

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 Answer

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

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

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

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

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

Answer the questions below

✓ Woop woop! Your answer is correct

Does the target ip respond to ICMP echo (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 [Crylllic'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

✓ Correct Answer

Task 15 : Conclusion



You did it! 🎉 Nmap complete!

Points earned

🏆 328

Completed tasks

📋 15

Room type


👤 Walkthrough

Difficulty

📶 Easy

Streak

🔥 1



76,126 users are actively learning this week