Task 3: Nmap

Introduction

Nmap (Network Mapper) is a powerful open-source network scanning tool used for network discovery, security auditing, and penetration testing. The *Further Nmap* TryHackMe room explores advanced Nmap functionalities, scan types, NSE (Nmap Scripting Engine), and firewall evasion techniques.

This report documents the step-by-step completion of each task in the room, explaining the concepts, command syntax, and observations. Screenshots are included to validate the results

Objective

The objective of the *Further Nmap* room is to explore advanced features of Nmap, including specific scripts, NSE (Nmap Scripting Engine), timing, firewall evasion, and version detection, while performing scans on the provided target machine.

Summary

The *Further Nmap* room provides a deep dive into advanced scanning techniques and the powerful capabilities of Nmap. After deploying the lab (Task 1) and reviewing the introduction (Task 2), the course builds upon basic knowledge to explore more sophisticated switches and features. Task 3 introduces advanced **Nmap switches**, demonstrating how to customize scans with options like -p for port selection, -A for aggressive scanning, and -O for OS detection. The following tasks (4–9) focus on various **scan types**. Task 4 gives an overview, while Task 5 details **TCP Connect scans**, which complete the TCP handshake but are easier to detect. Task 6 covers **SYN scans**, which send SYN packets without completing the handshake, making them stealthier. Task 7 examines **UDP scans**, which check open UDP ports by sending empty datagrams, though they are slower and often require multiple retries. Task 8 discusses **NULL, FIN, and Xmas scans**, which manipulate TCP flags to bypass basic firewall rules. Task 9 explains **ICMP network scanning** for discovering live hosts without port scanning.

Tasks 10–12 focus on the **Nmap Scripting Engine (NSE)**. Task 10 introduces the concept, explaining that NSE scripts automate enumeration, vulnerability detection, and exploitation. Task 11 demonstrates how to run scripts (--script=<name>), and Task 12 teaches searching for scripts by category or keyword. Task 13 addresses **firewall evasion techniques**, such as fragmenting packets, decoys, and spoofing source IPs to avoid detection. Task 14 provides a **practical exercise** where all learned techniques are applied in a simulated penetration testing scenario, reinforcing hands-on skills. Finally, Task 15 offers the **conclusion**, encouraging further learning through Nmap's documentation and experimentation.

Overall, this room transitions learners from basic Nmap usage to an advanced, penetration-testing-ready skill set. By combining multiple scan types, scripting, and evasion techniques, Nmap becomes a versatile tool for reconnaissance and vulnerability assessment.

Screenshots

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

Answer the questions below

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

open|filtered ✓ Correct Answer

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?

ICMP ✓ Correct Answer

Answer the questions below

Which of the three shown scan types uses the URG flag?

xmas ✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion ✓ Correct Answer

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Microsoft Windows ✓ Correct Answer

Answer the questions below

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

nmap -sn 172.16.0.0/16 ✓ Correct Answer Hint

Answer the questions below

What language are NSE scripts written in?

Lua ✓ Correct Answer

Which category of scripts would be a *very* bad idea to run in a production environment?

intrusive ✓ Correct Answer

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

maxlist ✓ Correct Answer

Answer the questions below

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?

ICMP — ✓ Correct Answer

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

--data-length — ✓ Correct Answer

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