TryHackMe Nmap Room Completion Report

Prepared by: vaishnav k

Git : vaishnav4281

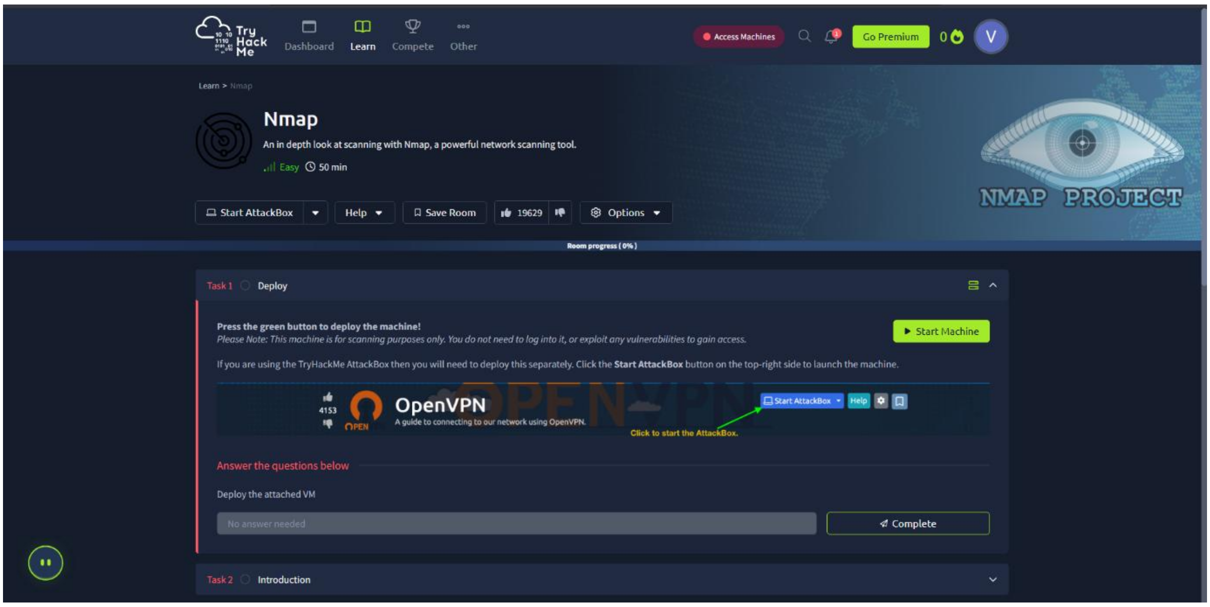
Date: August 7, 2025

---

1. Introduction

This report documents the successful completion of the "Nmap" room on the TryHackMe cybersecurity training platform. This module provides an in-depth, hands-on look at network scanning using Nmap, the industry-standard tool for network exploration and security auditing. The training covered fundamental concepts of port scanning, various scan types, the Nmap Scripting Engine (NSE), and techniques for firewall evasion.

Figure 1: The "Nmap" Room on the TryHackMe Platform.



Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

Easy 50 min

Task 1 Deploy

Press the green button to deploy the machine!
Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.

If you are using the TryHackMe AttackBox then you will need to deploy this separately. Click the **Start AttackBox** button on the top-right side to launch the machine.

A guide to connecting to our network using OpenVPN.

Click to start the AttackBox.

Answer the questions below

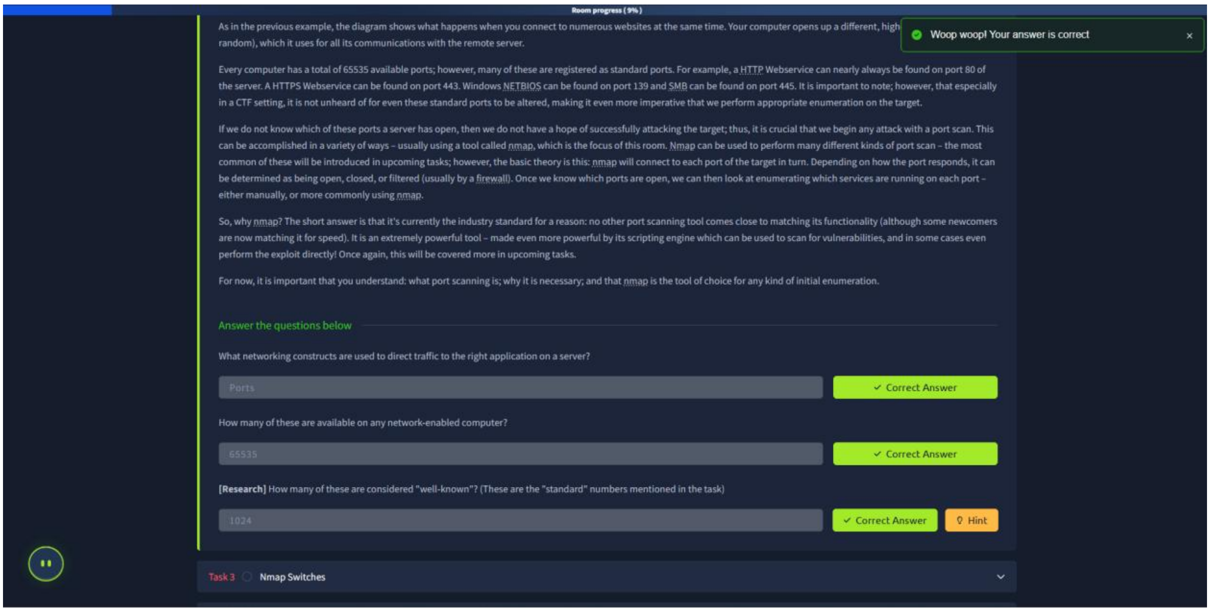
Deploy the attached VM

No answer needed

---

2. Proof of Completion

The following image serves as official confirmation that all 15 tasks within the Nmap room were successfully completed. The completion screen displays the total points earned and the number of tasks finished.



Room progress (9%)

As in the previous example, the diagram shows what happens when you connect to numerous websites at the same time. Your computer opens up a different, high random), which it uses for all its communications with the remote server.

Woop woop! Your answer is correct

Every computer has a total of 65535 available ports; however, many of these are registered as standard ports. For example, a HTTP Webservice can nearly always be found on port 80 of the server. A HTTPS Webservice can be found on port 443. Windows NETBIOS can be found on port 139 and SMB can be found on port 445. It is important to note; however, that especially in a CTF setting, it is not unheard of for even these standard ports to be altered, making it even more imperative that we perform appropriate enumeration on the target.

If we do not know which of these ports a server has open, then we do not have a hope of successfully attacking the target; thus, it is crucial that we begin any attack with a port scan. This can be accomplished in a variety of ways – usually using a tool called nmap, which is the focus of this room. Nmap can be used to perform many different kinds of port scan – the most common of these will be introduced in upcoming tasks; however, the basic theory is this: nmap will connect to each port of the target in turn. Depending on how the port responds, it can be determined as being open, closed, or filtered (usually by a firewall). Once we know which ports are open, we can then look at enumerating which services are running on each port – either manually, or more commonly using nmap.

So, why nmap? The short answer is that it's currently the industry standard for a reason: no other port scanning tool comes close to matching its functionality (although some newcomers are now matching it for speed). It is an extremely powerful tool – made even more powerful by its scripting engine which can be used to scan for vulnerabilities, and in some cases even perform the exploit directly! Once again, this will be covered more in upcoming tasks.

For now, it is important that you understand: what port scanning is; why it is necessary; and that nmap is the tool of choice for any kind of initial enumeration.

Answer the questions below

What networking constructs are used to direct traffic to the right application on a server?

Ports

✓ Correct Answer

How many of these are available on any network-enabled computer?

65535

✓ Correct Answer

[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024

✓ Correct Answer

Hint

Task 3 Nmap Switches

Figure 2: Official Completion Certificate for the Nmap Room.

Summary of Achievement:

- **Tasks Completed:** 15
- **Points Earned:** 328

---

3. Detailed Task Log

This section provides a summary of each task, including the core learning objectives, questions posed, and the correct answers submitted.

Task 1: Deploy

- **Objective:** To deploy the target virtual machine required for the hands-on exercises in the room.
- **Answer:** No answer was required for this task.

Task 2: Introduction

- **Objective:** This task introduced the core concepts of networking ports, the necessity of port scanning, and the role of Nmap in network enumeration. It explained that computers have 65,535 ports and that services listen on these ports to accept connections.
- **Questions & Answers:**
    - **What networking constructs are used to direct traffic to the right application on a server?**

        - **Answer:** Ports
    - **How many of these are available on any network-enabled computer?**
        - **Answer:** 65535
    - **[Research] How many of these are considered “well-known”?**
        - **Answer:** 1024

Figure 3: Correctly Answered Questions for Task 2.

Task 3: Nmap Switches

- **Objective:** To learn the fundamental command-line switches that control Nmap's scanning behavior, output, timing, and other functions.
- **Questions & Answers:**
    - **First switch for a ‘Syn Scan’:** -sS
    - **Switch for a “UDP scan”:** -sU
    - **Switch to detect the OS:** -O
    - **Switch to detect service versions:** -sV
    - **Switch to increase verbosity:** -v
    - **Switch for verbosity level two:** -vv
    - **Switch to save results in three major formats:** -oA
    - **Switch to save results in “normal” format:** -oN
    - **Switch to save results in a “grepable” format:** -oG
    - **Switch to activate “aggressive” mode:** -A
    - **Switch to set the timing template to level 5:** -T5
    - **Switch to scan only port 80:** -p 80
    - **Switch to scan ports 1000–1500:** -p 1000-1500
    - **Switch to scan all ports:** -p-
    - **Switch to activate a script from the NSE:** --script
    - **Switch to activate all scripts in the “vuln” category:** --script=vuln

Task 4: Scan Types Overview

- **Objective:** To provide a high-level overview of the different scan types available in Nmap, including TCP, SYN, UDP, and more stealthy methods.
- **Answer:** No answer was required for this task.

Task 5: Scan Types TCP Connect Scans

- **Objective:** To understand the mechanism of a TCP Connect Scan (-sT), which completes a full TCP three-way handshake to determine if a port is open, closed, or filtered.
- **Questions & Answers:**
  - **Which RFC defines the appropriate behaviour for the TCP protocol?**
    - **Answer:** RFC 793
  - **If a port is closed, which flag should the server send back to indicate this?**
    - **Answer:** RST

Task 6: Scan Types SYN Scans

- **Objective:** To learn about SYN "Stealth" Scans (-sS), a default scan type (with sufficient privileges) that is faster and less conspicuous because it does not complete the three-way handshake.
- **Questions & Answers:**
  - **Two other names for a SYN scan:** Half-Open, Stealth
  - **Can Nmap use a SYN scan without Sudo permissions (Y/N)?**
    - **Answer:** N

Task 7: Scan Types UDP Scans

- **Objective:** To understand the methods and challenges of UDP scans (-sU), which are inherently slower and less reliable due to the connectionless nature of the UDP protocol.
- **Questions & Answers:**
  - **If a UDP port doesn’t respond to an Nmap scan, what will it be marked as?**
    - **Answer:** open|filtered
  - **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?**

        - **Answer:** ICMP

Task 8: Scan Types NULL, FIN, and Xmas

- **Objective:** To learn about stealthy scan types (-sN, -sF, -sX) that send malformed TCP packets to bypass stateless firewalls.
- **Questions & Answers:**
    - **Which of the three shown scan types uses the URG flag?**
        - **Answer:** xmas
    - **Why are NULL, FIN and Xmas scans generally used?**
        - **Answer:** Firewall Evasion
    - **Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?**
        - **Answer:** Microsoft Windows

Task 9: ICMP Network Scanning

- **Objective:** To learn how to perform a "ping sweep" (-sn) to discover which hosts on a network are active without conducting a full port scan.
- **Questions & Answers:**
    - **How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)**
        - **Answer:** nmap -sn 172.16.0.0/16

Task 10: NSE Scripts Overview

- **Objective:** To introduce the Nmap Scripting Engine (NSE), a powerful feature that allows users to automate a wide variety of networking tasks using Lua scripts.
- **Questions & Answers:**
    - **What language are NSE scripts written in?**
        - **Answer:** LUA
    - **Which category of scripts would be a very bad idea to run in a production environment?**
        - **Answer:** Intrusive

Task 11: NSE Scripts Working with the NSE

- **Objective:** To learn the practical application of NSE scripts, including how to pass arguments to them.
- **Questions & Answers:**
  - **What optional argument can the ftp-anon.nse script take?**
    - **Answer:** maxlist

Task 12: NSE Scripts Searching for Scripts

- **Objective:** To learn methods for finding available NSE scripts on a local machine.
- **Questions & Answers:**
  - **What is the filename of the script which determines the underlying OS of the SMB server?**
    - **Answer:** smb-os-discovery.nse
  - **Read through this script. What does it depend on?**
    - **Answer:** smb-brute

Task 13: Firewall Evasion

- **Objective:** To explore advanced techniques for bypassing firewalls, such as using -Pn to skip the host discovery phase when ICMP is blocked.
- **Questions & Answers:**
  - **Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?**
    - **Answer:** ICMP
  - **[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?**
    - **Answer:** --data-length

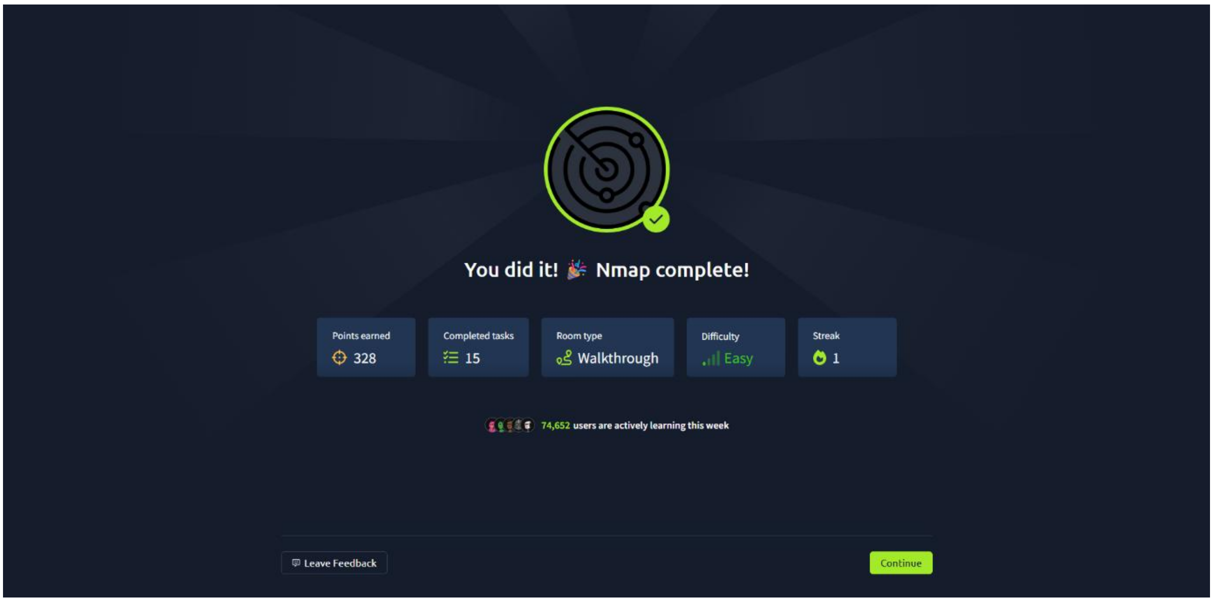
Task 14: Practical

- **Objective:** A final hands-on lab to apply the Nmap techniques learned throughout the room against the target machine.
- **Questions & Answers:**
  - **Does the target (MACHINE_IP)respond to ICMP (ping) requests (Y/N)?**
    - **Answer:** N

    - **Perform an Xmas scan on the first 999 ports of the target — how many ports are shown to be open or filtered?**
        - **Answer:** 999
    - **Perform a TCP SYN scan on the first 5000 ports of the target — how many ports are shown to be open?**
        - **Answer:** 5
    - **Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)**
        - **Answer:** Y

Task 15: Conclusion

- **Objective:** To formally conclude the training room and highlight resources for continued learning.
- **Answer:** No answer was required for this task.



You did it! 🎉 Nmap complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
328	15	Walkthrough	Easy	1

74,652 users are actively learning this week