Chapter 2: MISSION APLHA – Reconnaissance 2 - System Analysis

Introduction:

Introduction:

In Chapter 2, you have identified a rogue device on the corporate network and are tasked with conducting an Nmap scan and writing a minimum 200-word report of your findings. The mission involves using TryHackMe rooms, launching the room and the attack box, scanning the system, and writing a comprehensive report.

Mission Instructions:

1. **Identifying the Rogue Device:**
   - Locate the rogue device on the corporate network. (Pick a THM Room from the list below)
2. **Conducting the Nmap Scan:**
   - Start the attack box provided in the TryHackMe environment.
   - Perform a thorough Nmap scan on the target system to identify possible operating system, active services, open ports and vulnerabilities.
3. **Documenting Findings:**
   - Write a report with a minimum of 200 words detailing the findings from the Nmap scan of the rogue device.
   - Include information about the discovered open ports, services, possible operating system, and any vulnerabilities identified.
4. **Exfiltrating Scan Data:**
   - Take screenshots of the Nmap scan results.
   - Use the Optical Character Recognition (OCR) tool on CyberChef to convert the screenshots into text format.

Key Points:

- **Objective:** Identify the rogue device on the network, conduct a comprehensive Nmap scan, and document the findings.
- **Tools:** Use TryHackMe rooms, Nmap for scanning, and CyberChef for OCR conversion.
- **Deliverable:** A detailed 200-word report

Target List:

Pick one target from the list below to be the rogue device.

https://tryhackme.com/r/room/internal

https://tryhackme.com/r/room/agentsudoctf

https://tryhackme.com/r/room/services

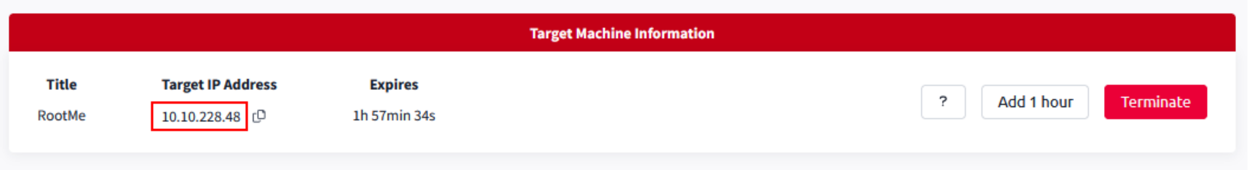
https://tryhackme.com/r/room/rrootme

Resources

Example Nmap Command: nmap -sC -sV 10.10.50.114

The `nmap` command `nmap -sC -sV 10.10.50.114` is used to perform a network scan on the specified IP address (`10.10.50.114`). Here's a breakdown of the command and its components:

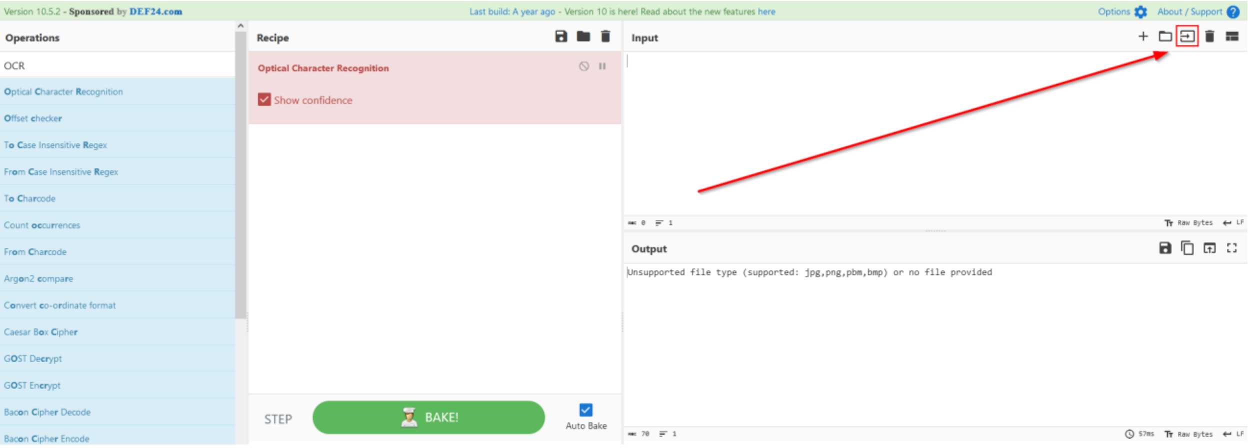
- `nmap`: This is the network scanning tool itself.
- `-sC`: This option tells Nmap to run a set of default scripts against the target. These scripts are part of the Nmap Scripting Engine (NSE) and are used to detect various information such as open ports, service versions, and potential vulnerabilities. The `-sC` flag is equivalent to using `--script=default`.
- `-sV`: This option enables version detection. It tells Nmap to attempt to determine the version of the services running on open ports. This helps in identifying not just that a service is running, but also which specific software and version it is.
- `10.10.50.114`: This is the IP address of the target device that you are scanning. Replace this address with the IP address from the machine you launched.



Target Machine Information

Title	Target IP Address	Expires
RootMe	10.10.228.48	1h 57min 34s

CyberChef OCR Tool: https://cyberchef.org/#recipe=Optical_Character_Recognition(true)



Version 10.5.2 - Sponsored by DEF24.com

Last build: A year ago - Version 10 is here! Read about the new features here

Recipe: Optical Character Recognition

☑ Show confidence

☑ Auto Bake

Output

```
Unsupported file type (supported: jpg,png,pbm,bmp) or no file provided
```