


Nmap -TryHackMe

Task 1 Deploy

Press the green button to deploy the machine!

Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.

 Start Machine

If you are using the TryHackMe AttackBox then you will need to deploy this separately.

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

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

Nmap -TryHackMe

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?

Correct Answer

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

Correct Answer

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

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?

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?

Correct Answer

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

How would you tell nmap to only scan port 80?

Correct Answer

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

Correct Answer

A very useful option that should not be ignored:

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

Correct Answer



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

Correct Answer

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

Correct Answer

Hint

Task 4  Scan Types Overview 

Answer the questions below

Read the Scan Types Introduction.

Correct Answer

Task 5  Scan Types TCP Connect Scans 

Nmap -TryHackMe

Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

Correct Answer

Hint

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

Correct Answer

Task 6 Scan Types SYN Scans

Answer the questions below

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

Correct Answer

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

Correct Answer

Task 7 Scan Types UDP Scans

Answer the questions below

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

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?

Correct Answer

Task 8 Scan Types NULL, FIN and Xmas

Answer the questions below

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

Correct Answer

Why are NULL, FIN and Xmas scans generally used?

Correct Answer

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

Correct Answer

Task 9 Scan Types 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)

Correct Answer

Hint

Task 10 NSE Scripts Overview

Nmap -TryHackMe

Answer the questions below

What language are NSE scripts written in?

Correct Answer

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

Correct Answer

Task 11 NSE Scripts Working with the NSE

Answer the questions below

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

Correct Answer

Task 12 NSE Scripts 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?

Correct Answer

Read through this script. What does it depend on?

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?

Correct Answer

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

Correct Answer

Task 14 Practical

Answer the questions below

Does the target (`MACHINE_IP`) respond to ICMP (ping) requests (Y/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?

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!

Correct Answer

 Hint

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

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.

Correct Answer

Nmap -TryHackMe

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 have now completed the Further Nmap room -- hopefully you enjoyed it, and learnt something new!

There are lots of great resources for learning more about Nmap on your own. Front and center are Nmap's own (highly extensive) [docs](#) which have already been mentioned several times throughout the room. These are a superb resource, so, whilst reading through them line-by-line and learning them by rote is entirely unnecessary, it would be highly advisable to use them as a point of reference, should you need it.

Answer the questions below

Read the conclusion.

No answer needed

Correct Answer

