

TryHackMe Write-up - Nmap

Room: Nmap

Prepared by: Adhithyan KJ

Date: July 31, 2025

Further Nmap Room

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

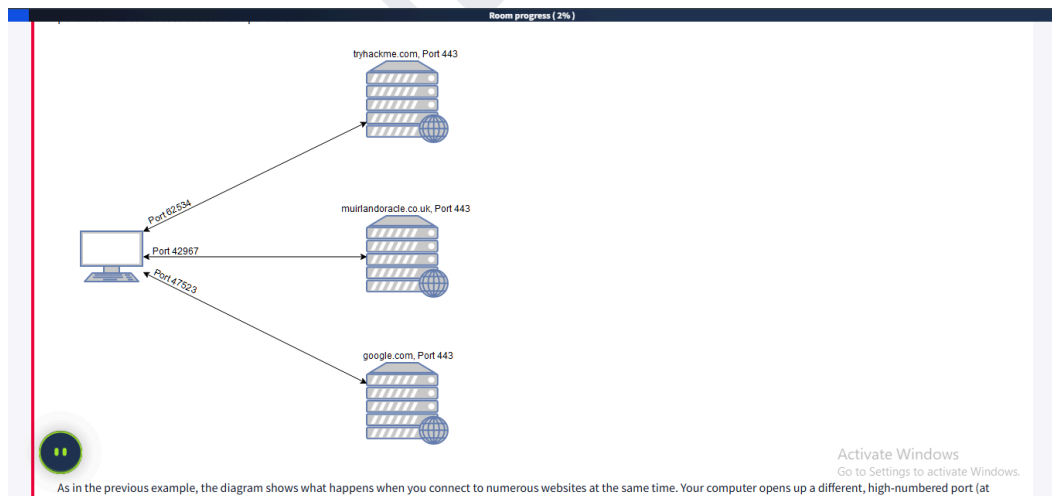
Answer: Deployed via TryHackMe - no response needed

Task 2 - Introduction

Nmap is used to scan open ports and identify vulnerabilities.

Task 3 - Nmap Switches

Nmap uses switches to control scan behavior such as -sS, -sU, -A, -T5, etc.



Task 4 - Scan Types Overview

Different scan types like SYN, TCP Connect, UDP, NULL, FIN, XMAS.

Task 5 - TCP Connect Scans

Basic TCP scan behavior following RFC standards.

Task 6 - SYN Scans

SYN scans are stealthy and efficient.

Room progress (56%)

[1] SYN scans can also be made to work by giving Nmap the CAP_NET_RAW, CAP_NET_ADMIN and CAP_NET_BIND_SERVICE permissions to run properly.

Woop woopl! Your answer is correct

Answer the questions below

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

Half-Open, Stealth ✓ Correct Answer

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

N ✓ Correct Answer

Task 7 ○ Scan Types UDP Scans

Task 8 ○ Scan Types NULL, FIN and Xmas

Task 6 ○ Scan Types ICMP Network Scanning

Activate Windows
Go to Settings to activate Windows.

Task 7 - UDP Scans

UDP scanning results and detection methods.

Room progress (61%)

Woop woopl! Your answer is correct

Due to this difficulty in identifying whether a UDP port is actually open, UDP scans tend to be incredibly slow in comparison to the first 1000 ports, with a good connection). For this reason it's usually good practice to run an Nmap scan with `--top-ports <number>` enabled. For example, scanning with `nmap -sU --top-ports 20 <target>` will scan the top 20 most commonly used UDP ports, resulting in a much more acceptable scan time.

When scanning UDP ports, Nmap usually sends completely empty requests -- just raw UDP packets. That said, for ports which are usually occupied by well-known services, it will instead send a protocol-specific payload which is more likely to elicit a response from which a more accurate result can be drawn.

Answer the questions below

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

open/filtered ✓ Correct Answer

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 ✓ Correct Answer

Task 7 ○ Scan Types NULL, FIN and Xmas

Task 8 ○ Scan Types ICMP Network Scanning

Activate Windows
Go to Settings to activate Windows.

Task 8 - NULL, FIN and Xmas

Scan types used for firewall evasion.

Room progress (60%)

is not always the case in practice. In particular Microsoft Windows (and a lot of Cisco network devices) are known to respond with a RST to any malformed TCP packet -- regardless of whether the port is actually open or not. This results in all ports showing up as being closed.

That said, the goal here is, of course, firewall evasion. Many firewalls are configured to drop incoming TCP packets to blocked ports which have the SYN flag set (thus blocking new connection initiation requests). By sending requests which do not contain the SYN flag, we effectively bypass this kind of firewall. Whilst this is good in theory, most modern IDS solutions are savvy to these scan types, so don't rely on them to be 100% effective when dealing with modern systems.

Answer the questions below

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

xmas

✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion

✓ Correct Answer

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

Microsoft Windows

✓ Correct Answer

Task 9

Scan Types

ICMP Network Scanning

Activate Windows
Go to Settings to activate Windows.

Task 9 - ICMP Network Scanning

How to perform ping sweeps using Nmap.

Room progress (70%)

✓ Woop woop! Your answer is correct

✕

The `-sn` switch tells Nmap not to scan any ports -- forcing it to rely primarily on ICMP echo packets (or ARP requests on a local network, if run with `sudo` or directly as the root user) to identify targets. In addition to the ICMP echo requests, the `-sn` switch will also cause nmap to send a TCP SYN packet to port 443 of the target, as well as a TCP ACK (or TCP SYN if not run as root) packet to port 80 of the target.

Answer the questions below

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

✓ Correct Answer

Hint

Task 10

NSE Scripts

Overview

Task 11

NSE Scripts

Working with the NSE

Task 12

NSE Scripts

Searching for Scripts

3

Firewall Evasion

Activate Windows
Go to Settings to activate Windows.

Task 10 - NSE Scripts Overview

Overview of Nmap Scripting Engine.

Room progress (75%)

A more exhaustive list can be found [here](#).

In the next task we'll look at how to interact with the NSE and make use of the scripts in these categories.

Woop woopl! Your answer is correct

Answer the questions below

What language are NSE scripts written in?

Lua

✓ Correct Answer

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

intrusive

✓ Correct Answer

Task 11 ○ NSE Scripts Working with the NSE

Task 12 ○ NSE Scripts Searching for Scripts

Task 13 ○ Firewall Evasion

Task 14 ○ Practical

Activate Windows
Go to Settings to activate Windows

Task 11 - NSE Scripts (working with NSE)

Example with ftp-anon.nse script and optional args.

Room progress (77%)

A full list of scripts and their corresponding arguments (along with example use cases) can be found [here](#).

Woop woopl! Your answer is correct

Nmap scripts come with built-in help menus, which can be accessed using `nmap --script-help <script-name>`. This tends not to be as extensive as in the link given above, however, it can still be useful when working locally.

Answer the questions below

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

maxlist

✓ Correct Answer

Task 12 ○ NSE Scripts Searching for Scripts

Task 13 ○ Firewall Evasion

Task 14 ○ Practical

Task 15 ○ Conclusion

Activate Windows
Go to Settings to activate Windows

Task 12 - NSE Scripts (searching)

Searching NSE scripts and understanding dependencies.

Room progress (81%)

```
sudo apt install nmap
```

 should fix this; however, it's also possible to install the scripts manually by downloading the script from Nmap (`sudo wget -O /usr/share/nmap/scripts/<script-name>.nse https://svn.nmap.org/nmap/scripts/<script-name>.nse`). This must then be followed up with `nmap --script-updatedb`, which updates the `script.db` file to contain the newly downloaded script.

It's worth noting that you would require the same "updatedb" command if you were to make your own NSE script and add it into Nmap -- a more than manageable task with some basic knowledge of Lua!

Answer the questions below

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 the underlying OS of the SMB server?

✓ Correct Answer

Read through this script. What does it depend on?

✓ Correct Answer

Hint

Task 13 ☐ Firewall Evasion

Task 14 ☐ Practical

Activate Windows
Go to Settings to activate Windows.

Task 13 - Firewall Evasion

Firewall evasion techniques using various Nmap switches.

Room progress (86%)

may be in place.

- `--badsum` - this is used to generate an invalid checksum for packets. Any real TCP/IP stack would drop this packet, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence

✓ Woop woopl! Your answer is correct

Answer the questions below

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

✓ Correct Answer

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

✓ Correct Answer

Task 14 ☐ Practical

Task 15 ☐ Conclusion

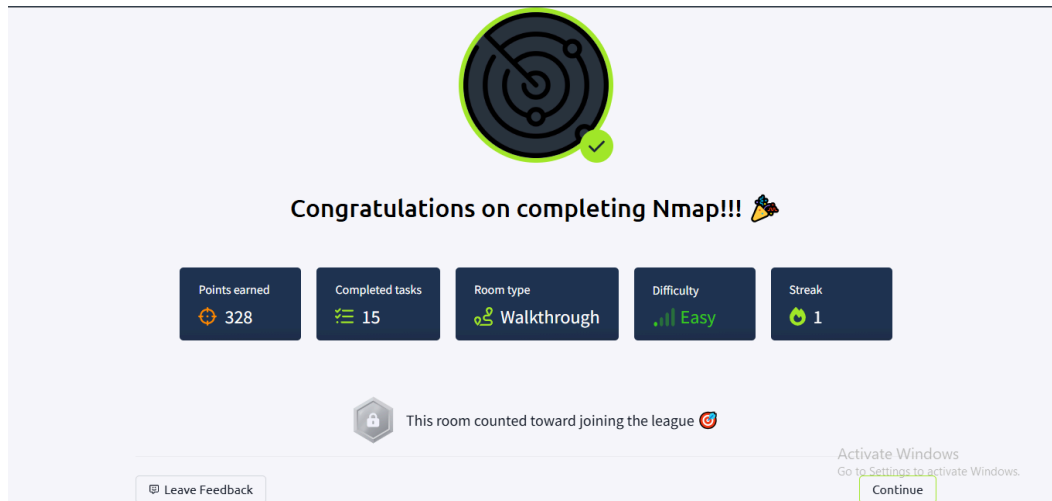
How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Activate Windows
Go to Settings to activate Windows.

Task 14 - Practical

Summary of practical scanning exercises and results.



Task 15 - Conclusion

Practical understanding of scan types and their network impact.

My TryHackMe Profile: <https://tryhackme.com/p/adhithyankj>

By Adhithyan K J