TASK – 3

TryHackMe Write-up

Room: Further Nmap Prepared

by: Dennis Jacob

Further Nmap page

The Further Nmap room helps to learn advanced Nmap scanning techniques. It covers different scan types, switches, output formats, and NSE scripts. This room improves skills in network enumeration and firewall evasion using Nmap.

Task 1 - Deploy

Objective: Deploy the attached VM

Answer: Deployed via TryHackMe - no response needed

Task 2 - Introduction

Before hacking, it's important to gather info about the target by scanning its ports. Ports let a machine run multiple services, like web servers on ports 80 and 443. Nmap is the main tool used to scan these ports, find open services, and identify vulnerabilities. Proper port scanning is the first step in any security assessment.

1. What networking constructs are used to direct trac to the right application on a server?
   - ports
2. How many of these are available on any network-enabled computer?
   - 65535
3. [Research] How many of these are considered "well-known"?

   (These are the "standard" numbers mentioned in the task)

   - 1024

Task 3 - Nmap Switches

Nmap is a tool you run in the terminal. It works on both Windows and Linux, but this room uses Linux. Kali Linux and TryHackMe Attack Box already have nmap installed.

You type nmap plus options called switches to do different scans. To see all switches, use nmap -h or man nmap. Always include the hyphen (-) when writing a switch.

1.What is the first switch listed in the help menu for a 'SynScan' (more on this later!)?

- -sS

2.Which switch would you use for a "UDP scan"?

- -sU

3.If you wanted to detect which operating system the target is running on, which switch would you use?

- -O

4.If you wanted to detect which operating system the target is running on, which switch would you use?

- -sV

5.The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

- -v

6.Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?(Note: it's highly advisable to always use at least this option)

- -vv

We should always save the output of our scans -- this means that we only need to run the scan once (reducing network trac and thus chance of detection), and gives us a reference to use when writing reports for clients.

7.What switch would you use to save the nmap results in three major

formats?

- -oA

8.What switch would you use to save the nmap results in a "normal"

format?

- -oN

9.A very useful output format: how would you save results in a "grepable" format?

- -oG

Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

10.How would you activate this setting?

- -A

Nmap offers five levels of "timing" templates. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!

11.How would you set the timing template to level 5?

- -T5

We can also choose which port(s) to scan.

12.How would you tell nmap to only scan port 80?

- -p 80

13.How would you tell nmap to scan ports 1000-1500?

- -p 1000-1500

A very useful option that should not be ignored:

14.How would you tell nmap to scan all ports?

- -p-

15.How would you activate a script from the nmap scripting library (lots more on this later!)?

- --script

16.How would you activate all of the scripts in the "vuln" category?

- --script=vuln

Task 4 - Scan Types Overview

Nmap offers different scan types based on how it probes the target:

● SYN Scan (-sS): Fast and stealthy, doesn’t complete handshake.

● TCP Connect Scan (-sT): Completes full TCP connection.

● UDP Scan (-sU): Scans UDP ports, slower and less reliable.

● Null/FIN/Xmas Scans (-sN, -sF, -sX): Use unusual flags, may bypass firewalls.

Choose scan type based on your permissions and target defenses.

Task 5 - TCP Connect Scans

1.Which RFC defines the appropriate behaviour for the TCP protocol?

- RFC 9293

2.If a port is closed, which flag should the server send back to indicate this?

- RST

Task 6 - SYN Scans

1.There are two other names for a SYN scan, what are they?

- Half-Open, Stealth

2.Can Nmap use a SYN scan without Sudo permissions (Y/N)?

- N

Task 7 - UDP Scans

1.If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

- open|filtered

2.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?

- ICMP

Task 8 - NULL, FIN and Xmas

1.Which of the three shown scan types uses the URG flag?

- xmas

2.Why are NULL, FIN and Xmas scans generally used?

- Firewall Evasion

3.Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

- Microsoft Windows

Task 9 - ICMP Network Scanning

1.How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

- nmap -sn 172.16.0.0/16

Task 10 - NSE Scripts Overview

1.What language are NSE scripts written in?

- Lua

2.Which category of scripts would be a very bad idea to run in a production environment?

- Intrusive

Task 11 - NSE Scripts (working with NSE)

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

- maxlist

Task 12 - NSE Scripts (searching)

1.Search for "smb" scripts in the /usr/share/nmap/scripts/ directory using either of the demonstrated methods.What is the filename of the script which determines theunderlying OS of the SMB server?

- smb-os-discovery.nse

2.Read through this script. What does it depend on?

- smb-brute

Task 13 - Firewall Evasion

1.Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

- ICMP

2.[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

- --data-length

Task 14 - Practical

1.Does the target ip respond to ICMP echo (ping) requests (Y/N)?

- N

2.Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

- 999

3.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

4.Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

- 5

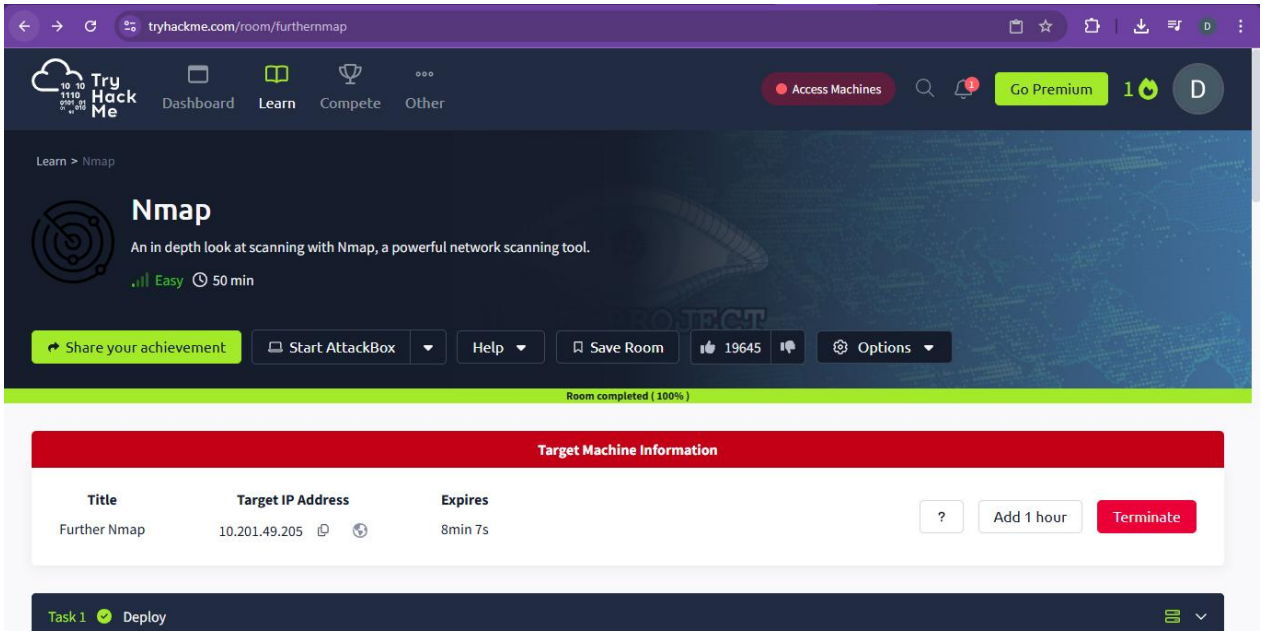
5.Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

- Y

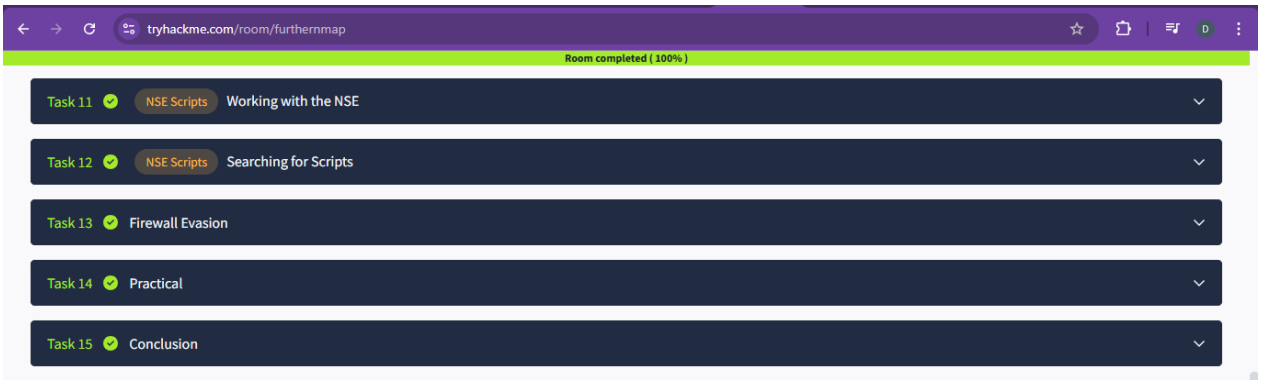
Task 15 - Conclusion

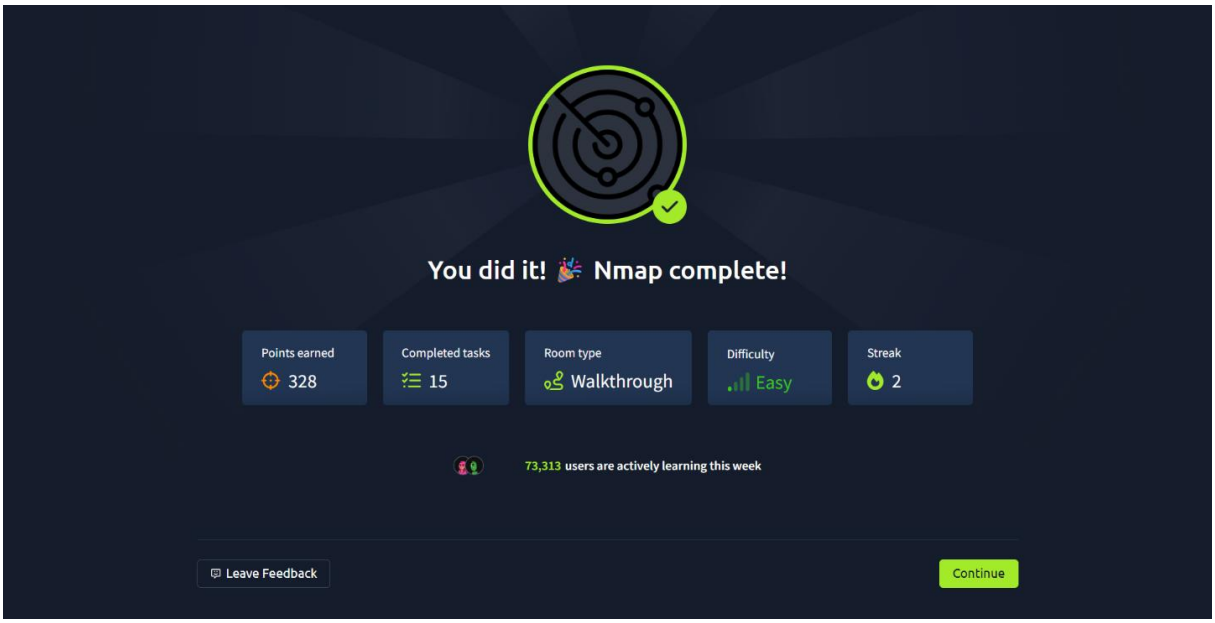
In this lab, various Nmap scan types such as SYN scan, XMAS scan, and TCP connect scan were performed to identify open, closed, or filtered ports on target systems. Each scan method provided different insights into the system's network behavior and firewall configurations. The results demonstrated how scan types can help in enumerating services and assessing network security. This practical understanding of scanning techniques is essential for ethical hacking and network analysis.I have successfully completed the “TryHackMe: Further Nmap”room, covering all tasks and learning important Nmap scanning techniques.

Screenshots




tryhackme.com/room/furthernmap
Room completed (100%)
Task 2 Introduction
Task 3 Nmap Switches
Task 4 Scan Types Overview
Task 5 Scan Types TCP Connect Scans
Task 6 Scan Types SYN Scans
Task 7 Scan Types UDP Scans
Task 8 Scan Types NULL, FIN and Xmas
Task 9 Scan Types ICMP Network Scanning
Task 10 NSE Scripts Overview


tryhackme.com/room/furthernmap
Room completed (100%)
Task 11 NSE Scripts Working with the NSE
Task 12 NSE Scripts Searching for Scripts
Task 13 Firewall Evasion
Task 14 Practical
Task 15 Conclusion


You did it! Nmap complete!
Points earned
328
Completed tasks
15
Room type
Walkthrough
Difficulty
Easy
Streak
2
73,313 users are actively learning this week
Leave Feedback
Continue