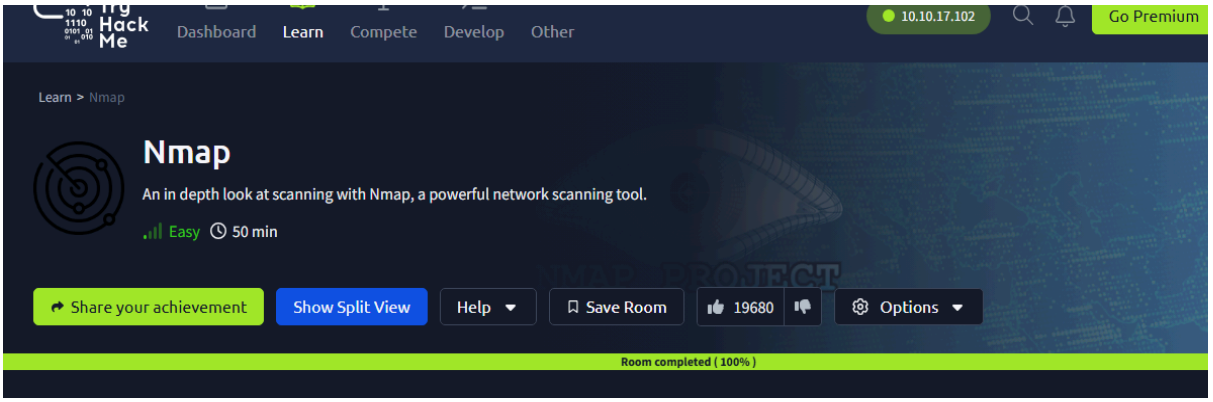
TryHackMe Writeup - Further Nmap

Task 1 – Deploy



To begin this room, we first launch the TryHackMe room and start the attack box.

Introduction to Nmap:
Nmap, which stands for Network Mapper, is a powerful and free tool used for scanning and discovering devices on a network. It helps security professionals and network administrators find out what hosts and services are running by identifying open ports and gathering information about networked systems.

The very first task in the room is pretty straightforward: simply deploy the target machine. Once it's up and running, just mark the task as complete to move on.

Task 2 -- Introduction

It gives a quick overview of Nmap, its main uses, and offers clear hints for the questions by explaining port details and what Nmap does.

Task 3 – Nmap Switches

Nmap uses switches (or options) like -sS, -sU, -A, and -T5 to customize how scans are performed, controlling aspects like scan type, intensity, and additional information gathered.

Task 4 – Scan Types Overview:

Covers various scan types such as SYN, TCP Connect, UDP, NULL, FIN, and XMAS, explaining their differences and uses.

Task 5 – TCP Connect Scans:

Describes the basic TCP scan that completes the full connection according to RFC standards.

Task 6 – SYN Scans:

Explains SYN scans as stealthy, faster, and more efficient because they don't complete the full TCP handshake.

Task 7 – UDP Scans:

Covers how Nmap performs UDP scans, interpreting results, and how these scans can be detected.

Task 8 – NULL, FIN, and Xmas Scans:

Explains these stealthy scan types used mainly to evade firewalls and intrusion detection systems.

Task 9 – ICMP Network Scanning:

Demonstrates how to conduct ping sweeps using Nmap to discover live hosts on a network.

Task 10 – NSE Scripts Overview:

Introduces the Nmap Scripting Engine (NSE) and its capabilities for automating tasks during scans.

Task 11 – NSE Scripts (Working with NSE):

Walkthrough using an example script (`ftp-anon.nse`) including optional arguments.

Task 12 – NSE Scripts (Searching):

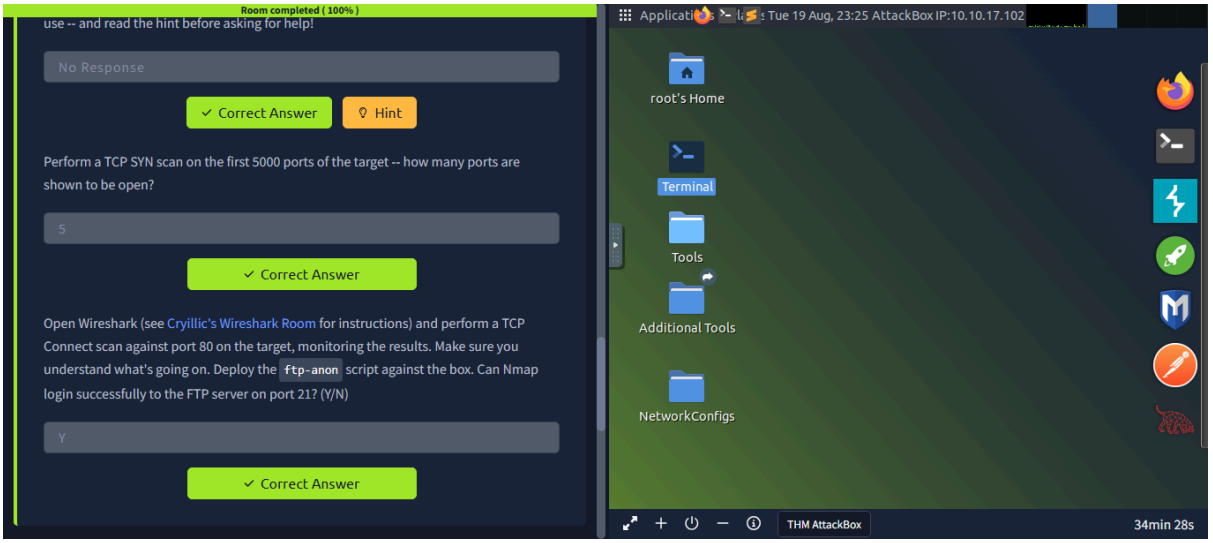
Shows how to search for NSE scripts and understand their dependencies.

Task 13 – Firewall Evasion:

Details various techniques and Nmap switches to evade firewalls during scanning.

Task 14 – Practical:

Summarizes the practical scanning exercises performed and the key findings from the room.


Room completed (100%)
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 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. Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)
Y
Correct Answer
Tue 19 Aug, 23:25 AttackBox IP:10.10.17.102
root's Home
Terminal
Tools
Additional Tools
NetworkConfigs
THM AttackBox
34min 28s