Furthernmap Tryhackme

In this task, I performed active network enumeration on the target machine using Nmap to identify open ports, running services, and potential firewall rules. The process began with an Xmas scan to detect filtered or potentially open ports, followed by a targeted TCP SYN scan over a wider range to confirm which services were accessible. Once open ports were identified, further Nmap service/version detection was conducted to gather detailed information for the next stage of exploitation.

Task 1: Deploy

Deploy the target virtual machine, no additional configuration is required once it is running.

Task 2: Introduction

1. What networking constructs are used to direct traffic to the right application on a server ?
   ans: Ports
2. How many of these are available on any network-enabled computer?
   ans: 65535
3. How many of these are considered “well-known” ? (These are the “standard” numbers mentioned in the task)
   ans: 1024

Task 3: Nmap Switche

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

ans: -sS

2. Which switch would you use for a “UDP scan”?

ans: -sU

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

ans: -O

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

ans: -sV

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

ans: -v

6. Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two ?

ans: -vv

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

ans: -oA

8. What switch would you use to save the nmap results in a “normal” format ?

ans: -oN

9. A very useful output format: how would you save results in a “grepable” format?

ans: -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.

10. How would you activate this setting ?

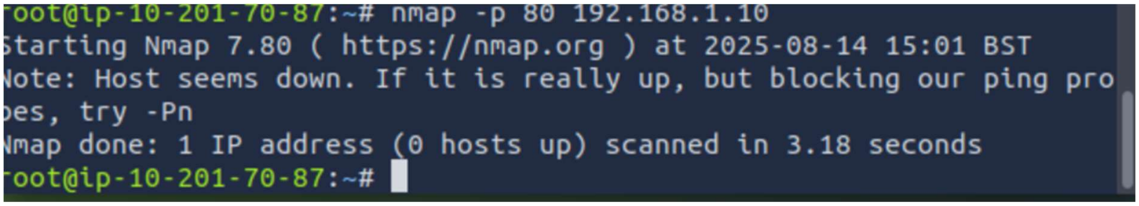
ans: -A

11. How would you set the timing template to level 5 ?

ans: -T5

12. How would you tell nmap to only scan port 80 ?

ans: -p 80



```
root@ip-10-201-70-87:~# nmap -p 80 192.168.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-14 15:01 BST
Note: Host seems down. If it is really up, but blocking our ping pro
bes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
root@ip-10-201-70-87:~# 
```

13. How would you tell nmap to scan ports 1000–1500 ?

ans: -p 1000-1500

14. How would you tell nmap to scan all ports ?

ans: -P15. How would you activate a script from the nmap scripting library (lots more on this later!) ?

ans: --script

16. How would you activate all of the scripts in the “vuln” category ?

ans: --script=vuln

Task 4 – Scan Types Overview

learned about Nmap’s main scan types (TCP Connect, SYN, and UDP) and some less common ones (Null, FIN, and Xmas). Each scan type works differently, and some are useful for stealth or firewall evasion.

Task 5: TCP Connect Scans

1. Which RFC defines the appropriate behavior for the TCP protocol?

ans: RFC 9293

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

ans: RST

Task 6: SYN Scans

1. There are two other names for a SYN scan. What are they?

ans: Half-open, Stealth

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

ans: N

Task 7: UDP Scans

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

ans: open|filtered

2. 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?

ans: ICMP

Task 8: NULL, FIN and Xmas Scans

1. Which of the three scan types uses the URG flag?

ans: Xmas

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

ans: Firewall evasion

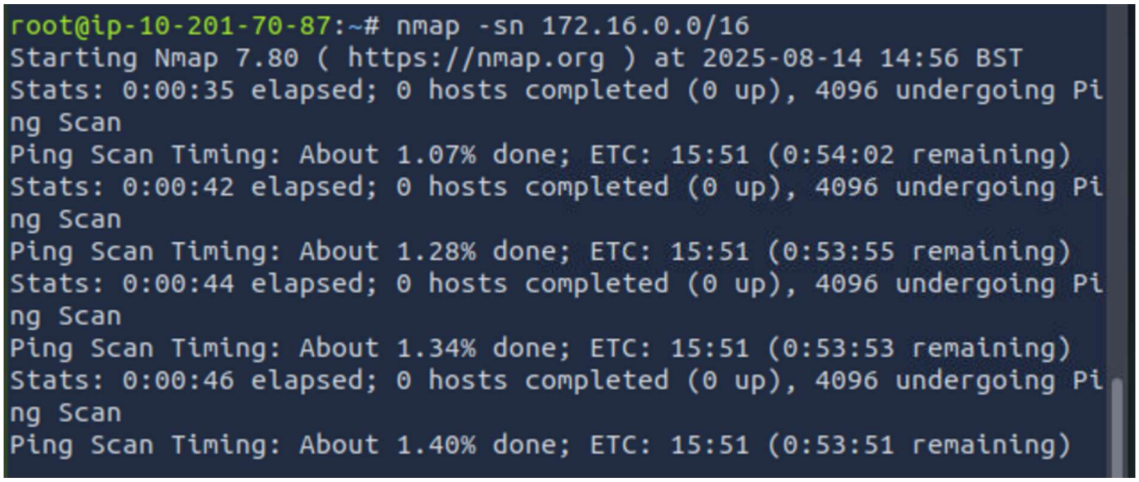
3. Which common OS may respond to a NULL, FIN, or Xmas scan with a RST for every port?

ans: Microsoft Windows

Task 9: ICMP Network Scanning

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

ans: nmap -sn 172.16.0.0/16



```
root@ip-10-201-70-87:~# nmap -sn 172.16.0.0/16
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-14 14:56 BST
Stats: 0:00:35 elapsed; 0 hosts completed (0 up), 4096 undergoing Pi
ng Scan
Ping Scan Timing: About 1.07% done; ETC: 15:51 (0:54:02 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (0 up), 4096 undergoing Pi
ng Scan
Ping Scan Timing: About 1.28% done; ETC: 15:51 (0:53:55 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (0 up), 4096 undergoing Pi
ng Scan
Ping Scan Timing: About 1.34% done; ETC: 15:51 (0:53:53 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (0 up), 4096 undergoing Pi
ng Scan
Ping Scan Timing: About 1.40% done; ETC: 15:51 (0:53:51 remaining)
```

Task 10: NSE Scripts Overview

1. What language are NSE scripts written in?

ans: Lua

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

ans: Intrusive

Task 11: Working with the NSE

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

ans: maxlist

Task 12: Searching for Scripts

1. What is the filename of the script which determines the underlying OS of the SMB server?

ans: smb-os-discovery.nse

2. What does the smb-os-discovery.nse script depend on?

ans: smb-brute

Task 13: Firewall Evasion

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

ans: ICMP

2. Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

ans:--data-length

Task 14: Practical

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

ans: N

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

ans: 999

3. What is the reason for the above result?

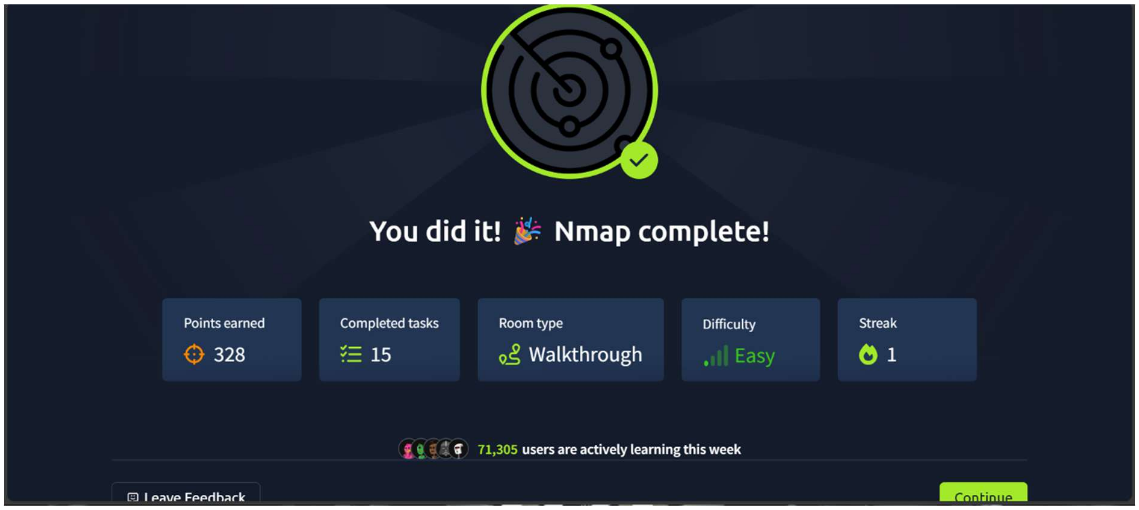
ans: No response
4. Perform a TCP SYN scan on the first 5000 ports of the target — how many ports are shown to be open?
ans: 5

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

ans: Y

Conclusion

The “Further Nmap” room provided hands-on experience with advanced scanning techniques. Each scan type demonstrated its strengths and limitations in detecting services and bypassing filtering mechanisms. Using Xmas, SYN, and UDP scans, along with NSE scripting, allowed the enumeration of TCP and UDP services, detection of OS information, and identification of accessible FTP services. Mastery of these techniques is essential for penetration testing, vulnerability assessment, and network security analysis.



You did it! 🎉 Nmap complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
328	15	Walkthrough	Easy	1

71,305 users are actively learning this week