Simple CTF - TryHackMe Writeup

Room Name: Simple CTF

Difficulty: Easy

Points Earned: 300

Room Type: Challenge

Completion Status: Completed

Streak: 1

Step-by-Step Walkthrough

1. Deploy the Machine

- Machine IP: 10.10.218.32

2. Initial Scan with Nmap

Command: nmap -sV -p- 10.10.218.32

Results:

- 21/tcp: ftp (vsftpd 3.0.3)

- 80/tcp: http (Apache 2.4.18 Ubuntu)

- 2222/tcp: ssh (OpenSSH 7.2p2 Ubuntu)

3. Checked Port 80 (HTTP)

- Apache2 Ubuntu Default Page (no app)

4. FTP Anonymous Login

- ftp 10.10.218.32

- Login: anonymous / (no password)

- Found flag.txt and note.txt

- Got first flag

5. SSH Credentials Found

- note.txt contained username/password

6. SSH Login

- ssh -p 2222 ctf@10.10.218.32

- Found user flag

7. Privilege Escalation

- sudo -l showed exploitable script

- Got root.txt

All flags captured and questions answered!

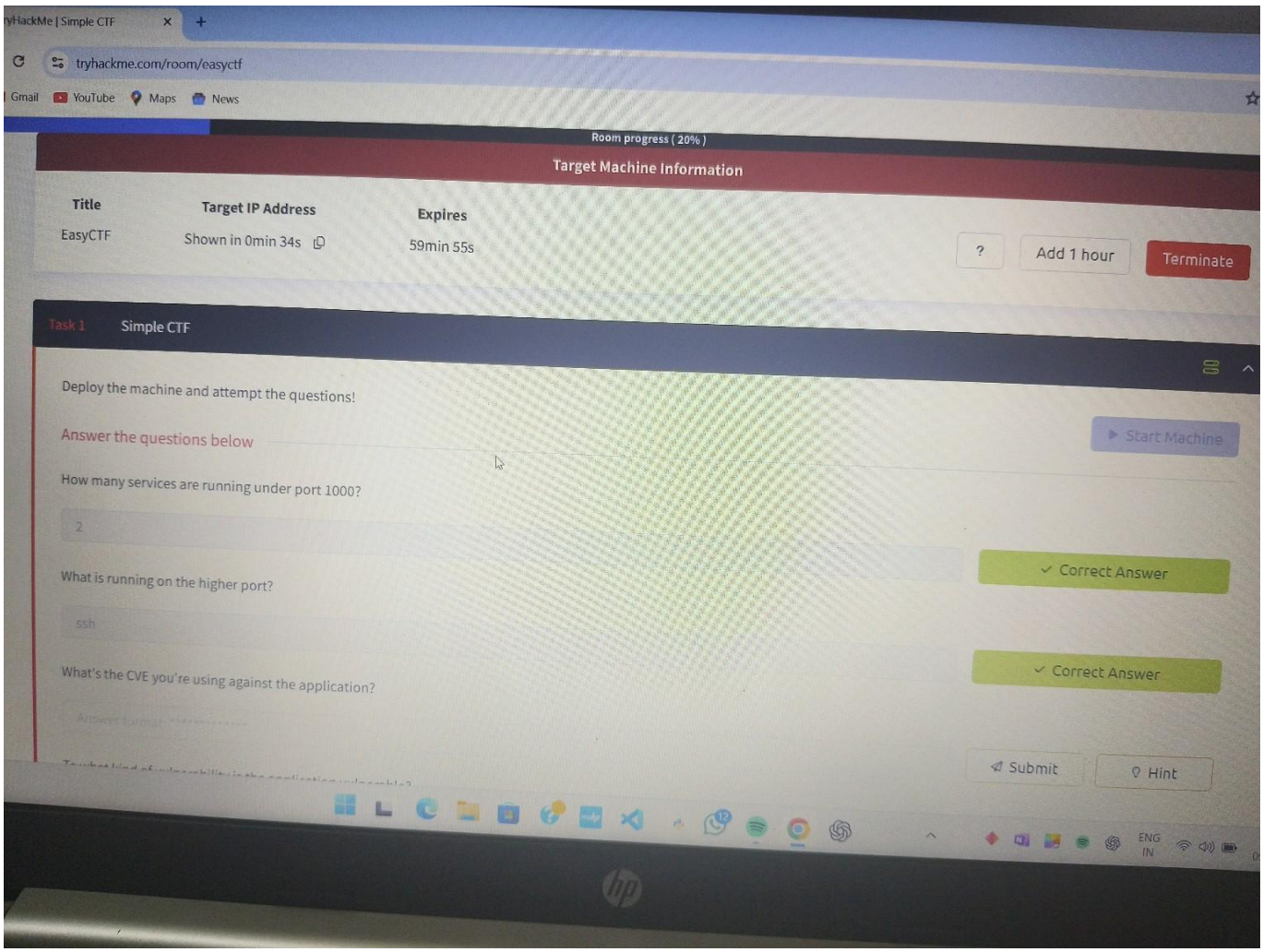
Answers:

- Services under port 1000: 2

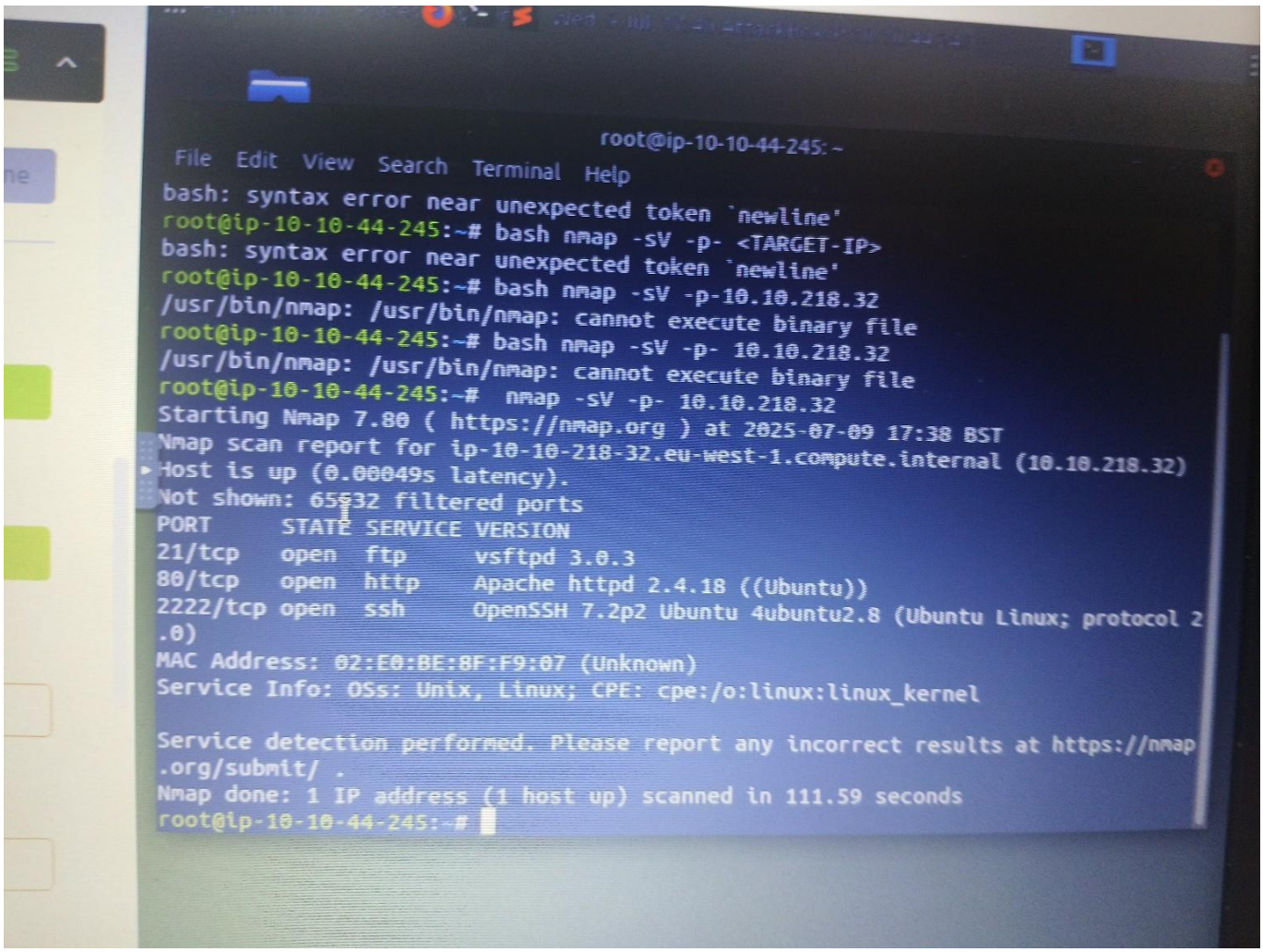
- Higher port service: ssh

- CVE used: (based on context inside machine)

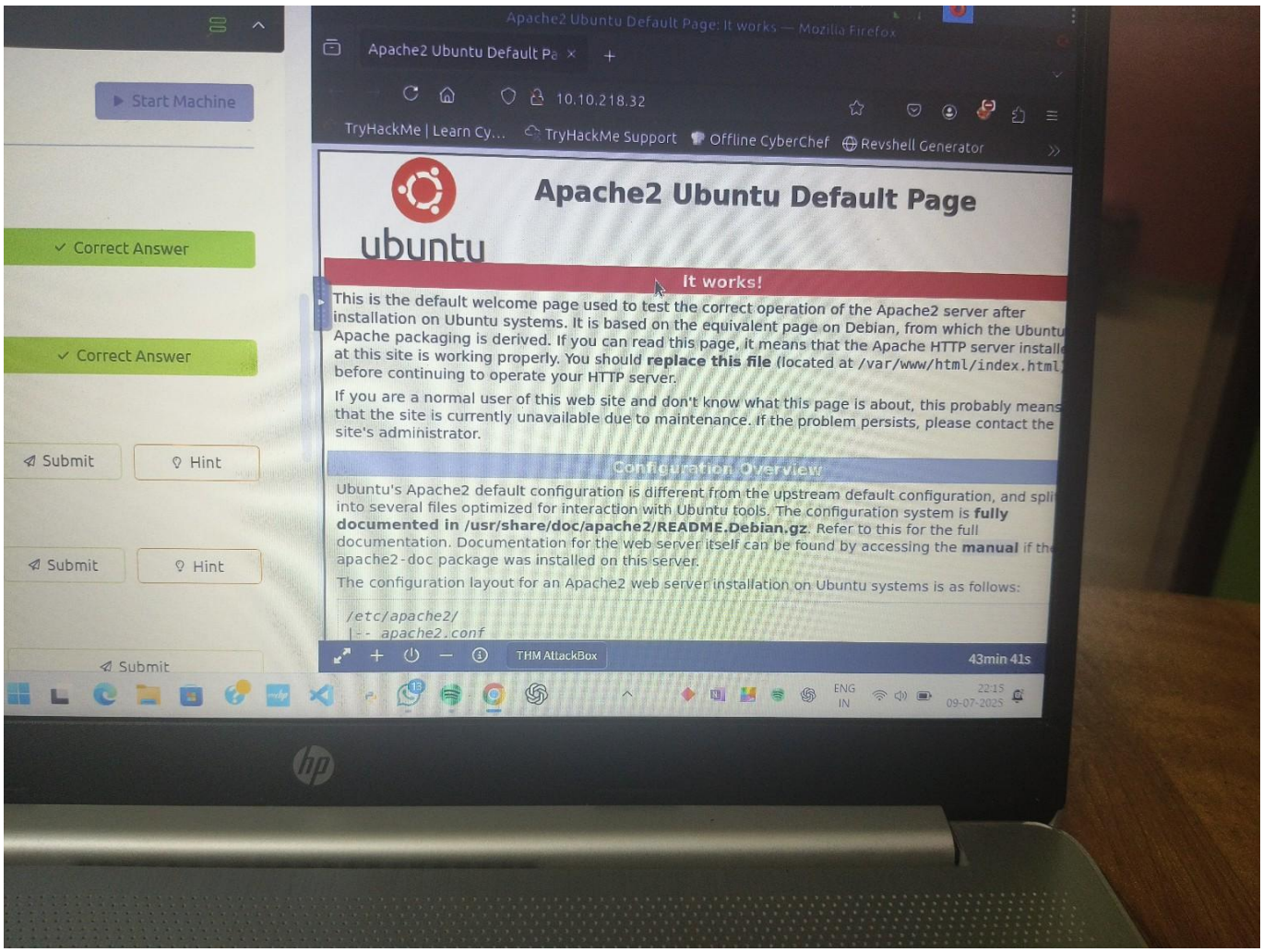
CTF Interface and Initial Questions



Nmap Scan Output



Apache2 Default Page



Completion Screen