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

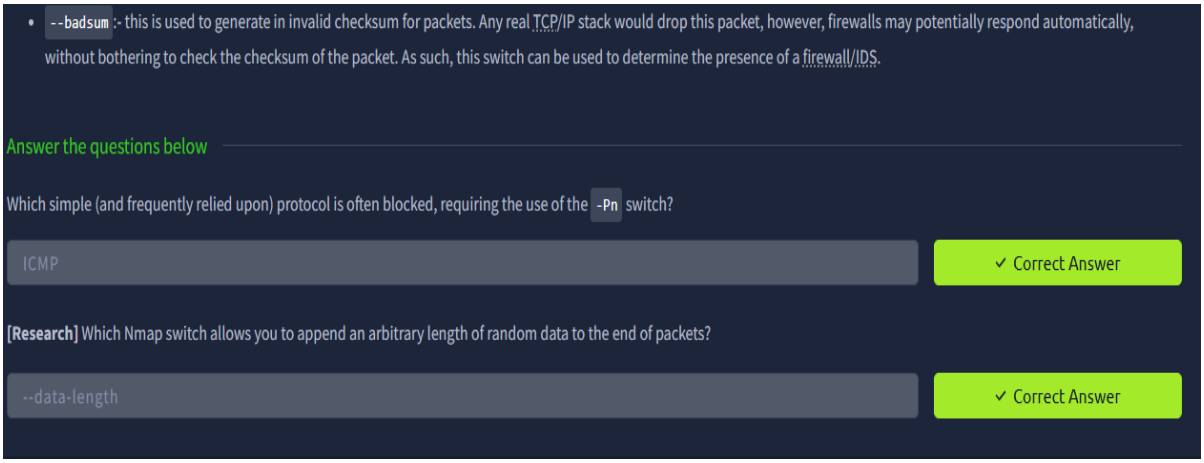
In this task, we explored various Nmap scan types beyond the standard TCP connect and SYN scans. Examples include Xmas scans, FIN scans, and NULL scans, each designed to bypass certain firewall rules and identify open or filtered ports.

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.

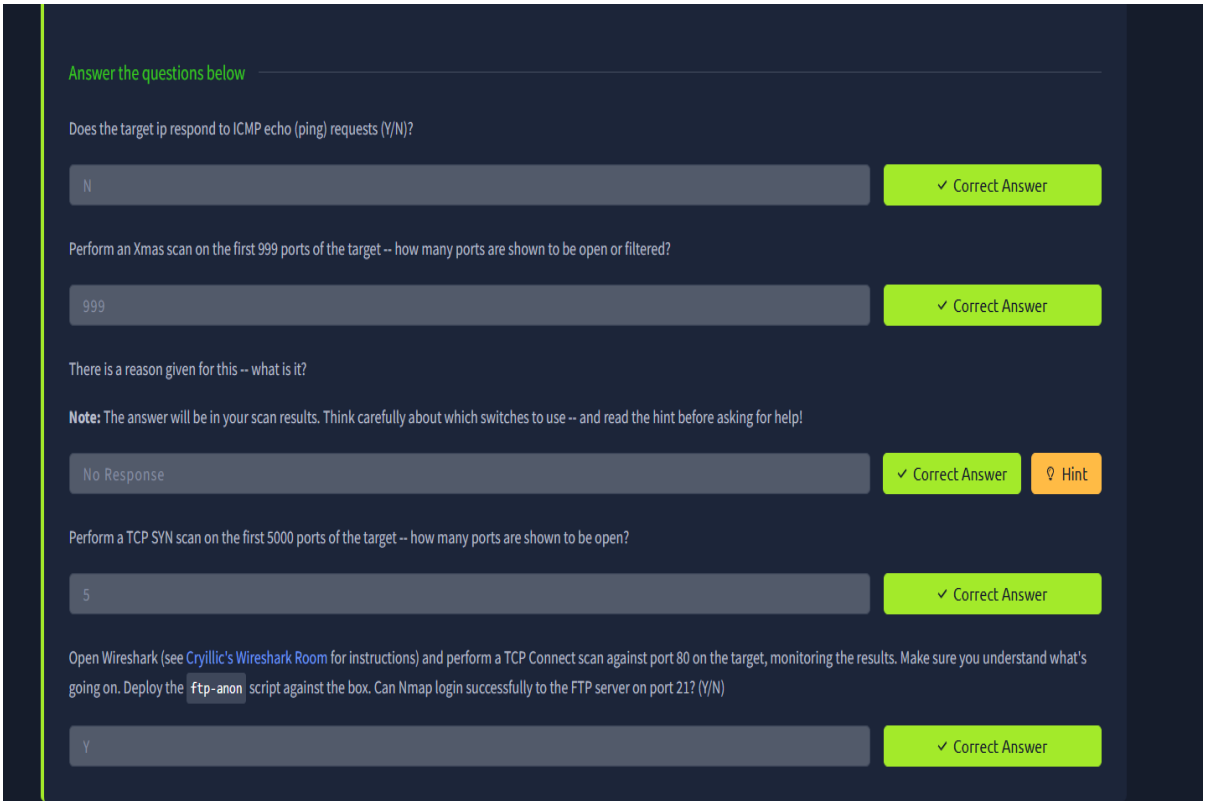
Task 3: Firewall Evasion

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.



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.



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.