Nmap Room TryHackMe

Nmap is a free tool used to scan networks and find connected devices, open ports, and possible security issues. It helps cybersecurity professionals test and troubleshoot networks. Nmap is fast, flexible, and supports many types of scans.

Task1: Deploy

Answer the questions below		
Deploy the attached VM		
No answer needed	✓ Correct Ans	wer
Task 2: Introduction Answer the questions below		
What networking constructs are used to direct traffic to the right application on a server?		
Ports	✓ Correct Ansv	wer
How many of these are available on any network-enabled computer?		
65535	✓ Correct Answ	wer
[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

- 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

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

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.

- 15. 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 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	

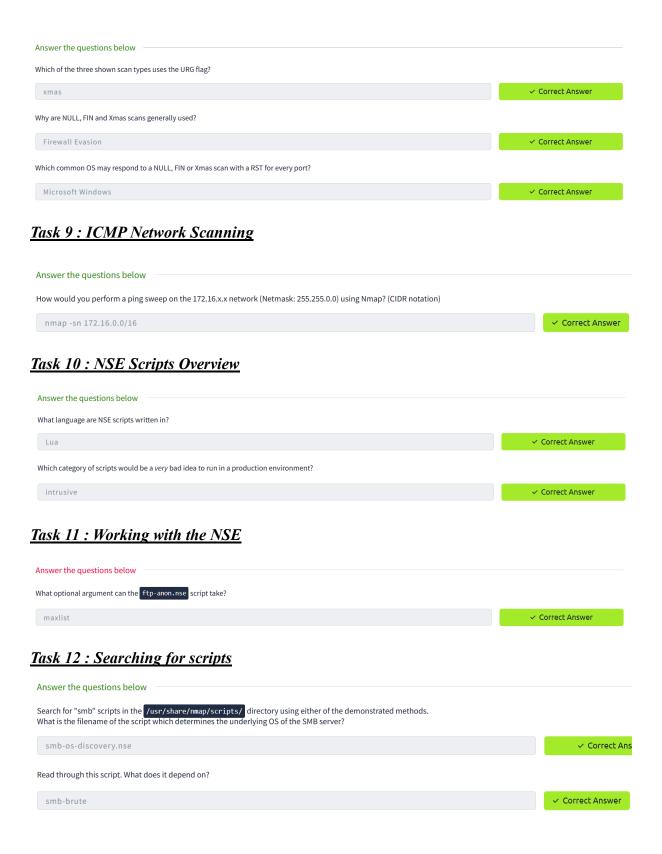
Task 6: SYN Scans

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

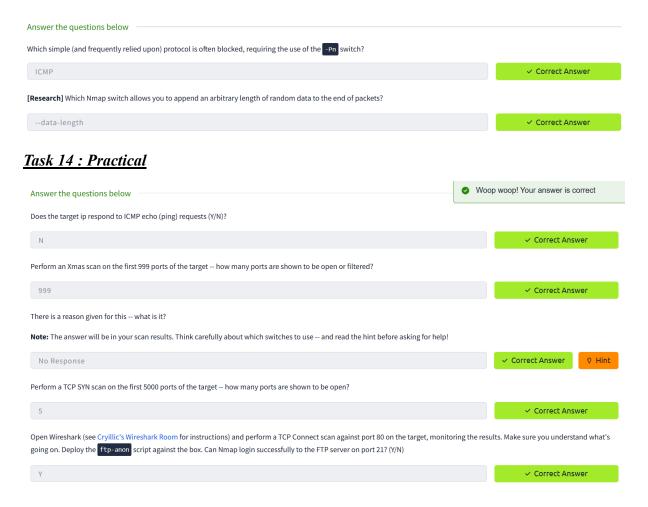
Task 7: UDP Scans

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



Task 13: Firewall Evasion



Task 15: Conclusion

