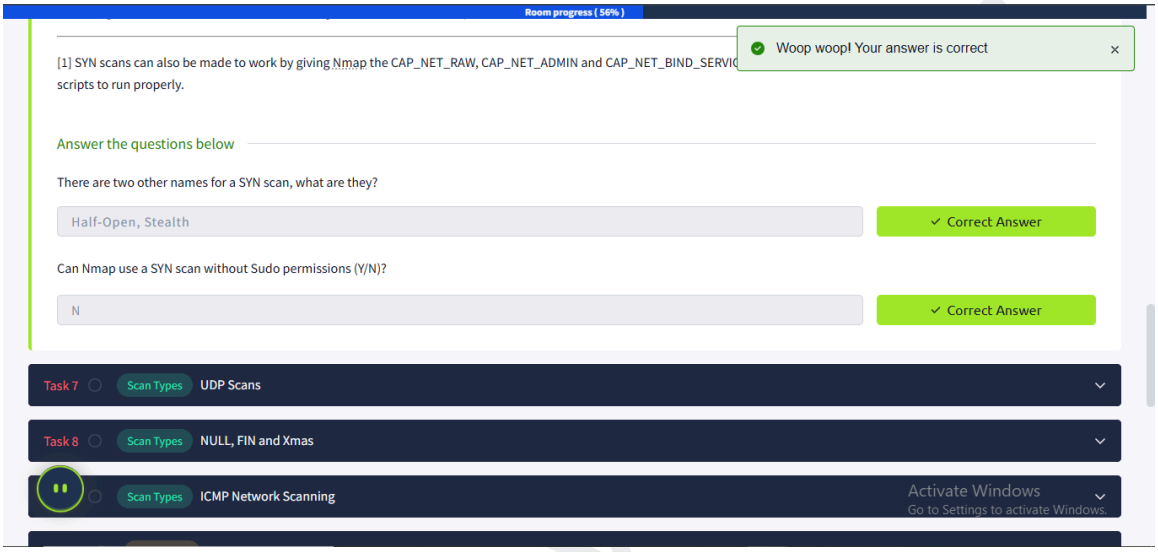
Different scan types like SYN, TCP Connect, UDP, NULL, FIN, XMAS.

Task 5 - TCP Connect Scans

Basic TCP scan behavior following RFC standards.

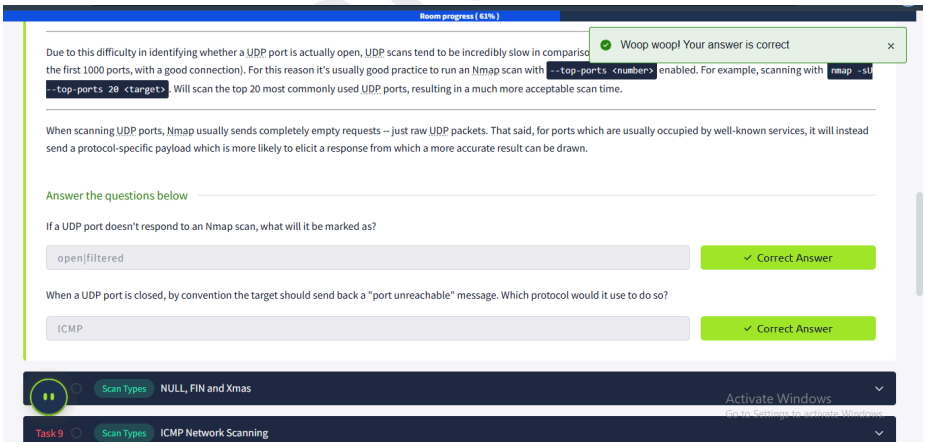
Task 6 - SYN Scans

SYN scans are stealthy and efficient.



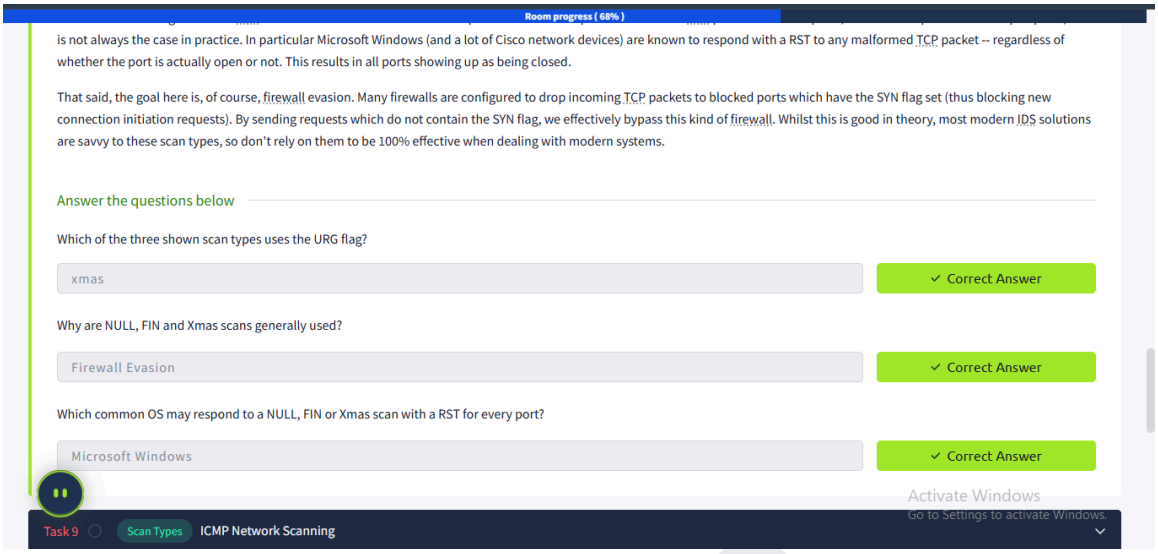
Task 7 - UDP Scans

UDP scanning results and detection methods.



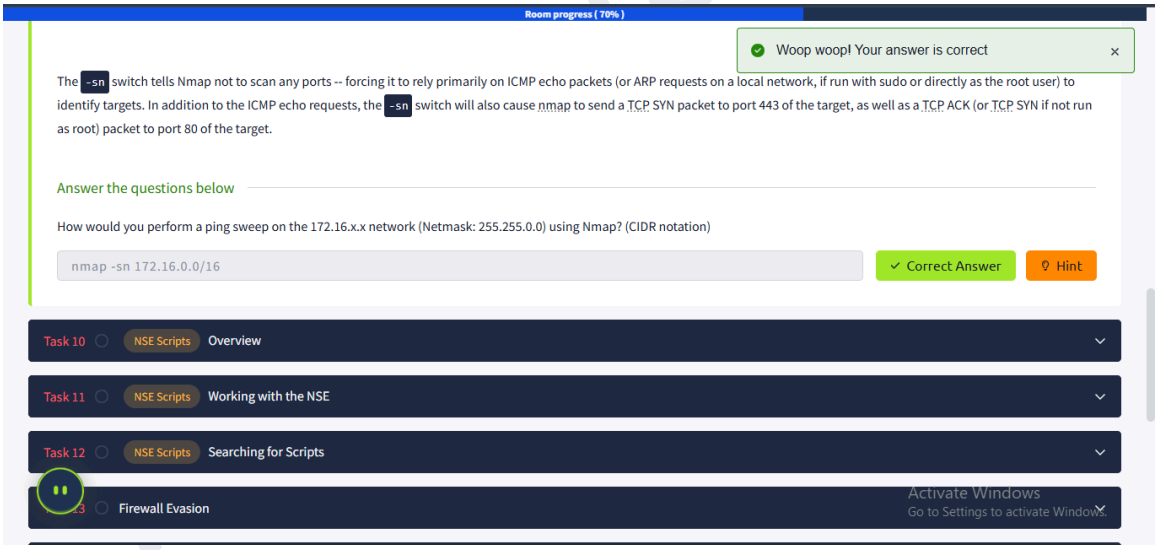
Task 8 - NULL, FIN and Xmas

Scan types used for firewall evasion.



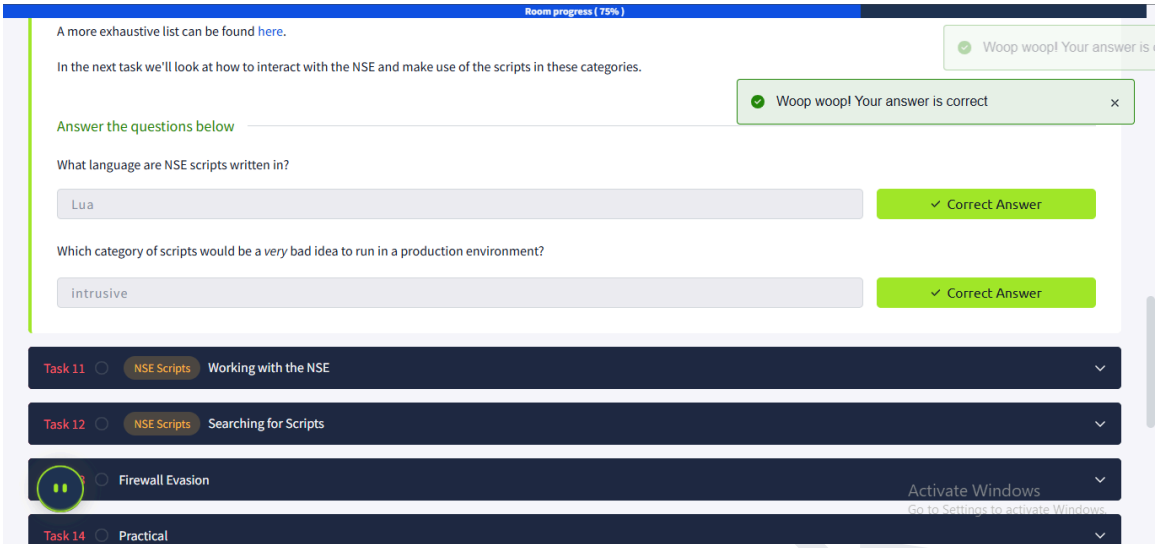
Task 9 - ICMP Network Scanning

How to perform ping sweeps using Nmap.



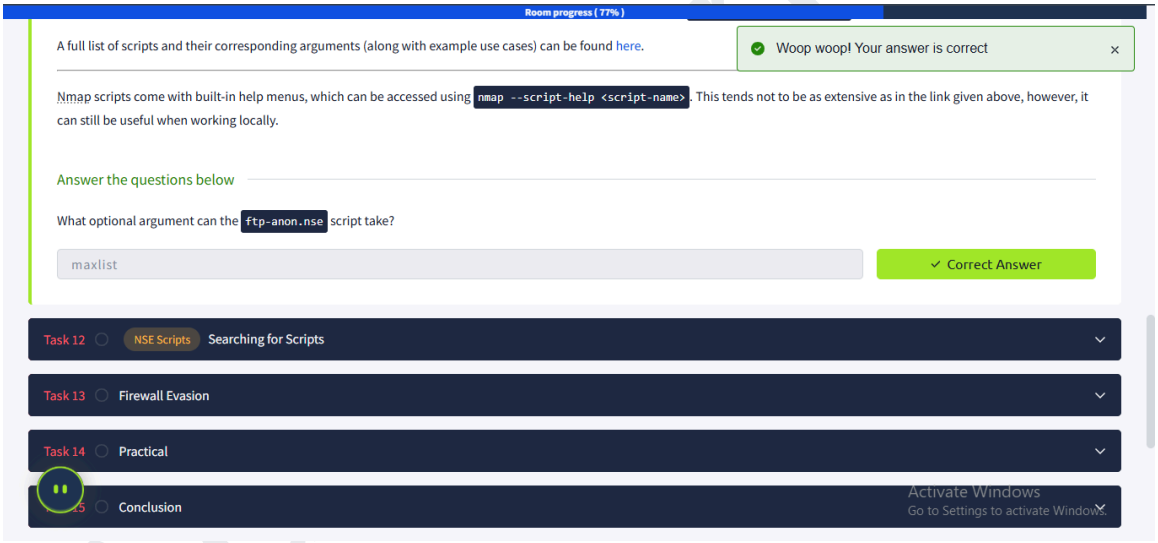
Task 10 - NSE Scripts Overview

Overview of Nmap Scripting Engine.



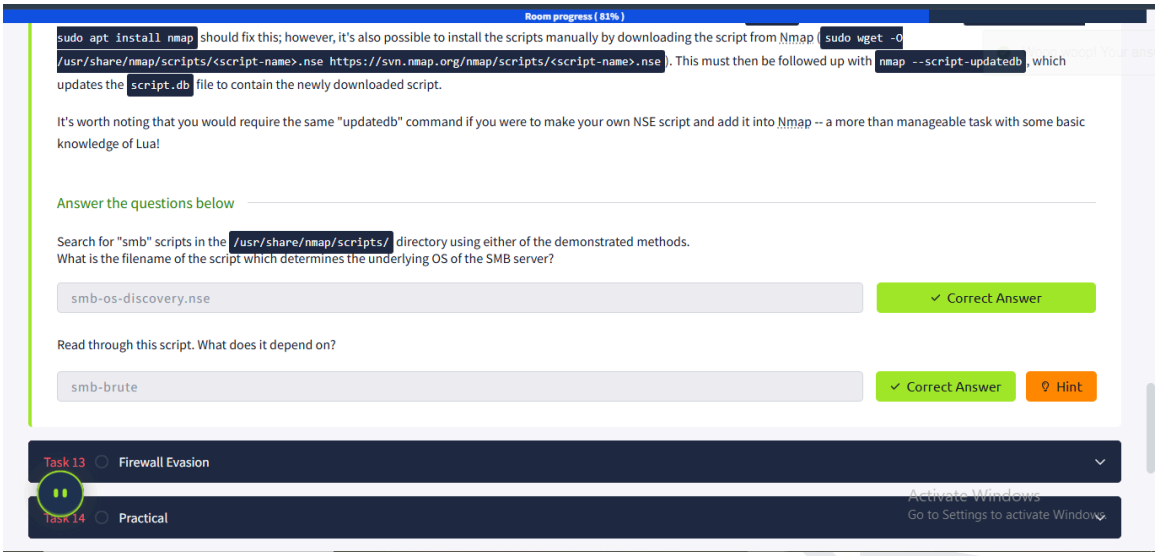
Task 11 - NSE Scripts (working with NSE)

Example with ftp-anon.nse script and optional args.



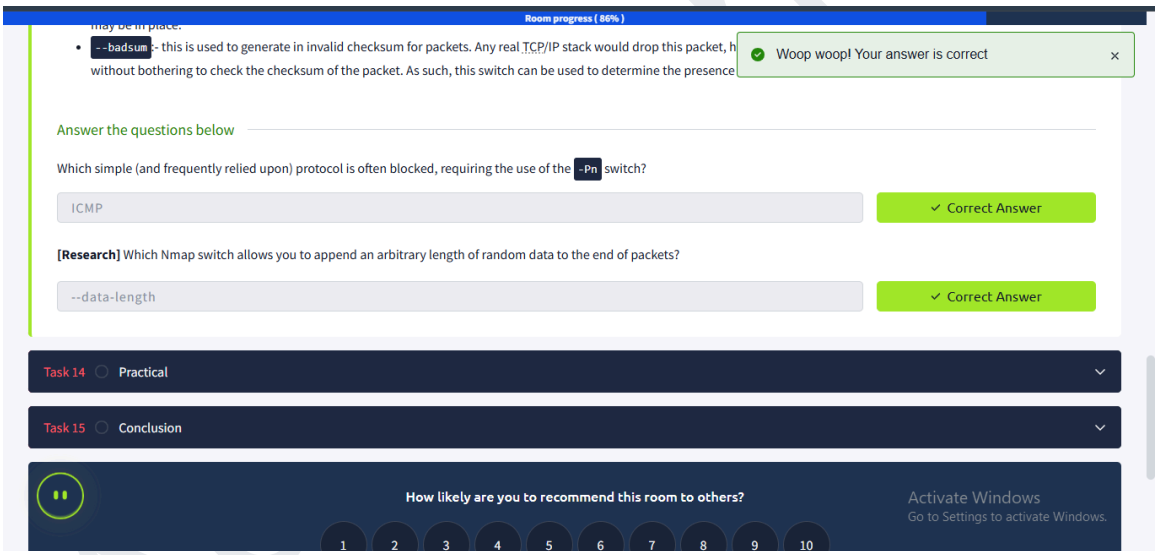
Task 12 - NSE Scripts (searching)

Searching NSE scripts and understanding dependencies.



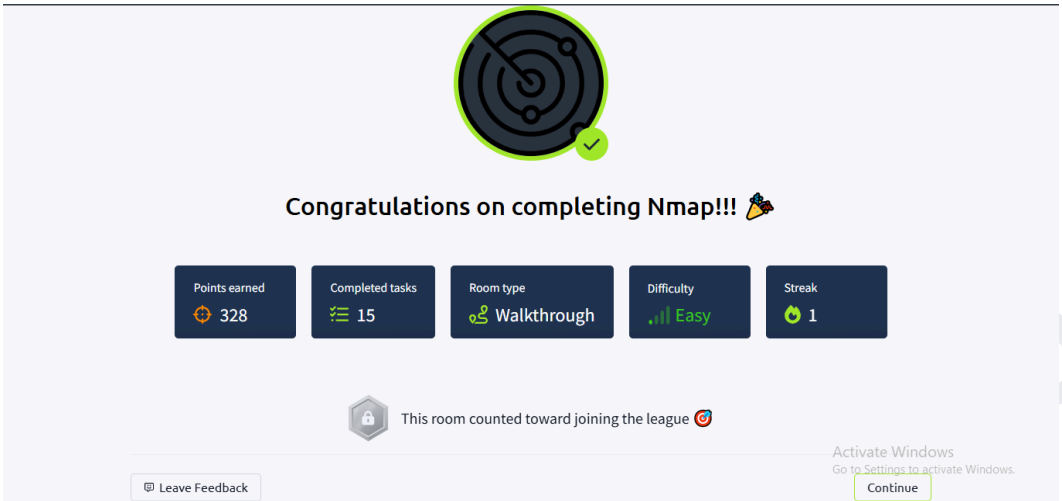
Task 13 - Firewall Evasion

Firewall evasion techniques using various Nmap switches.



Task 14 - Practical

Summary of practical scanning exercises and results.



Task 15 - Conclusion

Practical understanding of scan types and their network impact.

My TryHackMe Profile: https://tryhackme.com/p/adhithyankj

By Adhithyan K J