articles by cisca

Follow

TryHackMe: Nmap Walkthrough

Francisca

May 18, 2022 · 5 min read

In this article, I'm going to write a walkthrough of the Nmap room on TryHackMe

Enjoy!!!

Task 1: Deploy

Deploy the attached VM

Task 2: Introduction

- What networking constructs are used to direct traffic to the right application on a server?

Answer: Ports

- How many of these are available on any network-enabled computer?

Answer: 65535

- [Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

Answer: 1024

Task 3: Nmap Switches

- What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

Answer: -sS

- Which switch would you use for a "UDP scan"?

Answer: -sU

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

Answer: -O

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

Answer: -sV

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

Answer: -v

- 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)

Answer: -vv

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?

Answer: -oA

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

Answer: -oN

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

Answer: -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.

- How would you activate this setting?

Answer: -A

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?

Answer: -T5

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

- How would you tell nmap to only scan port 80?

Answer: -p 80

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

Answer: -p 1000-1500

A very useful option that should not be ignored:

- How would you tell nmap to scan all ports?

Answer: -p-

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

Answer: --script

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

Answer: --script=vuln

Task 4: `Scan Types` Overview

Read the Scan Types Introduction.

Task 5: `Scan Types` TCP Connect Scans

- Which RFC defines the appropriate behaviour for the TCP protocol?

Answer: RFC 793

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

Answer: RST

Task 6: `Scan Types` SYN Scans

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

Answer: half-open, stealth

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

Answer: N

Task 7: `Scan Types` UDP Scans

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

Answer: open|filtered

- 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?

Answer: ICMP

Task 8: `Scan Types` NULL, FIN, and Xmas

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

Answer: xmas

- Why are NULL, FIN and Xmas scans generally used?

Answer: Firewall Evasion

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

Answer: Microsoft Windows

Task 9: `Scan Types` ICMP Network Scanning

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

Answer: nmap -sn 172.16.0.0/16

Task 10: `NSE Scripts` Overview

- What language are NSE scripts written in?

Answer: Lua

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

Answer: intrusive

Task 11: `NSE Scripts` Working with the NSE

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

Answer: maxlist

Task 12: `NSE Scripts` Searching for Scripts

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?

Answer: smb-os-discovery.nse

- Read through this script. What does it depend on?

Answer: smb-brute

Task 13: Firewall Evasion

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

Answer: ICMP

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

Answer: --data-length

Task 14: Practical

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

Answer: N

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

Answer: 999

- 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!

Answer: No response

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

Answer: 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.

No answer needed

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

Answer: Y

Task 15: Conclusion

Read the Conclusion

I hope you enjoyed the Nmap room and also learned a lot while going through it.

#cybersecurity CyberSec Tutorial

ARTICLE SERIES
TryHackMe

1

TryHackMe: Nmap Walkthrough

In this article, I'm going to write a walkthrough of the Nmap room on TryHackMe Enjoy!!! Task 1: Dep...