Task 3: NMap THM Room Writeup

Profile: https://tryhackme.com/p/anusreebabu.2401

Task 2: Introduction

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

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

No answer needed

Task 5: TCP Connect Scans

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

Task 6: SYN scans

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: UDP scans

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 8: NULL, FIN and XMAS

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: ICMP network scanning

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

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: Working with the NSE

Answer the questions below

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

maxlist ✓ Correct Answer

Task 12: Searching for Scripts

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

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

Task 14: Practical

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

```
root@ip-10-10-203-140:~# ping 10.10.207.221
PING 10.10.207.221 (10.10.207.221) 56(84) bytes of data.
```

Answer: N

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

```
root@ip-10-10-203-140:~# nmap 10.10.207.221 -sX -p 0-998
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-18 17:16 GMT
Nmap scan report for 10.10.207.221
Host is up (0.000054s latency).
All 999 scanned ports on 10.10.207.221 are open|filtered
MAC Address: 02:B0:14:AE:47:EB (Unknown)
```

Answer: 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!

```
root@ip-10-10-203-140:~# nmap 10.10.207.221 -sX -p 0-998 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-18 17:18 GMT
Initiating ARP Ping Scan at 17:18
Scanning 10.10.207.221 [1 port]
Completed ARP Ping Scan at 17:18, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:18
Completed Parallel DNS resolution of 1 host. at 17:18, 0.00s elapsed
Initiating XMAS Scan at 17:18
Scanning 10.10.207.221 [999 ports]
Completed XMAS Scan at 17:18, 21.09s elapsed (999 total ports)
Nmap scan report for 10.10.207.221
Host is up, received arp-response (0.000057s latency).
All 999 scanned ports on 10.10.207.221 are open|filtered because of 999 no-responses
MAC Address: 02:B0:14:AE:47:EB (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.31 seconds
           Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
```

Answer: No Response

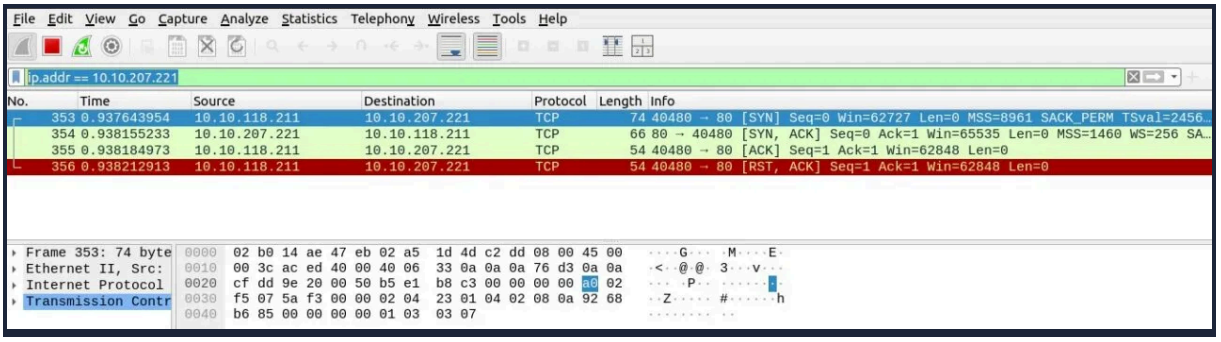
4. Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

```
root@ip-10-10-203-140:~# nmap 10.10.207.221 -sS -p 0-4999 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-18 17:24 GMT
Initiating ARP Ping Scan at 17:24
Scanning 10.10.207.221 [1 port]
Completed ARP Ping Scan at 17:24, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:24
Completed Parallel DNS resolution of 1 host. at 17:24, 0.00s elapsed
Initiating SYN Stealth Scan at 17:24
Scanning 10.10.207.221 [5000 ports]
Discovered open port 135/tcp on 10.10.207.221
Discovered open port 53/tcp on 10.10.207.221
Discovered open port 3389/tcp on 10.10.207.221
Discovered open port 21/tcp on 10.10.207.221
Discovered open port 80/tcp on 10.10.207.221
Completed SYN Stealth Scan at 17:25, 30.72s elapsed (5000 total ports)
Nmap scan report for 10.10.207.221
Host is up, received arp-response (0.00053s latency).
Scanned at 2025-01-18 17:24:31 GMT for 31s
Not shown: 4995 filtered ports
Reason: 4995 no-responses
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 128
53/tcp   open  domain        syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
MAC Address: 02:B0:14:AE:47:EB (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 30.92 seconds
           Raw packets sent: 15015 (660.644KB) | Rcvd: 30 (1.304KB)
```

Answer: 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)



Answer: Y