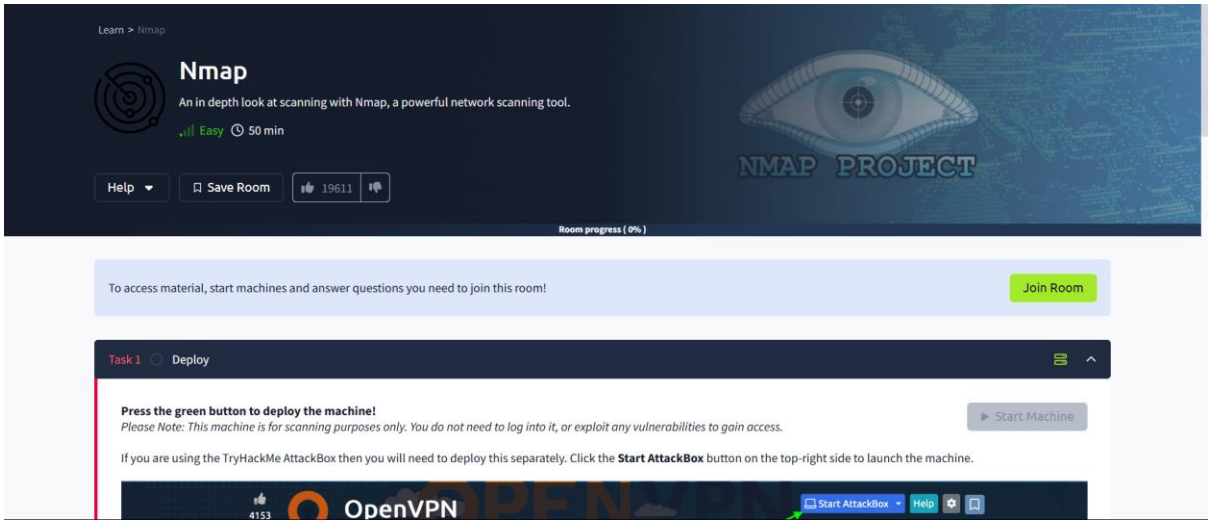


Nmap helps us establish which services are running on the targets that we are testing. We can perform a port scan to see which ports are open. Ports are necessary for making multiple multiple network requests of having multiple services available.

Deployed the machine

Task 3 Nmap Switches

Like most pentesting tools, nmap is run from the terminal. There are versions available for both Windows and Linux. For this room we will assume that you are using Linux; however, the switches should be identical. Nmap is installed by default in both Kali Linux and the TryHackMe Attack Box.

Nmap can be accessed by typing `nmap` into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do different things) we will be covering below.

All you'll need for this is the help menu for nmap (accessed with `nmap -h`) and/or the nmap man page (access with `man nmap`). For each answer, include all parts of the switch unless otherwise specified. This includes the hyphen at the start (`-`).

Answer the questions below

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

-sS ✓ Correct Answer

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

-sU ✓ Correct Answer

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

-O ✓ Correct Answer

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV ✓ Correct Answer

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

-v ✓ Correct Answer

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 ✓ Correct Answer

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

What switch would you use to save the nmap results in three major formats?

-oA ✓ Correct Answer

What switch would you use to save the nmap results in a "normal" format?

-oN ✓ Correct Answer

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

-oG ✓ Correct Answer

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.

How would you activate this setting?

-A ✓ Correct Answer

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

How would you set the timing template to level 5?

-T5 ✓ Correct Answer

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

How would you tell nmap to only scan port 80?

-p 80

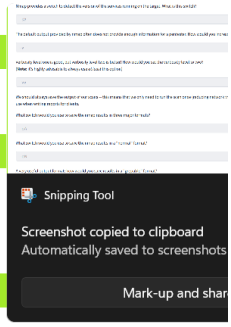
How would you tell nmap to scan ports 1000-1500?

-p 1000-1500

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

-p-



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

--script ✓ Correct Answer

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

--script=vuln ✓ Correct Answer Hint

Task 4 Scan Types Overview

When port scanning with Nmap, there are three basic scan types. These are:

- TCP Connect Scans (`-sT`)
- SYN "Half-open" Scans (`-sS`)
- UDP Scans (`-sU`)

Additionally there are several less common port scan types, some of which we will also cover (albeit in less detail). These are:

- TCP Null Scans (`-sN`)
- TCP FIN Scans (`-sF`)
- TCP Xmas Scans (`-sX`)

Most of these (with the exception of UDP scans) are used for very similar purposes, however, the way that they work differs between each scan. This means that, whilst one of the first three scans are likely to be your go-to in most situations, it's worth bearing in mind that other scan types exist.

In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Answer the questions below

Read the Scan Types Introduction.

No answer needed ✓ Correct Answer

Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 9293 ✓ Correct Answer Hint

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

RST ✓ Correct Answer

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

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

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

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

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

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?

smb-os-discovery.nse ✓ Correct Answer

Read through this script. What does it depend on?

smb-brute ✓ Correct Answer Hint

Answer the questions below

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

ICMP — ✓ Correct Answer

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

--data-length — ✓ Correct Answer

Answer the questions below

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

N — ✓ Correct Answer

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

999 — ✓ Correct Answer

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!

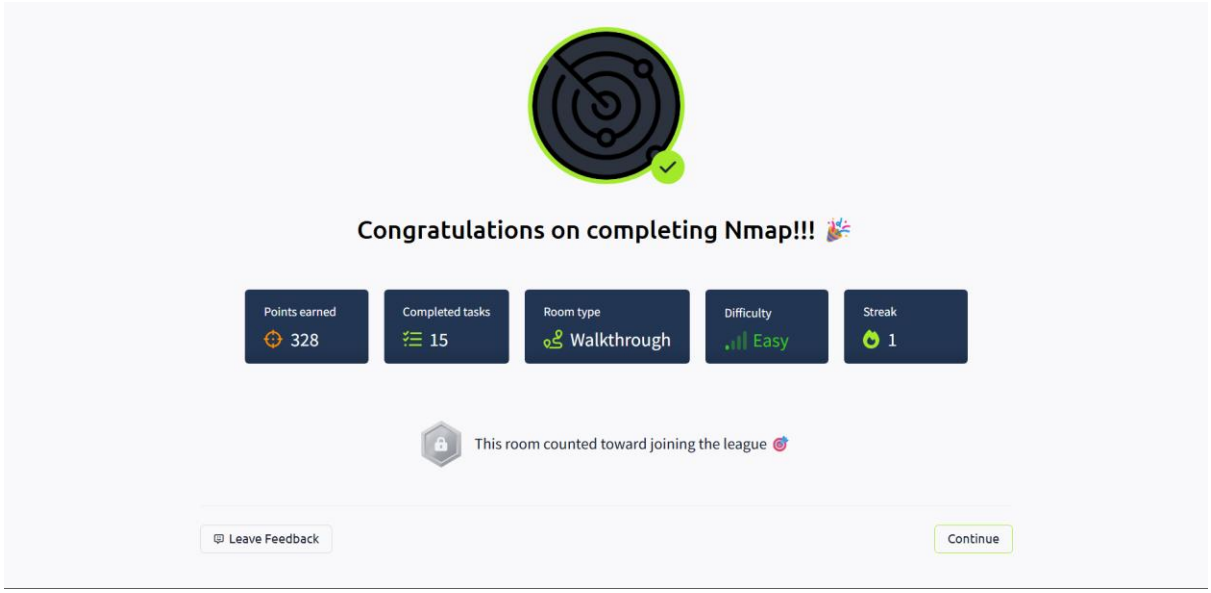
No Response — ✓ Correct Answer — Hint

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

5 — ✓ Correct Answer

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 — ✓ Correct Answer



Completed the lab !