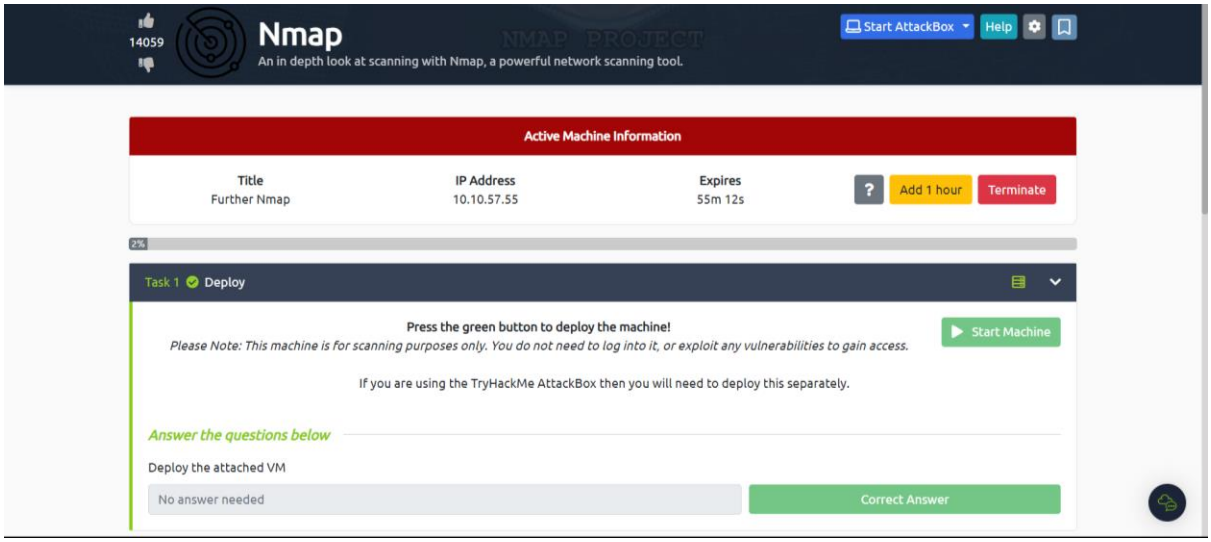
Assignment 1

THE CYBERHOST Cyber Security Intern

Task 1: Deploy

First, we have to join the room to access the room then we just have to deploy the attached VM and start the Machine.



After starting the machine, we will get a IP Address after 60 seconds. And the task will be completed.

Task 2: Introduction

Here we are introduced to ports.

We have to go through the all of the text. Then answer the questions:

Q1. What networking constructs are used to direct traffic to the right application on a server?

A1. ports

Q2. How many of these are available on any network-enabled computer?

A2. 65535

Q3. [Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

A3. 1024.

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

I have Kali Linux installed but for now we will use our AttackBox provided by TryHackMe to access nmap.

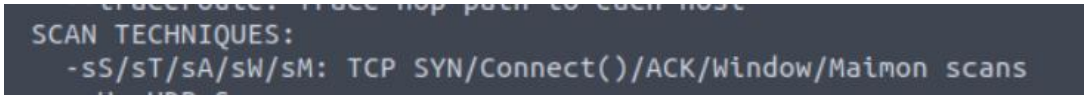
To understand nmap start the terminal and type ‘man nmap’ or ‘nmap -h’ it will give all the details about nmap tool.

Now we will go through all the commands mentioned.

And we will answer the questions:

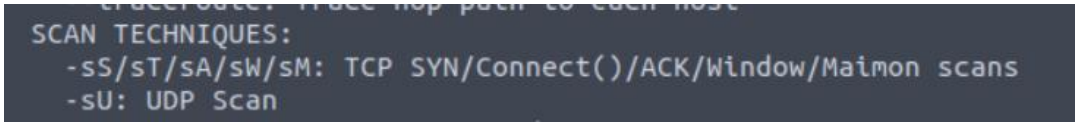
Q1. What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

A1. -sS



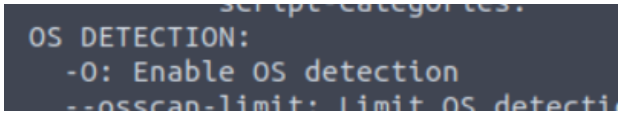
Q2. Which switch would you use for a "UDP scan"?

A2. -sU



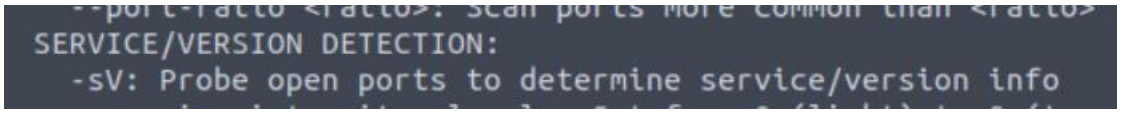
Q3. If you wanted to detect which operating system the target is running on, which switch would you use?

A3. -O



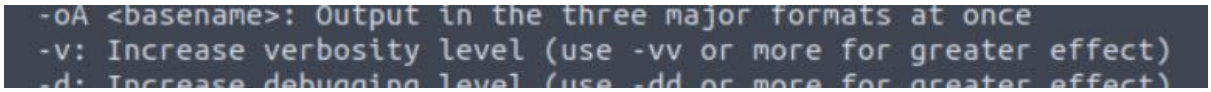
Q4. Nmap provides a switch to detect the version of the services running on the target. What is this switch?

A4. -sV



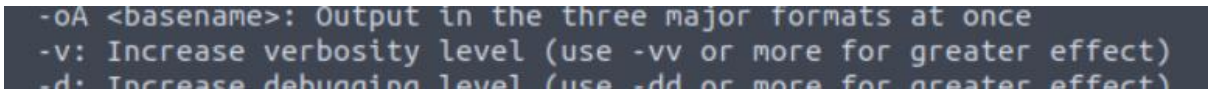
Q5. The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

A5. -V



Q6. 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)

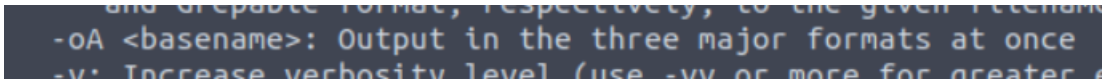
A6. -vv



Q7. 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?

A7. -oA

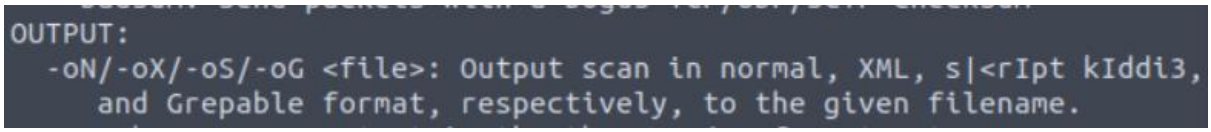


Q8. What switch would you use to save the nmap results in a "normal" format?

A8. -oN

Q9. A very useful output format: how would you save results in a "grepable" format?

A9. -oG



Q10. 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?
A10. -A

```
            -A: Enable OS detection, version detection, script scanning, and trace
route
```

Q11. 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?
A11. -T5

```
 -T<0-5>: Set timing template (higher is faster)
```

Q12. We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?
A12. -p 80

```
  -p <port ranges>: Only scan specified ports
```

Q13. How would you tell nmap to scan ports 1000-1500?

A13. -p 1000-1500

```
 Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
-exclude-ports <port ranges>: Exclude the specified ports from scanni
```

Q14. A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?
A14. -p-

Q15. How would you activate a script from the nmap scripting library (lots more on this later!)?

A15. --script

```
SCRIPT SCAN:
  -sC: equivalent to --script=default
```

Q16. How would you activate all of the scripts in the "vuln" category?

A16. --script=vuln

```
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
directories, script-files or script-categories
```

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 — Correct Answer

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

-P 1000-1500 — Correct Answer

A very useful option that should not be ignored:

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

-P- — Correct Answer

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.

Task 5: Scan Types: TCP Connect Scans

Here, we understand TCP 3-way handshake. And according to that nmap can get to know whether port is open or closed or hidden behind a firewall

If the request is sent to an *open* port, the target will respond with a TCP packet with the SYN/ACK flags set. Nmap then marks this port as being *open*.

If Nmap sends a TCP request with the *SYN* flag set to a *closed* port, the target server will respond with a TCP packet with the *RST* (Reset) flag set.

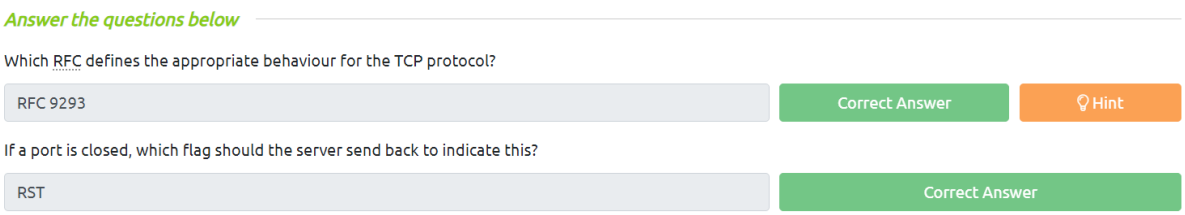
If Nmap sends a TCP SYN request, and receives nothing back. This indicates that the port is being protected by a firewall and thus the port is considered to be *filtered*.

Q1. Which RFC defines the appropriate behaviour for the TCP protocol?

A1. RFC 9293

Q2. If a port is closed, which flag should the server send back to indicate this?

A2. RST



Task 6: Scan Types: SYN Scans

SYN scans are sometimes referred to as "Half-open" scans, or "Stealth" scans.

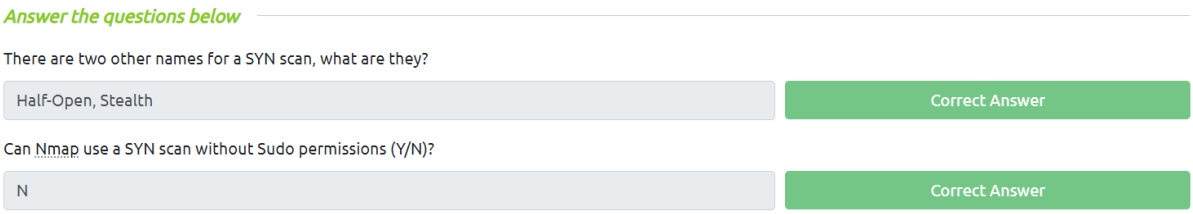
Where TCP scans perform a full three-way handshake with the target, SYN scans sends back a RST TCP packet after receiving a SYN/ACK from the server.

Q1. There are two other names for a SYN scan, what are they?

A1. Half-Open, Stealth

Q2. Can Nmap use a SYN scan without Sudo permissions (Y/N)?

A2. N



Task 7: Scan Types: UDP Scans

When a packet is sent to an open UDP port, there should be no response. When this happens, Nmap refers to the port as being open|filtered.

In other words, it suspects that the port is open, but it could be firewalled.

If it gets a UDP response (which is very unusual), then the port is marked as open.

When a packet is sent to a closed UDP port, the target should respond with an ICMP (ping) packet containing a message that the port is unreachable.

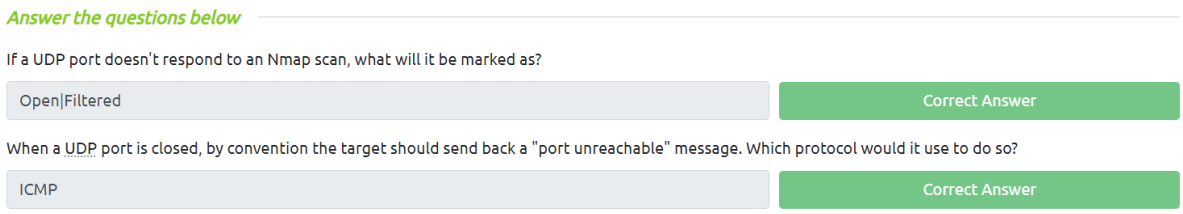
This clearly identifies closed ports, which Nmap marks as such and moves on.

Q1. If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

A1. Open|Filtered

Q2. 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?

A2. ICMP



Task 8: Scan Types: NULL, FIN and Xmas

NULL scans (-sN) are when the TCP request is sent with no flags set at all. As per the RFC, the target host should respond with a RST if the port is closed.

FIN scans (-sF) work in an almost identical fashion; however, instead of sending a completely empty packet, a request is sent with the FIN. Once again, Nmap expects a RST if the port is closed.

Xmas scans (-sX) send a malformed TCP packet and expects a RST response for closed ports. It's referred to as an xmas scan as the flags that it sets (PSH, URG and FIN) give it the appearance of a blinking christmas tree when viewed as a packet capture in Wireshark.

Q1. Which of the three shown scan types uses the URG flag?

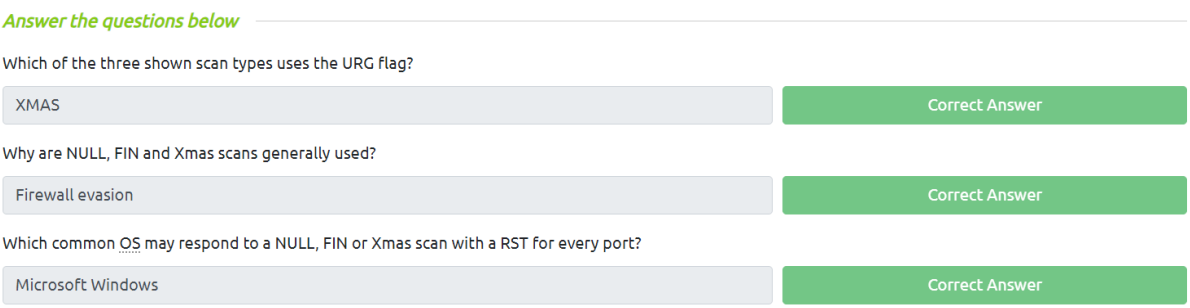
A1. XMAS

Q2. Why are NULL, FIN and Xmas scans generally used?

A2. Firewall evasion

Q3. Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

A3. Microsoft Windows

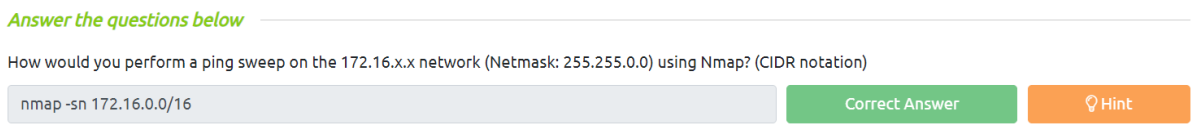


Task 9: Scan Types: ICMP Network Scanning

Nmap sends an ICMP packet to each possible IP address for the specified network. When it receives a response, it marks the IP address that responded as being alive.

Q1. How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

A1. nmap -sn 172.16.0.0/16



Task 10: NSE Scripts: Overview

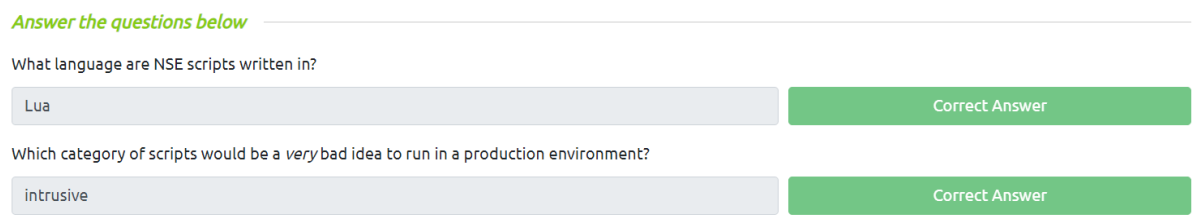
The **N**map **S**cripting **E**ngine (NSE) is an incredibly powerful addition to Nmap, extending its functionality quite considerably. NSE Scripts are written in the Lua programming language, and can be used to do a variety of things: from scanning for vulnerabilities, to automating exploits for them. The NSE is particularly useful for reconnaissance, however, it is well worth bearing in mind how extensive the script library is.

Q1. What language are NSE scripts written in?

A1. Lua

Q2. Which category of scripts would be a very bad idea to run in a production environment?

A2. Intrusive



TryHackMe give us attack machine for 1 hr. My 1 hr is completed. So now I'll use my Virtual Machine and will create a attack machine with other ID.

Task 11: NSE Scripts: Working with the NSE

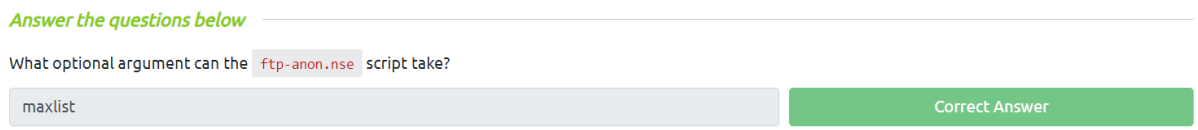
To run a specific script, we would use `--script=<script-name>` , e.g. `--script=http-fileupload-exploiter`.

Multiple scripts can be run simultaneously in this fashion by separating them by a comma. For example: `--script=smb-enum-users,smb-enum-shares`.

Some scripts require arguments (for example, credentials, if they're exploiting an authenticated vulnerability). These can be given with the `--script-args` Nmap switch. An example of this would be with the `http-put` script (used to upload files using the PUT method). This takes two arguments: the URL to upload the file to, and the file's location on disk.

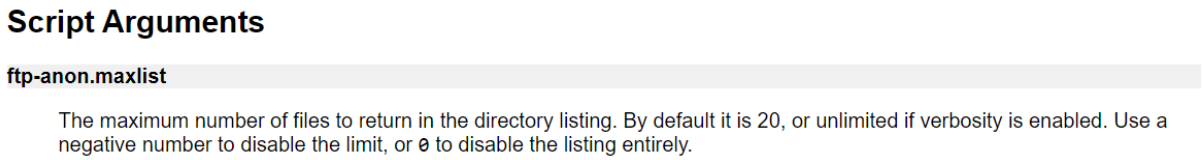
Q1. What optional argument can the ftp-anon.nse script take?

A1. Maxlist



We go to the website mentioned in the task. From there we go to another website using the URL: https://nmap.org/nsedoc/scripts/

Now we will scroll till we find ftp-anon and click on it. And there we see the optional argument ftp-anon takes.



Task 12: NSE Scripts: Searching for Scripts

Now we will get to know how to find scripts. And there are 2 ways to do

The first is the page on the Nmap website (mentioned in the previous task) which contains a list of all official scripts. The second is the local storage on your attacking machine. Nmap stores its scripts on Linux at `/usr/share/nmap/scripts`. All of the NSE scripts are stored in this directory by default -- this is where Nmap looks for scripts when you specify them.

Q1. 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?

A1. smb-os-discovery.nse

```
└─$ ls -l /usr/share/nmap/scripts | grep "smb"
-rw-r--r-- 1 root root  3753 Jan  9  2023 smb2-capabilities.nse
-rw-r--r-- 1 root root  2689 Jan  9  2023 smb2-security-mode.nse
-rw-r--r-- 1 root root  1408 Jan  9  2023 smb2-time.nse
-rw-r--r-- 1 root root  5269 Jan  9  2023 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root 45061 Jan  9  2023 smb-brute.nse
-rw-r--r-- 1 root root  5289 Jan  9  2023 smb-double-pulsar-backdoor.nse
-rw-r--r-- 1 root root  4840 Jan  9  2023 smb-enum-domains.nse
-rw-r--r-- 1 root root  5971 Jan  9  2023 smb-enum-groups.nse
-rw-r--r-- 1 root root  8043 Jan  9  2023 smb-enum-processes.nse
-rw-r--r-- 1 root root 27274 Jan  9  2023 smb-enum-services.nse
-rw-r--r-- 1 root root 12017 Jan  9  2023 smb-enum-sessions.nse
-rw-r--r-- 1 root root  6923 Jan  9  2023 smb-enum-shares.nse
-rw-r--r-- 1 root root 12527 Jan  9  2023 smb-enum-users.nse
-rw-r--r-- 1 root root  1706 Jan  9  2023 smb-flood.nse
-rw-r--r-- 1 root root  7471 Jan  9  2023 smb-ls.nse
-rw-r--r-- 1 root root  8758 Jan  9  2023 smb-mbenum.nse
-rw-r--r-- 1 root root  8220 Jan  9  2023 smb-os-discovery.nse
```

I used grep command to find the specific word I entered. So using grep and scrolling through the list I find smb-os-discovery.nse.

Q2. Read through this script. What does it depend on?

A2. smb-brute

```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/nmap/scripts/smb-os-discovery.nse | grep "dependencies"
dependencies = {"smb-brute"}
```

I opened the file using cat command and using grep I got the dependencies i.e., 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 — Correct Answer

Read through this script. What does it depend on?

smb-brute — Correct Answer — Hint

Task 13: Firewall Evasion

The following switches are useful for firewall evasion:

- -Pn, which tells Nmap to not bother pinging the host before scanning it.
- -f:- Used to fragment the packets (i.e. split them into smaller pieces) making it less likely that the packets will be detected by a firewall or IDS.
- An alternative to -f, but providing more control over the size of the packets: --mtu <number>, accepts a maximum transmission unit size to use for the packets sent. This *must* be a multiple of 8.
- --scan-delay <time>ms:- used to add a delay between packets sent. This is very useful if the network is unstable, but also for evading any time-based firewall/IDS triggers which may be in place.
- --badsum:- this is used to generate in invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond automatically, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence of a firewall/IDS.

Q1. Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

A1. ICMP

Q2. **[Research]** Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

A2. --data-length

I used the URL in the task to go to website and it took me to bypass firewall page. There I go the answer.

`--data-length <number>` (Append random data to sent packets)

Normally Nmap sends minimalist packets containing only a header.

Task 14: Practical

Q1. Does the target (10.10.253.104)respond to ICMP (ping) requests (Y/N)?

A1. N

Q2. Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

A2. 999

```
└─$ sudo nmap -vv -sX -PN -p 0-999 10.10.253.104
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 07:47 EDT
Initiating Parallel DNS resolution of 1 host. at 07:47
Completed Parallel DNS resolution of 1 host. at 07:47, 0.01s elapsed
Initiating XMAS Scan at 07:47
Scanning 10.10.253.104 [1000 ports]
XMAS Scan Timing: About 15.05% done; ETC: 07:50 (0:02:55 remaining)
XMAS Scan Timing: About 30.10% done; ETC: 07:50 (0:02:22 remaining)
XMAS Scan Timing: About 45.10% done; ETC: 07:50 (0:01:51 remaining)
XMAS Scan Timing: About 60.05% done; ETC: 07:50 (0:01:20 remaining)
XMAS Scan Timing: About 75.05% done; ETC: 07:50 (0:00:50 remaining)
Completed XMAS Scan at 07:50, 201.38s elapsed (1000 total ports)
Nmap scan report for 10.10.253.104
Host is up, received user-set.
Scanned at 2023-09-04 07:47:11 EDT for 201s
All 1000 scanned ports on 10.10.253.104 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
```

Q3. 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!

A3. no response

Q4. Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

A4. 5

Q5. Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

A5. Y

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=ftp-anon.nse 10.10.253.161 -p 21 -vv -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 08:19 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:19
Completed NSE at 08:19, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 08:19
Completed Parallel DNS resolution of 1 host. at 08:19, 0.00s elapsed
Initiating SYN Stealth Scan at 08:19
Scanning 10.10.253.161 [1 port]
Completed SYN Stealth Scan at 08:19, 2.05s elapsed (1 total ports)
NSE: Script scanning 10.10.253.161.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:19
Completed NSE at 08:19, 0.00s elapsed
Nmap scan report for 10.10.253.161
Host is up, received user-set.
Scanned at 2023-09-04 08:19:41 EDT for 2s

PORT   STATE    SERVICE REASON
21/tcp filtered ftp     no-response

NSE: Script Post-scanning.
```

Yes, We can login on port 21.

Answer the questions below

Does the target (`MACHINE_IP`)respond to ICMP (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.

No answer needed — Question Done

Deploy the `ftp-anon` script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

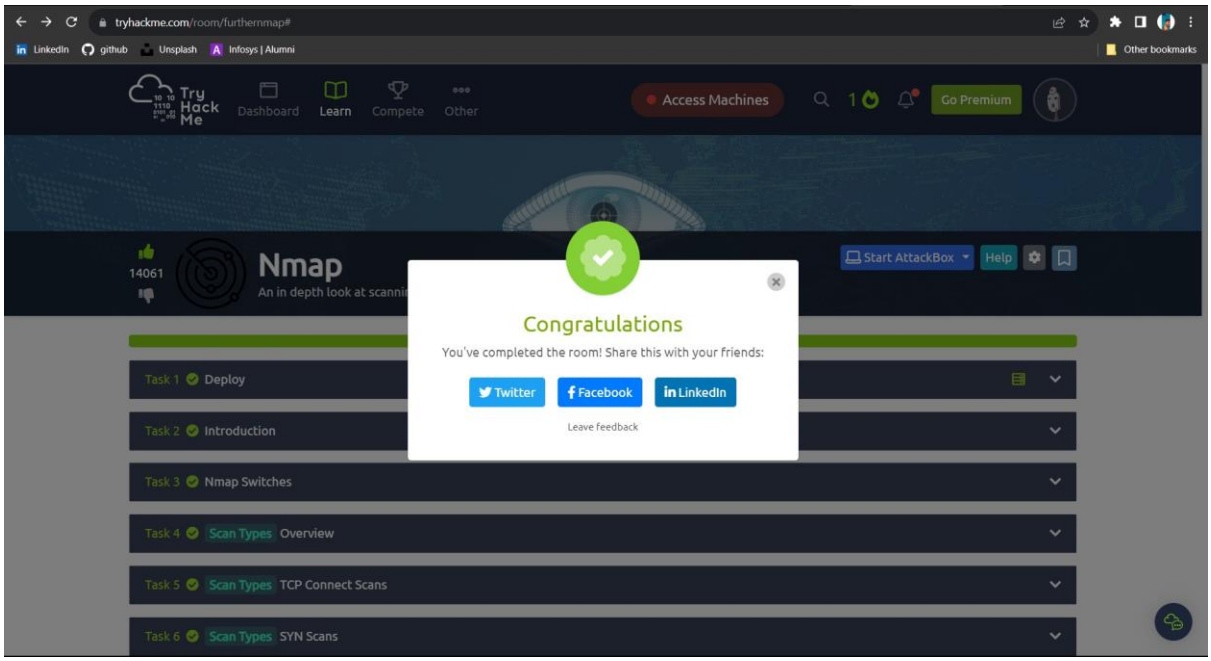
Y — Correct Answer

Task 15: Conclusion

Answer the questions below

Read the conclusion.

No answer needed — Correct Answer



The Room is completed

-Sadiq Sonalkar