

TryHackMe: Further Nmap - Task 3 Report

By Richu Joseph

Introduction

This report documents the completion of the 'Further Nmap' room on TryHackMe. The objective of this exercise was to deepen understanding of Nmap's capabilities, including advanced scanning techniques, NSE (Nmap Scripting Engine) usage, firewall evasion, and practical applications in network reconnaissance.

Objectives

- Understand advanced Nmap scan types and their purposes.
- Use Nmap Scripting Engine (NSE) for service enumeration.
- Learn firewall/IDS evasion techniques.
- Interpret Nmap scan outputs and results.
- Apply Nmap in real-world penetration testing scenarios.

Task 1: Advanced Scan Types

In this task, we explored various Nmap scan types beyond the standard TCP connect and SYN scans. Examples include Xmas scans, FIN scans, and NULL scans, each designed to bypass certain firewall rules and identify open or filtered ports.

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

Task 2: NSE Script Usage

We used the Nmap Scripting Engine (NSE) to run scripts for service enumeration. For example, the 'ftp-anon.nse' script checks for anonymous FTP login capability. Optional arguments can be provided to specify paths or behaviors.

Nmap scripts come with built-in help menus, which can be accessed using `nmap --script-help <script-name>`. This tends not to be as extensive as in the link given above, however, it can still be useful when working locally.

Answer the questions below

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

maxlist

✓ Correct Answer

Task 3: Firewall Evasion

This task demonstrated techniques to bypass firewalls and intrusion detection systems (IDS), such as fragmenting packets (-f), spoofing source ports, and using decoy IP addresses.

- `--badsum` :- this is used to generate an invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond automatically, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence of a firewall/IDS.

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

Task 4: Practical Scan Exercise

We applied all learned techniques to a target host to identify open ports, running services, and potential vulnerabilities. Multiple scan types were combined for more accurate enumeration.

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 [Cryllic'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

Observations & Analysis

From the scans, we observed differences in detection depending on the scan type and firewall configurations. Some scan types revealed open ports that were hidden from basic scans, and NSE scripts provided valuable additional information about services and potential misconfigurations.

Conclusion & Key Learnings

This exercise reinforced the importance of using a variety of scanning techniques in penetration testing. Nmap's versatility allows testers to adapt to different network defenses and extract more useful information. The NSE scripting capability significantly extends Nmap's functionality, making it a vital tool in any security assessment.

