TryHackMe Report: Further Nmap Room

R S Abhinav

August 9, 2025

Profile Verification

As per the submission requirements, my TryHackMe profile link is provided as proof of task completion: `https://tryhackme.com/p/rsabhinav666`

Room Overview

The "Further Nmap" room focuses on advanced usage of the `nmap` network scanning tool. It covers output formats, host discovery, port scanning techniques, OS and version detection, firewall evasion, timing control, and scripting.

This report documents each task with an explanation, the corresponding command(s), and the answer.

Task 1: Introduction

This task introduces the objectives: learning about Nmap switches, scan types, performance tuning, and evasion. **Answer:** No written response required.

Task 2: Nmap Switches

Q: Save results in three major formats

Command:

```
nmap -oA scan_results target-ip
```

Explanation: The `-oA` option saves output in Normal (`-oN`), XML (`-oX`), and Grepable (`-oG`) formats simultaneously. **Answer:** `-oA`

Q: Save results in normal format only

```
nmap -oN normal_results.txt target-ip
```

Explanation: `-oN` outputs human-readable results to a file. **Answer:** `-oN`

Task 3: Target Specification

Command:

```
nmap 10.10.X.X
```

Explanation: By default, specifying an IP address runs a basic scan on the top 1000 ports.

Task 4: Host Discovery

Command:

```
nmap -sn 10.10.X.X
```

Explanation: The `-sn` flag performs a "ping scan" to check if the host is up without port scanning.

Task 5: Port Scanning Techniques

Q: Default scan as root

Answer: SYN scan (`-sS`) **Explanation:** A SYN scan is stealthier and faster, sending SYN packets without completing the TCP handshake.

Task 6: Service and Version Detection

Command:

```
nmap -sV target-ip
```

Explanation: `-sV` probes open ports to determine running service versions.

Task 7: OS Detection

Command:

```
nmap -O target-ip
```

Explanation: The `-O` option attempts to guess the operating system using TCP/IP stack fingerprinting.

Task 8: Script Scanning

Default scripts:

```
nmap -sC target-ip
```

Specific script:

```
nmap --script=vuln target-ip
```

Explanation: `-sC` runs Nmap's default NSE scripts. `--script` allows targeted script execution.

Task 9: Timing and Performance

Most aggressive: `-T5` — fastest, least stealthy. **Slowest:** `-T0` — very slow, used for maximum stealth.

Task 10: Firewall Evasion

Command:

```
nmap --decoy IP1,IP2,ME target-ip
```

Explanation: `--decoy` sends traffic appearing to come from multiple IPs to confuse defenders.

Task 11: Output Formats

Answer: `-oX` — saves scan in XML format for automation or parsing.

Task 12: Scan Types Review

Two other names for SYN scan: Half-open, Stealth **Root requirement:** Yes — needs raw socket access.

Task 13: Verbosity

Command:

```
nmap -vv target-ip
```

Explanation: Increases output detail. Multiple `v`'s = more verbose.

Task 14: Scanning Specific Ports

Example:

```
nmap -p 80,443,22 target-ip
```

Explanation: `-p` lets you specify one, multiple, or a range of ports.

Task 15: Final Thoughts

This task was simply marking the room as complete.

Conclusion

The “Further Nmap” room expanded my skills beyond basic scanning. I learned about:

- Advanced output formats and reporting.
- Host discovery without port scans.
- Different port scan techniques and their trade-offs.
- Using scripts to automate information gathering.
- Timing templates to balance speed and stealth.
- Firewall evasion using decoys and fragmentation.

These skills are directly applicable to penetration testing and network reconnaissance in real-world scenarios.