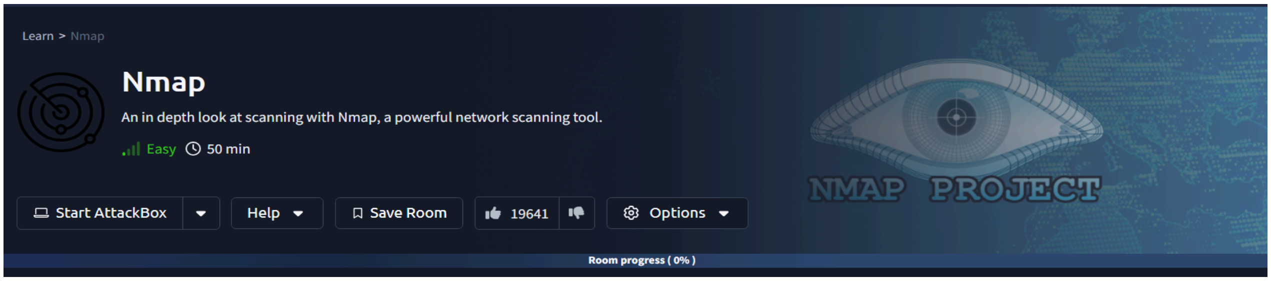
TryHackMe Nmap Room Walkthrough



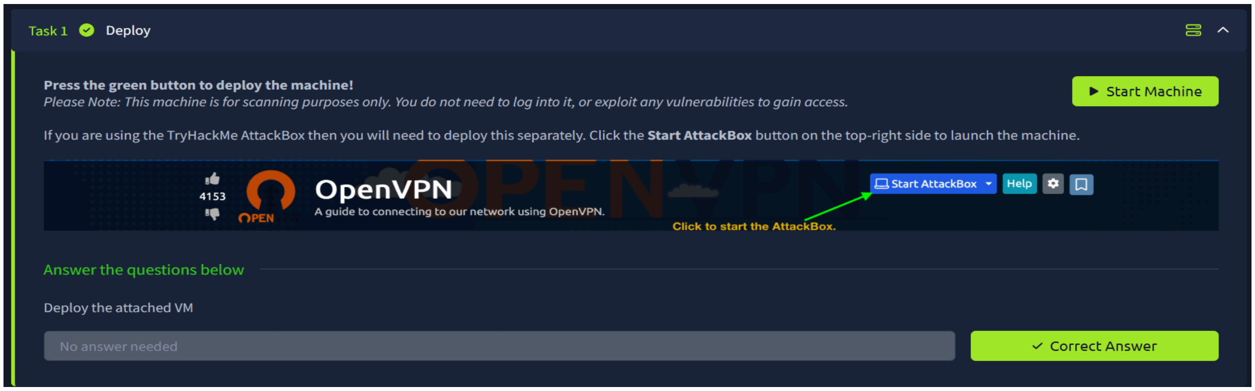
Learn > Nmap

Nmap

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

⭐ Task 1: Deploy the Machine

I deployed the target machine using the green “Start Machine” button.



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.

Start Machine
4153
OPEN
OpenVPN
A guide to connecting to our network using OpenVPN.
Start AttackBox
Help
Click to start the AttackBox.

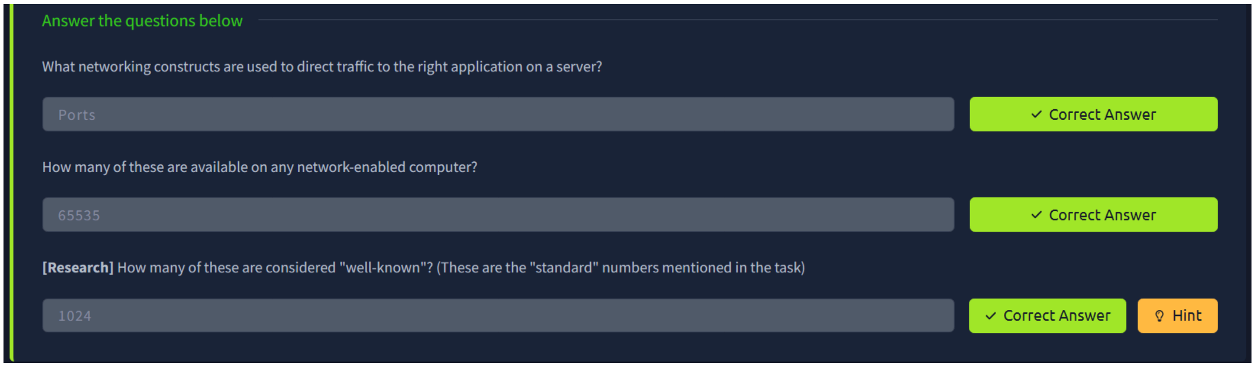
Answer the questions below

Deploy the attached VM

No answer needed

⭐ Task 2: Introduction

I revisited the fundamentals of how ports direct traffic to the correct application. I also reviewed how many ports are available on a system and which ranges are considered “well-known.”



Answer the questions below

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

Ports

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

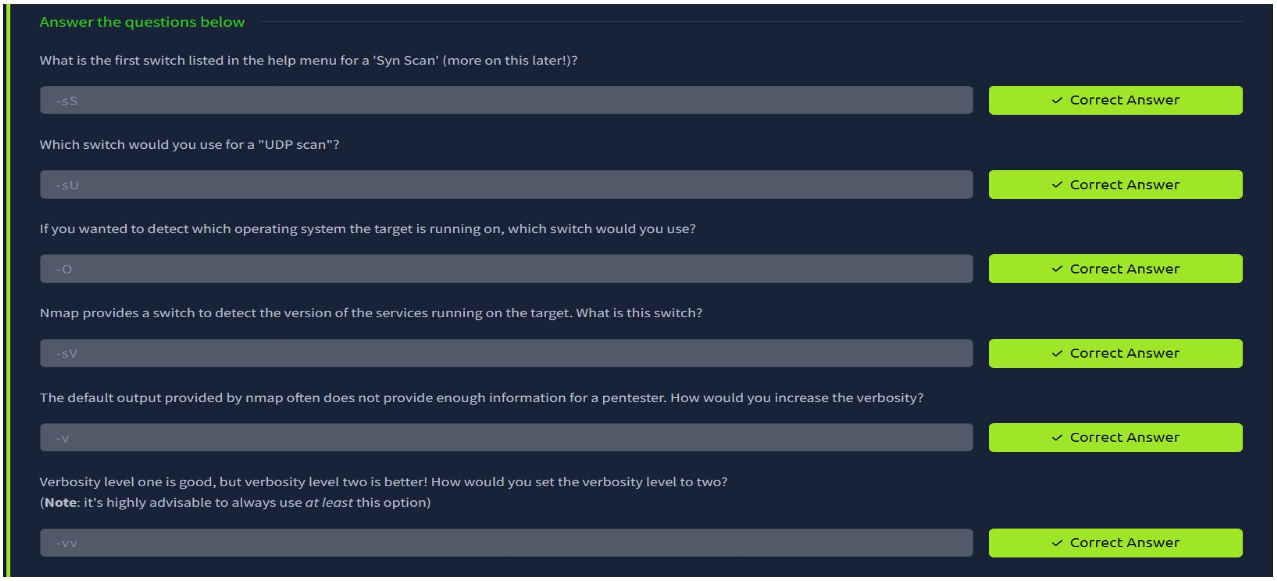
65535

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

1024

⭐ Task 3: Nmap Switches

Here, I explored Nmap's most useful switches. These include techniques to scan for services, detect the OS, increase verbosity in results, save scans in multiple formats, and even run vulnerability checks using Nmap scripts.



Answer the questions below

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

-sS

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

-sU

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

-O

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

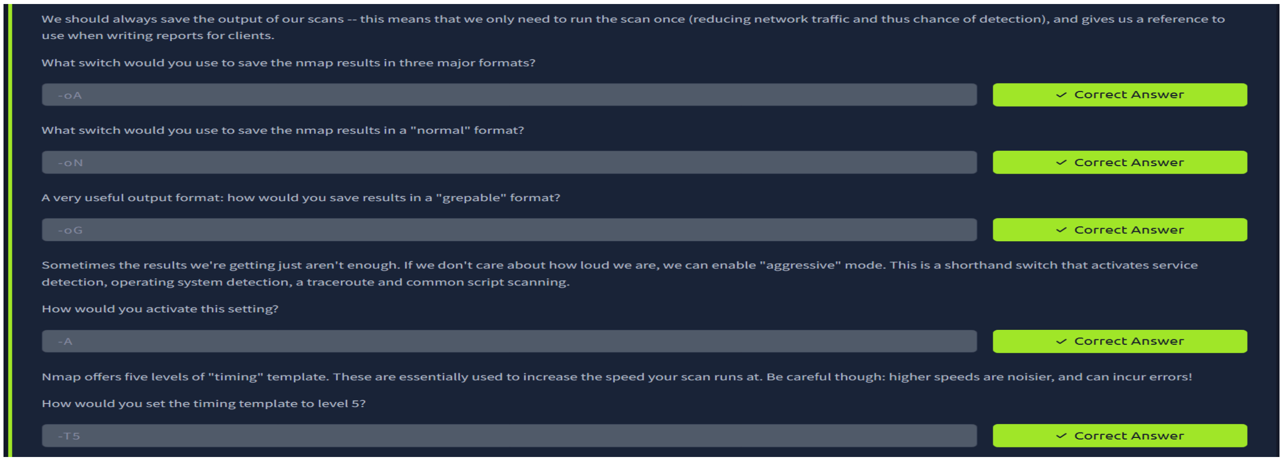
-sV

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

-v

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 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

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

-oN

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.

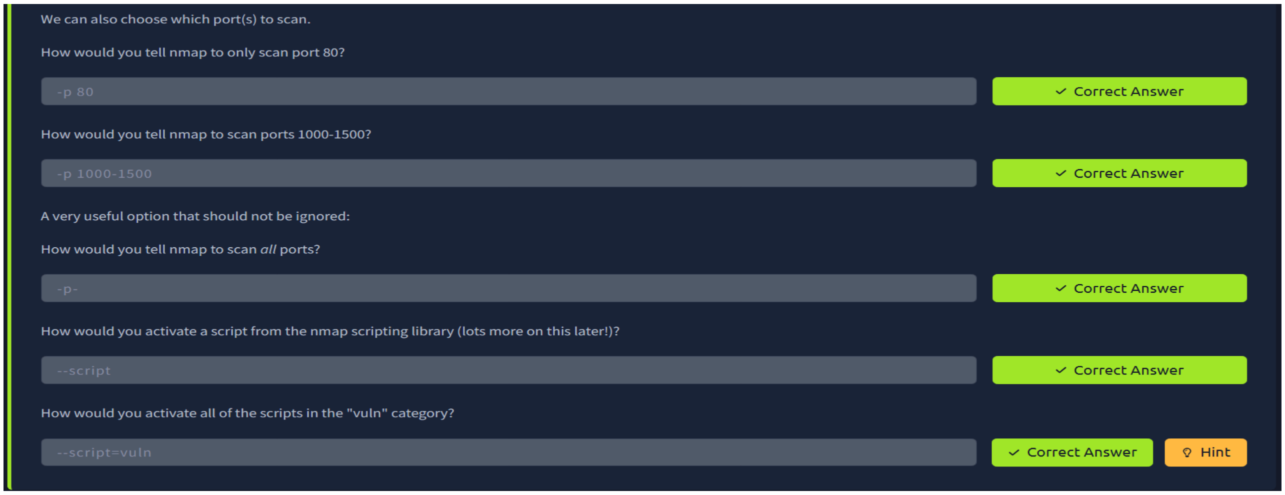
How would you activate this setting?

-A

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



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!)?

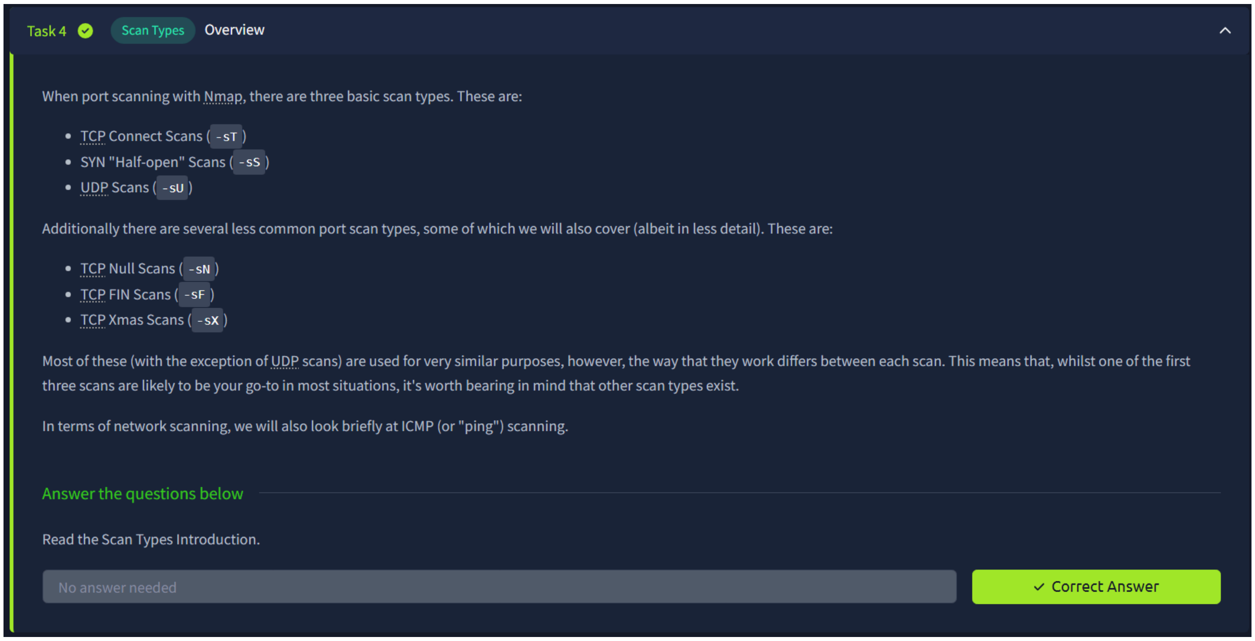
--script

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

--script=vuln

⭐ Task 4: Scan Types Overview

I looked at different types of port scans available in Nmap. Each scan type serves a specific purpose from stealth scans to full connection attempts and selecting the right one depends on the situation.



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.

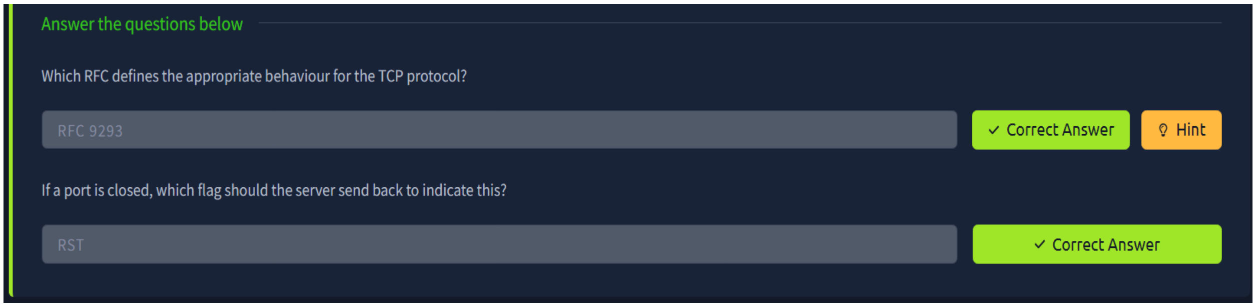
Answer the questions below

Read the Scan Types Introduction.

No answer needed

⭐ Task 5: TCP Connect Scans

In this task, I learned about TCP Connect scan, which establishes a full connection using the standard three-way handshake. Through this method, I learned how systems respond based on RFC 793, especially how closed ports send a reset flag (RST).



Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

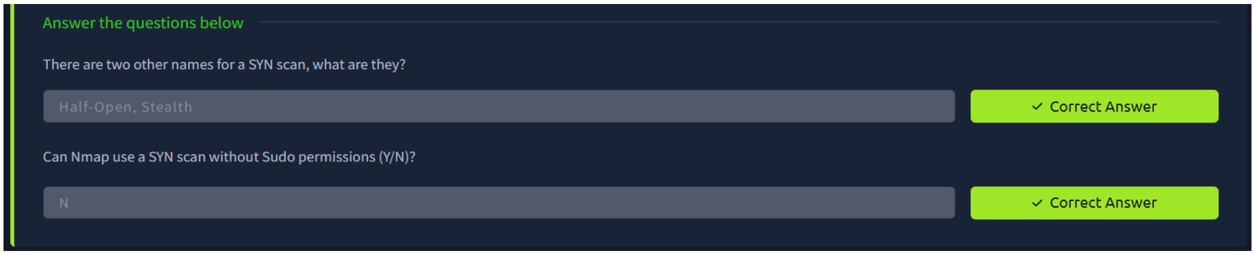
RFC 9293

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

RST

⭐ Task 6: SYN Scans

Next, I explored SYN scans, also known as “half-open” or “stealth” scans. These scans don’t complete the TCP handshake, making them less detectable — though they do require elevated privileges (sudo) to perform effectively.



Answer the questions below

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

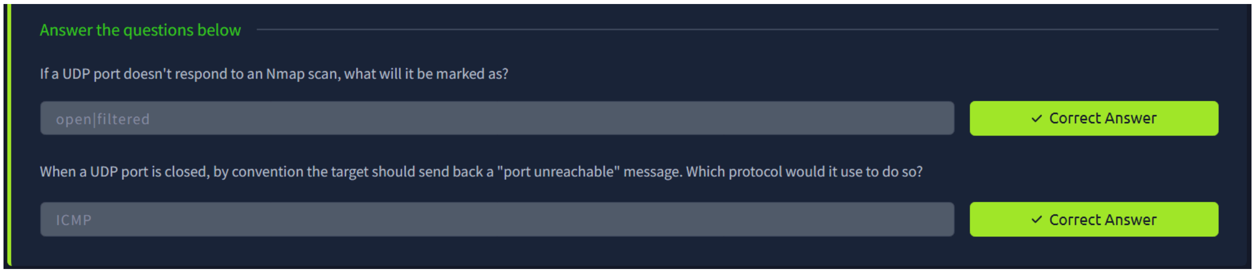
Half-Open, Stealth

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

N

⭐ Task 7: UDP Scans

When I moved on to UDP scanning, I realized it's much harder to draw strong conclusions due to the lack of responses from open ports. I also learned that closed UDP ports usually reply with ICMP port unreachable messages.



Answer the questions below

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

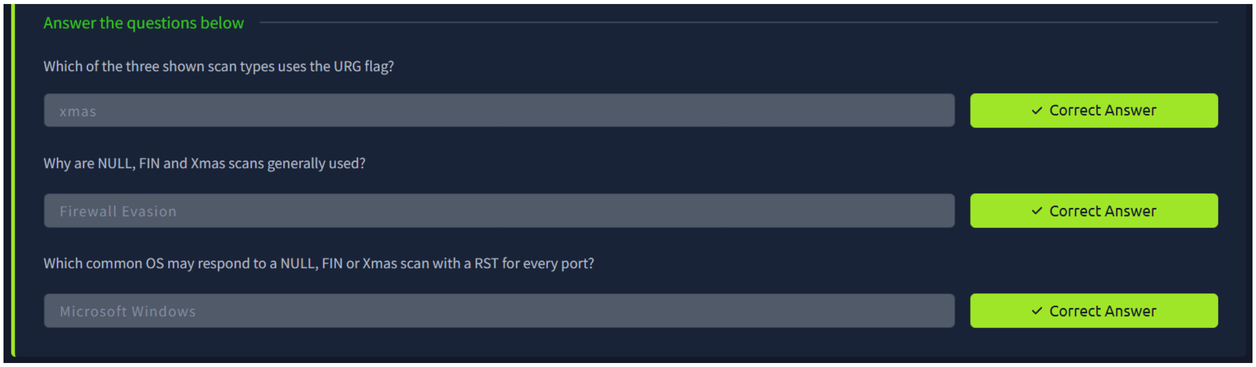
open|filtered

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?

ICMP

⭐ Task 8: NULL, FIN, and Xmas Scans

I then tried out some stealthier scans using unusual TCP flag combinations — such as NULL, FIN, and Xmas scans — to bypass firewalls. While effective in some cases, I also noted that Windows systems tend to send back RST packets for every port.



Answer the questions below

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

xmas

Why are NULL, FIN and Xmas scans generally used?

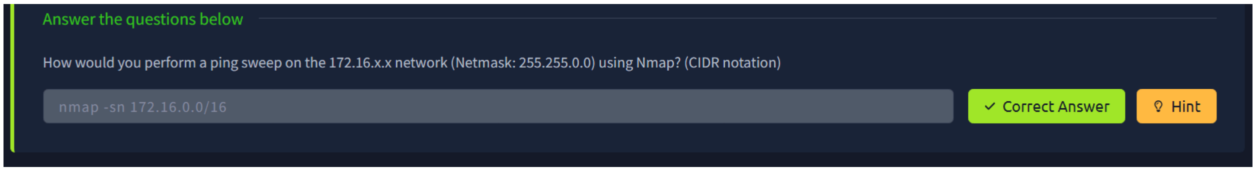
Firewall Evasion

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

While exploring ICMP-based scanning, I performed a ping sweep across a subnet using CIDR notation. This helped me identify which hosts were online within the 172.16.x.x range.



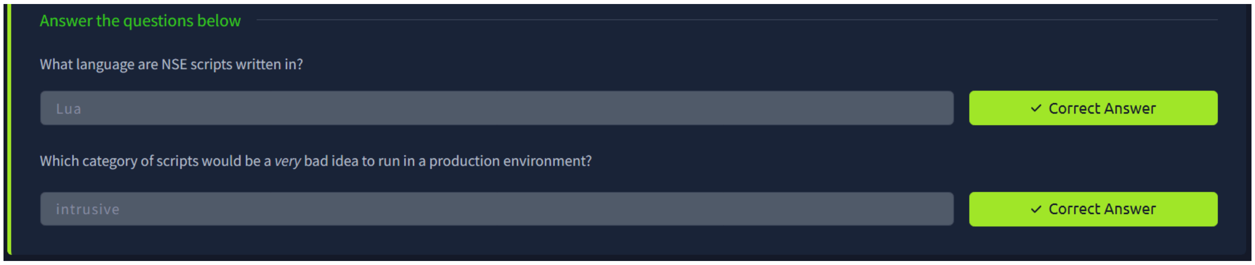
Answer the questions below

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
```

⭐ Task 10: NSE Script Overview

This task introduced me to the power of NSE (Nmap Scripting Engine). I looked at what language the scripts are written in (Lua) and noted that intrusive scripts should be avoided in production due to their potentially disruptive behavior.



Answer the questions below

What language are NSE scripts written in?

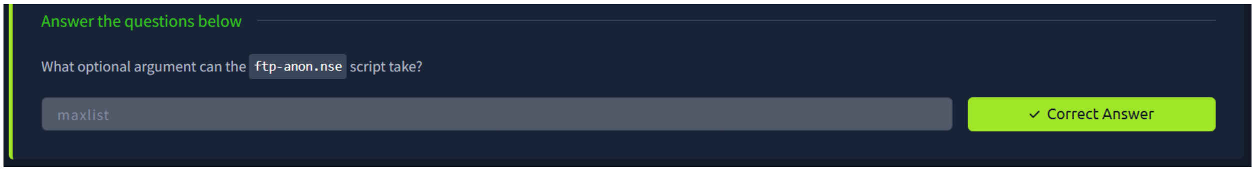
Lua

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

intrusive

⭐ Task 11: Working with the NSE

Here, I experimented with the ftp-anon.nse script to see how it behaves with optional arguments like maxlist, which allows deeper enumeration of accessible files on anonymous FTP servers.



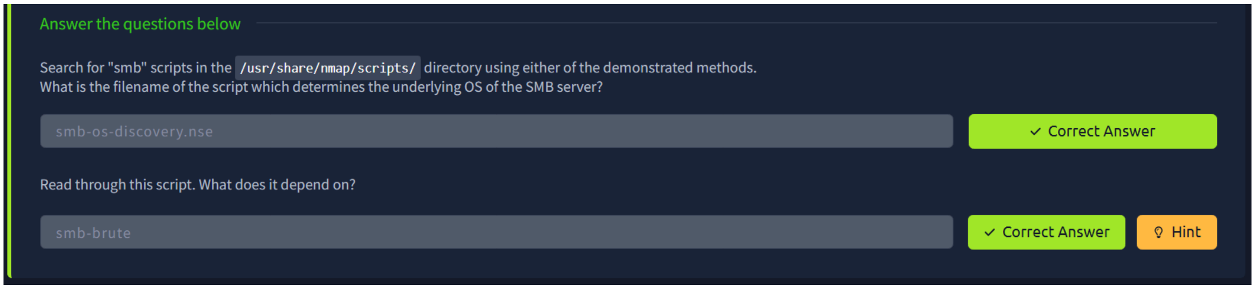
Answer the questions below

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

maxlist

⭐ Task 12: Searching for Scripts

I searched through Nmap's script directory for anything related to SMB. That's how I found smb-os-discovery.nse, which I confirmed depends on another script: smb-brute.



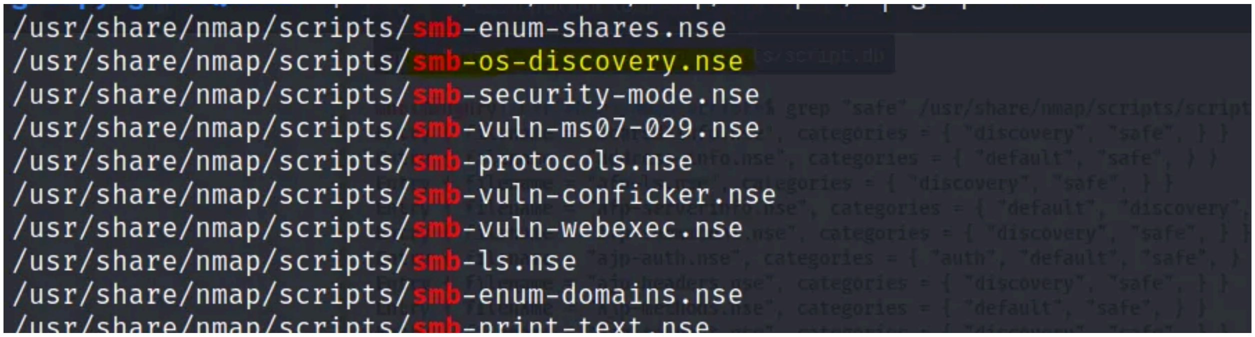
Answer the questions below

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?

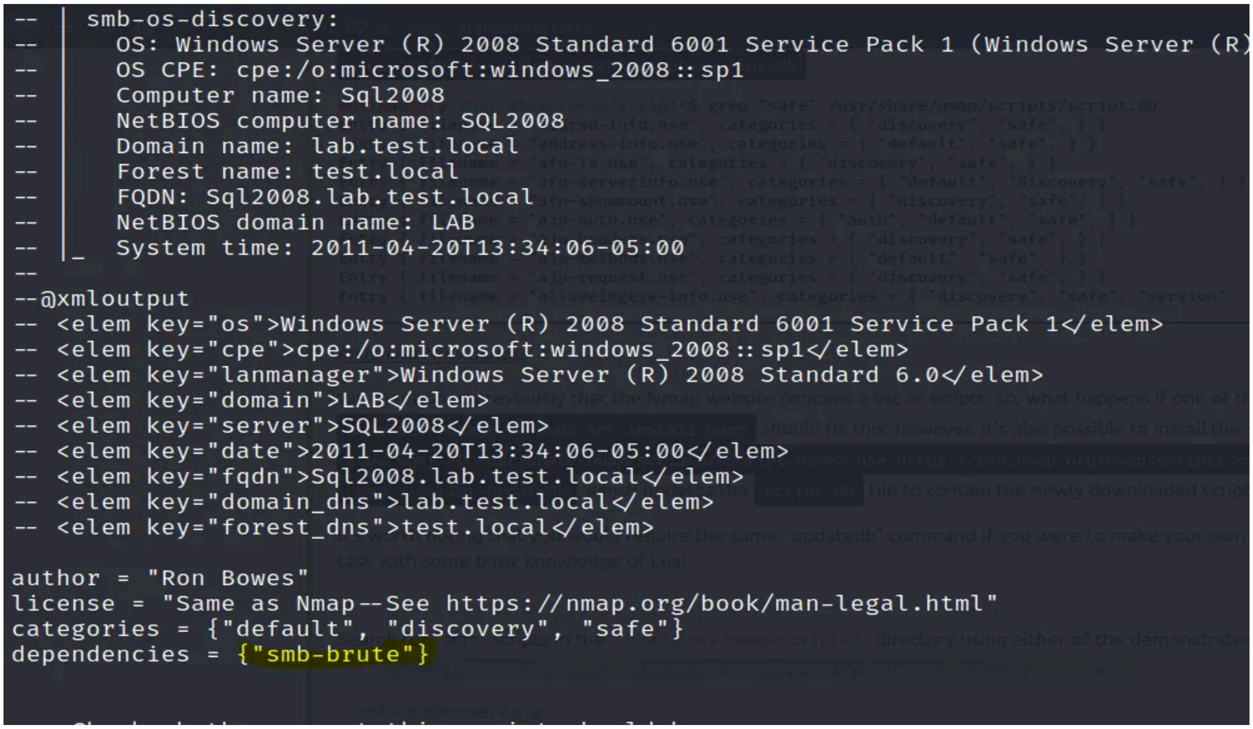
smb-os-discovery.nse

Read through this script. What does it depend on?

smb-brute



```
/usr/share/nmap/scripts/smb-enum-shares.nse
/usr/share/nmap/scripts/smb-os-discovery.nse
/usr/share/nmap/scripts/smb-security-mode.nse
/usr/share/nmap/scripts/smb-vuln-ms07-029.nse
/usr/share/nmap/scripts/smb-protocols.nse
/usr/share/nmap/scripts/smb-vuln-conficker.nse
/usr/share/nmap/scripts/smb-vuln-webexec.nse
/usr/share/nmap/scripts/smb-ls.nse
/usr/share/nmap/scripts/smb-enum-domains.nse
/usr/share/nmap/scripts/smb-print-text.nse
```

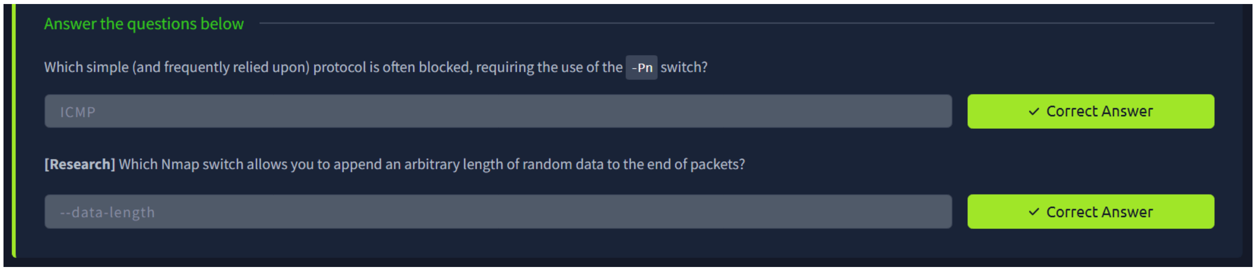


```
-- | smb-os-discovery:
--     OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R)
--     OS CPE: cpe:/o:microsoft:windows_2008::sp1
--     Computer name: Sql2008
--     NetBIOS computer name: SQL2008
--     Domain name: lab.test.local
--     Forest name: test.local
--     FQDN: Sql2008.lab.test.local
--     NetBIOS domain name: LAB
-- |_  System time: 2011-04-20T13:34:06-05:00
--
--@xmloutput
-- <elem key="os">Windows Server (R) 2008 Standard 6001 Service Pack 1</elem>
-- <elem key="cpe">cpe:/o:microsoft:windows_2008::sp1</elem>
-- <elem key="lanmanager">Windows Server (R) 2008 Standard 6.0</elem>
-- <elem key="domain">LAB</elem>
-- <elem key="server">SQL2008</elem>
-- <elem key="date">2011-04-20T13:34:06-05:00</elem>
-- <elem key="fqdn">Sql2008.lab.test.local</elem>
-- <elem key="domain_dns">lab.test.local</elem>
-- <elem key="forest_dns">test.local</elem>

author = "Ron Bowes"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
dependencies = {"smb-brute"}
```

⭐ Task 13: Firewall Evasion

In this section, I worked on evading firewall rules by using switches like -Pn, which skips host discovery when ICMP is blocked, and --data-length, which lets me append random data to packets to potentially confuse intrusion systems.



Answer the questions below

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

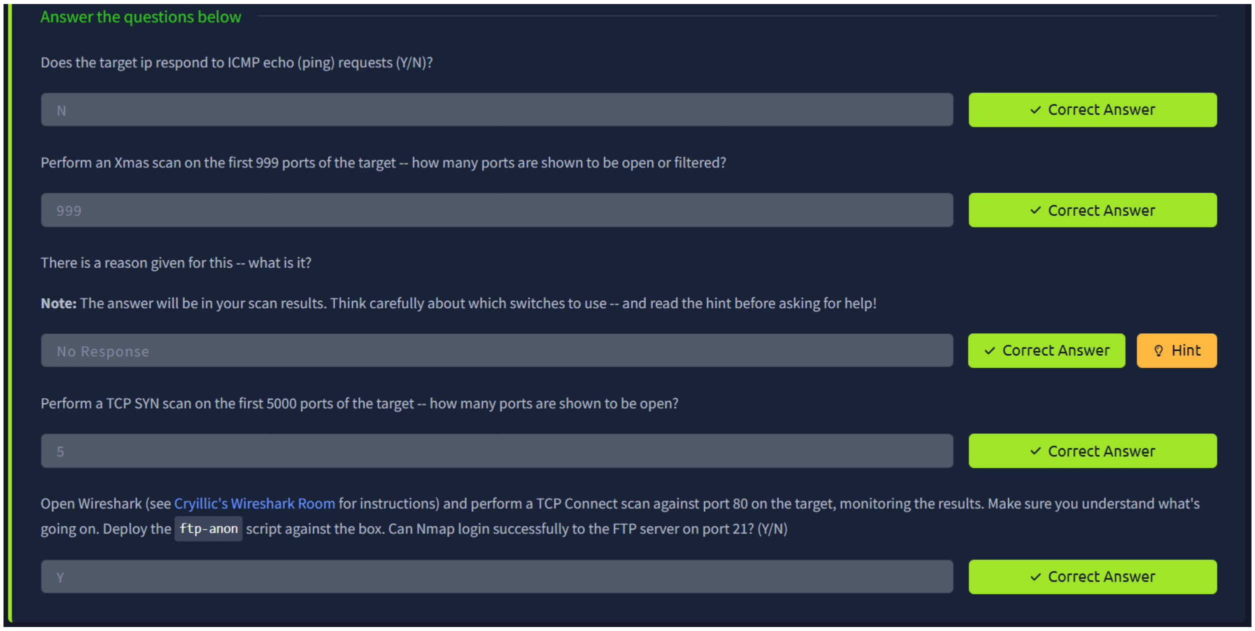
ICMP

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

--data-length

⭐ Task 14: Practical

Here, I put multiple scan techniques into action. I tested if the target responded to ICMP ran an Xmas scan, counted open or filtered ports, followed up with a SYN scan, and finally used the ftp-anon script to check for anonymous FTP access — which was successful.



Answer the questions below

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

N

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

999

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!

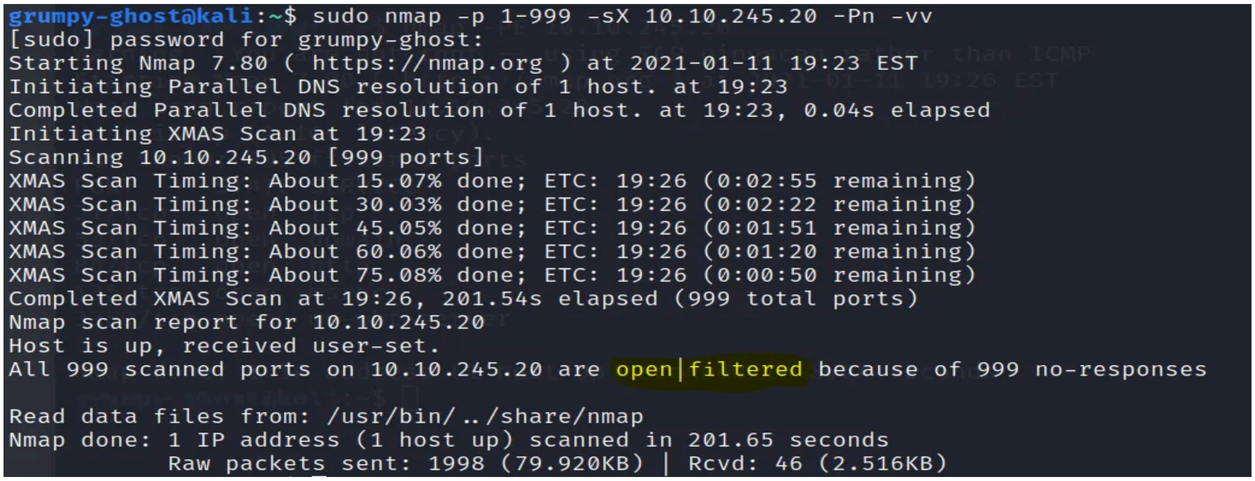
No Response

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

5

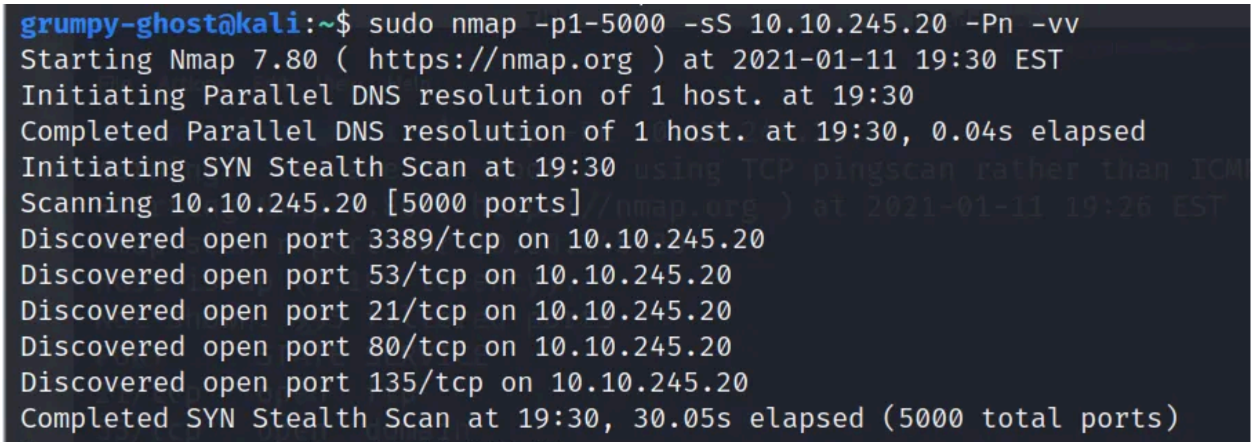
Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y



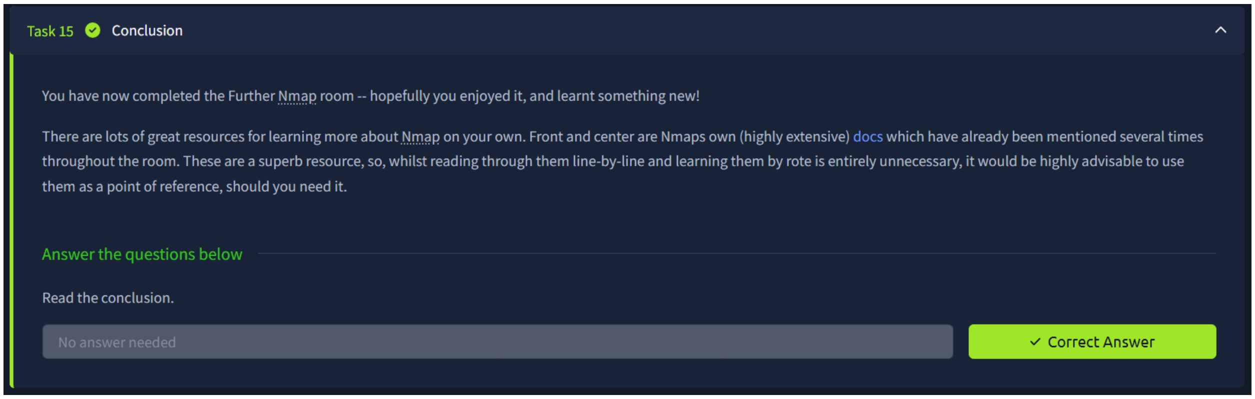
```
grumpy-ghost@kali:~$ sudo nmap -p 1-999 -sX 10.10.245.20 -Pn -vv
[sudo] password for grumpy-ghost:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:23 EST
Initiating Parallel DNS resolution of 1 host. at 19:23
Completed Parallel DNS resolution of 1 host. at 19:23, 0.04s elapsed
Initiating XMAS Scan at 19:23
Scanning 10.10.245.20 [999 ports]
XMAS Scan Timing: About 15.07% done; ETC: 19:26 (0:02:55 remaining)
XMAS Scan Timing: About 30.03% done; ETC: 19:26 (0:02:22 remaining)
XMAS Scan Timing: About 45.05% done; ETC: 19:26 (0:01:51 remaining)
XMAS Scan Timing: About 60.06% done; ETC: 19:26 (0:01:20 remaining)
XMAS Scan Timing: About 75.08% done; ETC: 19:26 (0:00:50 remaining)
Completed XMAS Scan at 19:26, 201.54s elapsed (999 total ports)
Nmap scan report for 10.10.245.20
Host is up, received user-set.
All 999 scanned ports on 10.10.245.20 are open|filtered because of 999 no-responses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.65 seconds
           Raw packets sent: 1998 (79.920KB) | Rcvd: 46 (2.516KB)
```



```
grumpy-ghost@kali:~$ sudo nmap -p1-5000 -sS 10.10.245.20 -Pn -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:30 EST
Initiating Parallel DNS resolution of 1 host. at 19:30
Completed Parallel DNS resolution of 1 host. at 19:30, 0.04s elapsed
Initiating SYN Stealth Scan at 19:30
Scanning 10.10.245.20 [5000 ports]
Discovered open port 3389/tcp on 10.10.245.20
Discovered open port 53/tcp on 10.10.245.20
Discovered open port 21/tcp on 10.10.245.20
Discovered open port 80/tcp on 10.10.245.20
Discovered open port 135/tcp on 10.10.245.20
Completed SYN Stealth Scan at 19:30, 30.05s elapsed (5000 total ports)
```

⭐ Task 15: Conclusion



Task 15 ✓ Conclusion

You have now completed the Further Nmap room -- hopefully you enjoyed it, and learnt something new!

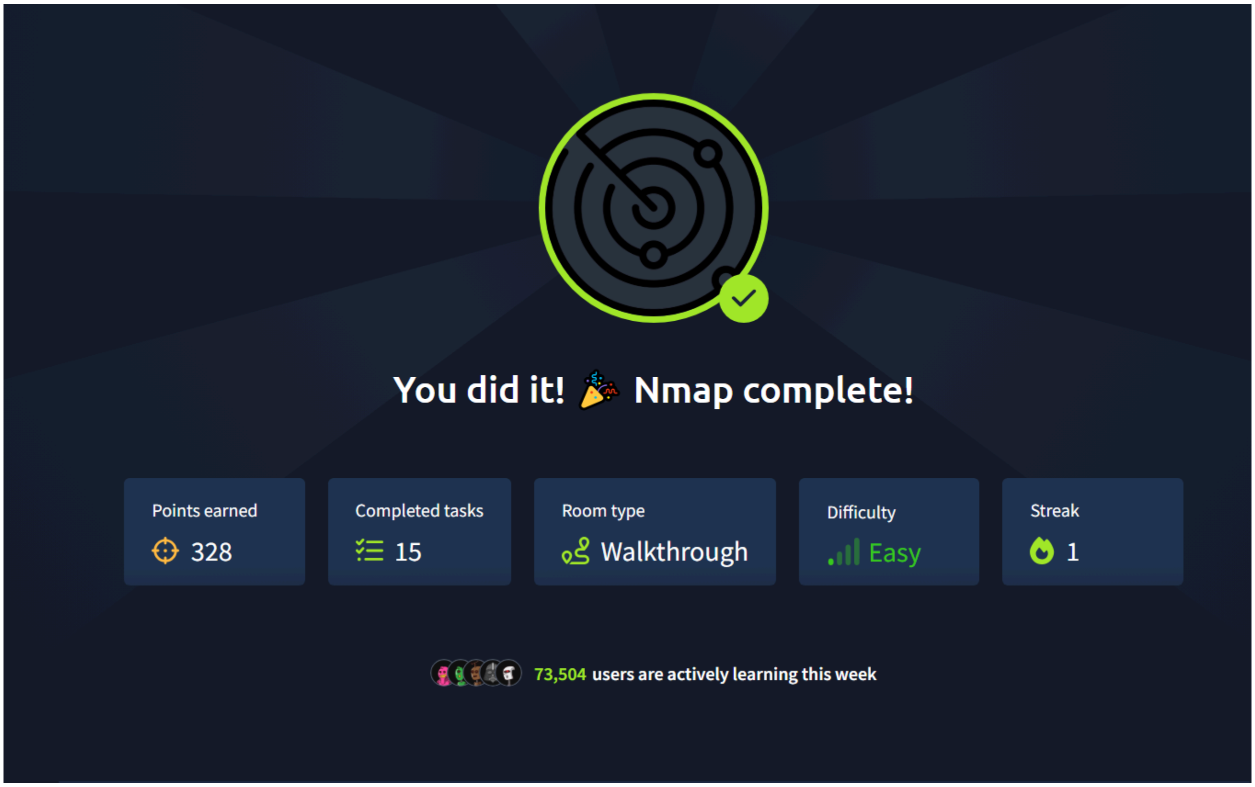
There are lots of great resources for learning more about Nmap on your own. Front and center are Nmaps own (highly extensive) docs which have already been mentioned several times throughout the room. These are a superb resource, so, whilst reading through them line-by-line and learning them by rote is entirely unnecessary, it would be highly advisable to use them as a point of reference, should you need it.

Answer the questions below

Read the conclusion.

No answer needed

✓ Correct Answer



You did it! 🎉 Nmap complete!

Points earned 328

Completed tasks 15

Room type Walkthrough

Difficulty Easy

Streak 1

73,504 users are actively learning this week
