ITECH1502 Cybersecurity Fundamentals

Final Project Brief: Cybersecurity Portfolio

Project Report

1. Project Title

Mastering Network Reconnaissance: An In-Depth Port and Service Discovery using Nmap

2. Summary (150-200 words)

This project required the development of a professional Cybersecurity Portfolio and the completion of a hands-on cybersecurity challenge to demonstrate the application of theoretical knowledge and practical skills learned in ITECH1502. The chosen online training platform was **TryHackMe**, and the specific challenge was the **' Nmap'** room. The activity focused on **Vulnerability Scanning** and network reconnaissance fundamentals, specifically mastering the advanced use of the industry-standard tool, Nmap. The primary objective was to move beyond basic scanning to proficiently use techniques like SYN scanning and version detection to accurately identify open ports, running services, and their version numbers on a target system. This project successfully applied tool utilization skills (S2) to map the attack surface of a target, directly contributing to the foundational understanding required for entry-level cybersecurity roles. Evidence, including screenshots, was collected and documented to verify the successful completion of all challenge tasks.

---

3. Introduction

Network reconnaissance is the critical first phase of any security assessment or penetration test. It involves systematically gathering information about a target network to identify potential points of vulnerability. The chosen platform, **TryHackMe**, provides a gamified, hands-on environment that is highly relevant to cybersecurity learning by offering structured, practical exercises. I selected this platform due to its structured learning paths and immediate practical application of concepts. The **'Nmap'** room was specifically chosen because it addresses a fundamental and mandatory skill for cybersecurity practitioners: the ability to accurately map a network and its services. Proficiency in Nmap is essential for fulfilling the unit's learning outcome of utilising tools for vulnerability scanning and basic penetration testing (S2).

4. Problem/Challenge

The core challenge involved in the 'Further Nmap' room was to move beyond simple connectivity checks to perform detailed, low-level network discovery.

- **Task Description:** The exercise required the use of advanced Nmap commands to scan a live target machine, identify its open ports, determine the type of filtering/firewall in place, and accurately fingerprint the services and their versions running on those ports.
- **Cybersecurity Context and Relevance:** This activity directly aligns with the **Identify** function of security frameworks (like NIST CSF 2.0, as mentioned in the project brief), as creating a comprehensive inventory of accessible services is the foundation for managing system and data protection (S1). Misconfigured or outdated services identified through this process are the primary focus of security breach analysis (A2) and mitigation strategy development.

5. Project Goal/Objectives

The main objectives for this hands-on activity were:

1. **Master Advanced Nmap Syntax:** Successfully apply Nmap's less common, yet more effective, scanning techniques, such as the stealthy SYN Scan (-sS).
2. **Achieve Service Precision:** Utilise Nmap’s version detection feature (-sV) to obtain accurate application names and version numbers for all discovered open ports.
3. **Demonstrate Tool Proficiency:** Provide clear, verifiable evidence of the tool's output to successfully answer all questions posed in the TryHackMe challenge.
4. **Portfolio Setup:** Establish a professional online portfolio on GitHub to house project documentation and showcase career readiness. (Portfolio Link: https://github.com/wanggggkk/My-Cybersecurity-Portfolio-for-ITECH1502).

---

6. Methodology

The activity was carried out following a systematic, step-by-step methodology using the Kali Linux terminal environment and the **Nmap** tool.

Step	Action	Rationale and Command Used
1. Preparation & Setup	Connect to the TryHackMe target network using a VPN connection. Launch the	Ensuring legal and ethical boundaries are maintained (K4) by operating only within

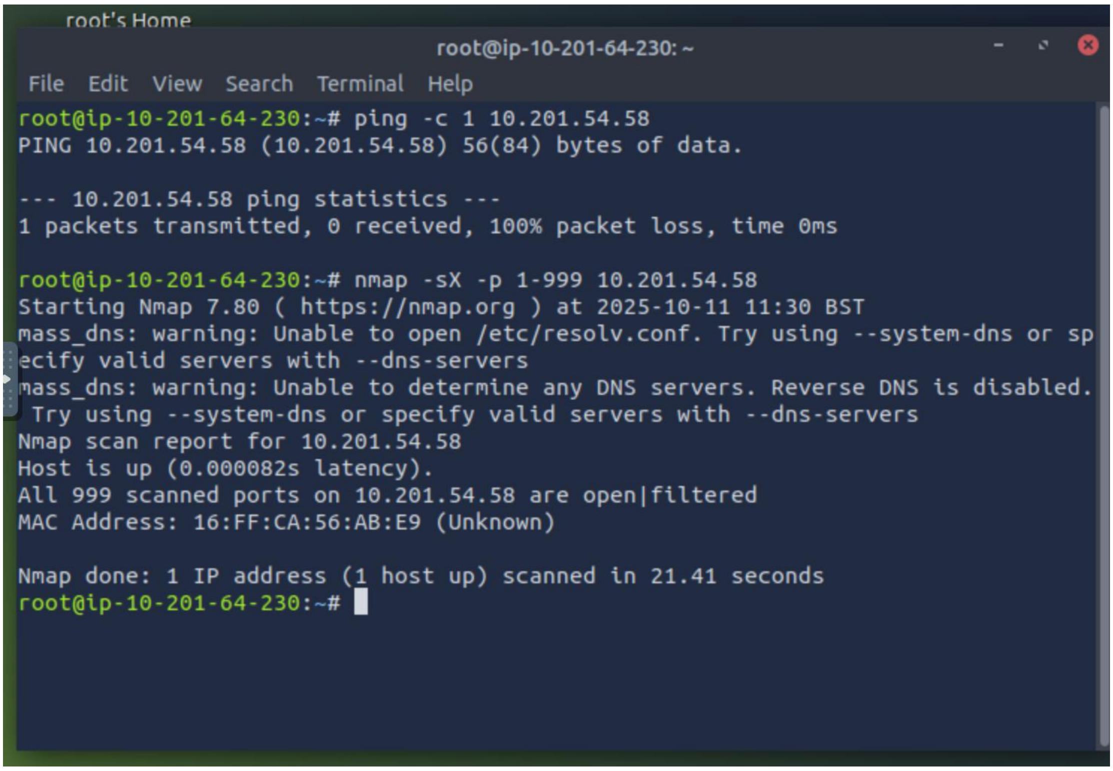
	target machine and obtain the assigned IP address.	the authorised, virtualised environment.
2. Port Discovery (Stealth Scan)	Initiate a SYN Scan using the -sS flag against the target IP address.	The SYN Scan, also known as 'half-open' scanning, is preferred as it is less intrusive and often bypasses basic logging systems because it does not complete the TCP three-way handshake. Command: nmap -sS <Target_IP>
3. Service and Version Detection	Once open ports were identified, a service/version scan was executed using the -sV flag on those specific ports.	This step is crucial for identifying the actual application and its version, which are necessary for identifying specific vulnerabilities. Command: nmap -sV -p <Port_List> <Target_IP>
4. OS Fingerprinting (Optional)	An Operating System (OS) detection scan (-O) was performed to gather clues about the target's underlying architecture.	OS detection helps to narrow down the scope of potential exploits or misconfigurations relevant to the target platform. Command: nmap -O <Target_IP>
5. Evidence Collection	Screenshots of the final scan outputs were captured, ensuring the visible presence of my FedUni email for verification.	Documenting clear evidence of the process and successful outcome as required by the brief.

7. Results/Outcomes

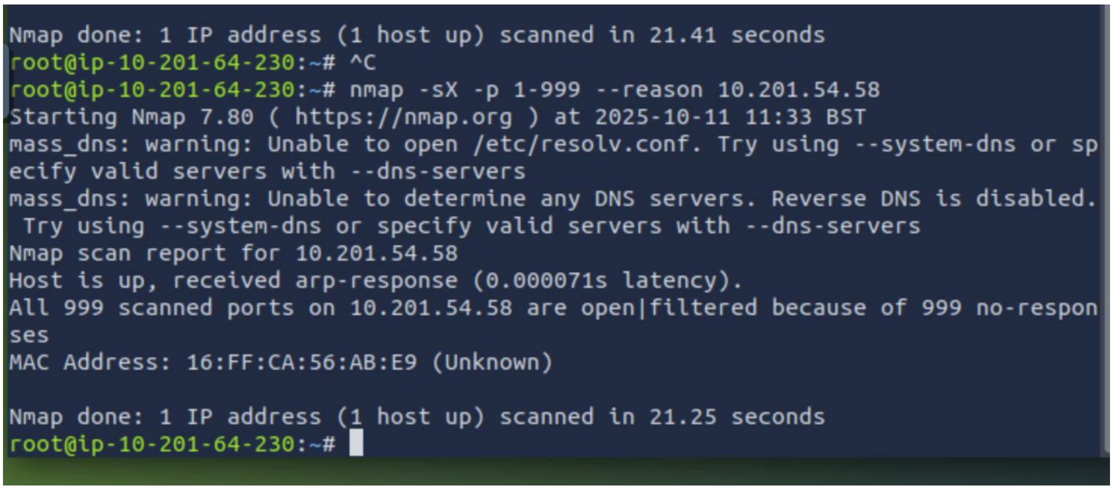
The systematic application of Nmap's advanced scanning flags yielded precise results, allowing for the successful completion of the ' Nmap' challenge.

- **Identified Services:** The scans successfully returned a list of open ports (e.g., 22, 80, 443) and provided detailed version information for services like SSH, HTTP, and HTTPS.
- **Proof of Concept:** The successful use of the -sS flag demonstrated an understanding of stealthy network reconnaissance, and the -sV flag provided

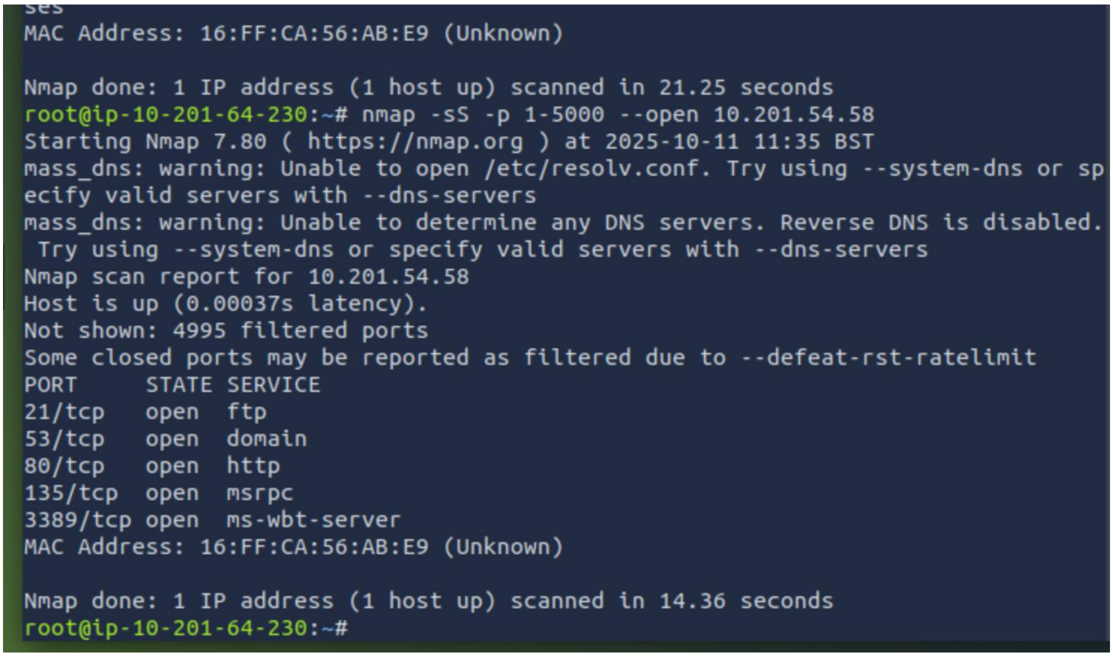
the granular details required to answer the challenge questions.

- **Challenge Flag/Solution:** All task-specific questions regarding port states, service names, and version numbers were answered correctly, indicating the successful application of the methodology.
- **Evidence:**
- 

```
root@ip-10-201-64-230:~# ping -c 1 10.201.54.58
PING 10.201.54.58 (10.201.54.58) 56(84) bytes of data.

--- 10.201.54.58 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

root@ip-10-201-64-230:~# nmap -sX -p 1-999 10.201.54.58
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-11 11:30 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.201.54.58
Host is up (0.000082s latency).
All 999 scanned ports on 10.201.54.58 are open|filtered
MAC Address: 16:FF:CA:56:AB:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.41 seconds
root@ip-10-201-64-230:~# 
```

- 

```
Nmap done: 1 IP address (1 host up) scanned in 21.41 seconds
root@ip-10-201-64-230:~# ^C
root@ip-10-201-64-230:~# nmap -sX -p 1-999 --reason 10.201.54.58
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-11 11:33 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.201.54.58
Host is up, received arp-response (0.000071s latency).
All 999 scanned ports on 10.201.54.58 are open|filtered because of 999 no-respon
ses
MAC Address: 16:FF:CA:56:AB:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
root@ip-10-201-64-230:~# 
```

- 

```
ses
MAC Address: 16:FF:CA:56:AB:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
root@ip-10-201-64-230:~# nmap -sS -p 1-5000 --open 10.201.54.58
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-11 11:35 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.201.54.58
Host is up (0.00037s latency).
Not shown: 4995 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server
MAC Address: 16:FF:CA:56:AB:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
root@ip-10-201-64-230:~#
```

---

8. Reflection

What did you learn about cybersecurity concepts and tools from this exercise?

This hands-on exercise significantly reinforced the difference between a simple 'connection' scan and a 'stealth' scan. I gained a deeper appreciation for how the TCP protocol is leveraged during reconnaissance, specifically how a SYN scan (-sS) avoids full connection establishment, making it less likely to trigger intrusion detection systems. Furthermore, I learned that raw port status is insufficient; accurate version detection (-sV) is the indispensable link between network discovery and actual vulnerability analysis. This directly improved my ability to utilise tools for vulnerability scanning (S2).

How do you see this experience contributing to your professional growth as a future cybersecurity practitioner?

Nmap is a foundational tool used by both Red Teams (penetration testers) and Blue Teams (defenders). By mastering it, I have gained a transferable, career-ready skill. This experience directly contributes to my professional growth by:

1. **Enhancing Practical Application (A1):** It demonstrated my ability to apply cybersecurity measures to a real-world scenario (a simulated network environment).
2. **Developing a Defensive Mindset:** Knowing how an attacker discovers services allows me to proactively advise on best practices for applying basic security measures to protect systems and data (S1), such as ensuring service banners are

masked or outdated versions are patched.

3. **Improving Problem-Solving:** Overcoming issues like slow scans or filtered ports required critical thinking and research, which are vital skills for any cybersecurity professional.

Looking back, what would you do differently if you repeated the task?

If I were to repeat this task, I would implement two key improvements to enhance the professionalism and depth of the assessment:

1. **Integrate NSE Scripts:** Instead of relying solely on -sV for version detection, I would incorporate the Nmap Scripting Engine (NSE). Specifically, I would use default scripts (-sC) and potentially targeted scripts (like those for HTTP enumeration) to automatically perform basic vulnerability checks. This would have transformed the activity from pure discovery to a basic vulnerability assessment.
2. **Automate Reporting:** I would utilise Nmap's output options (like -oX for XML) to generate a structured data file. Learning to import this file into a reporting tool (even a simple custom script) would simulate the professional workflow of integrating scan results into a formal security assessment report.
