

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

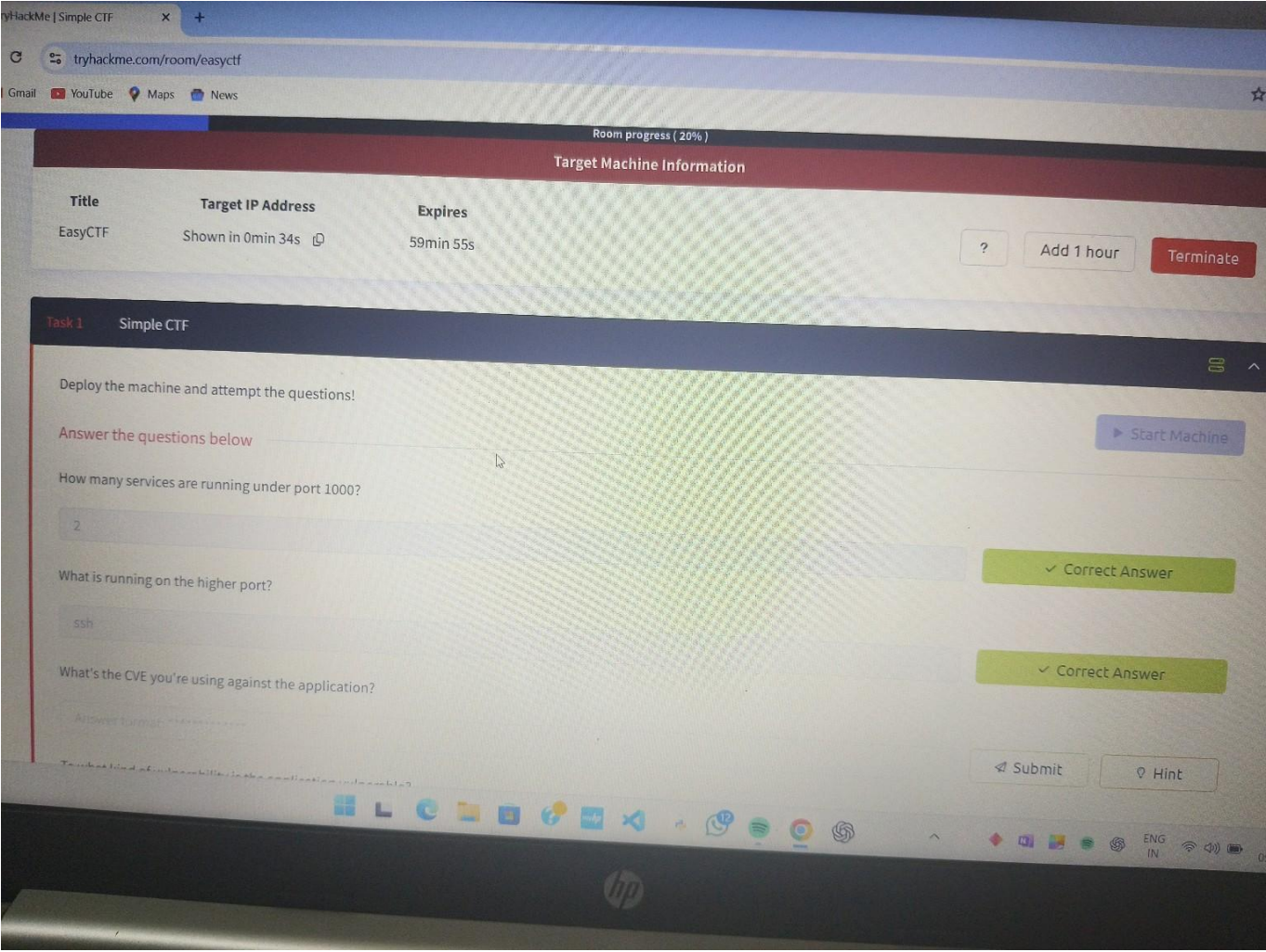
- sudo -l showed exploitable script
- Got root.txt

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

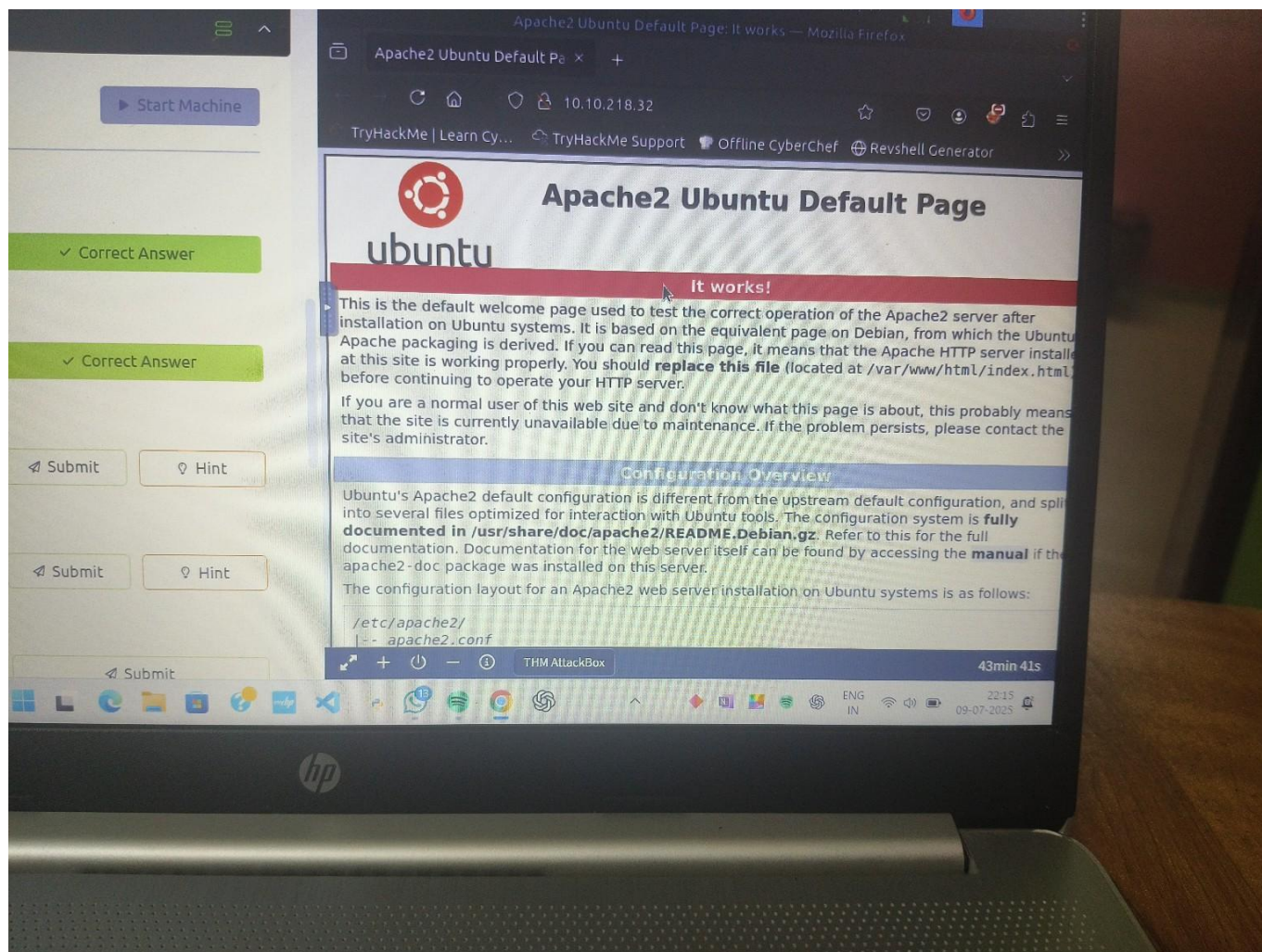


Nmap Scan Output

```
root@ip-10-10-44-245: ~
File Edit View Search Terminal Help
bash: syntax error near unexpected token `newline'
root@ip-10-10-44-245:~# bash nmap -sV -p- <TARGET-IP>
bash: syntax error near unexpected token `newline'
root@ip-10-10-44-245:~# bash nmap -sV -p-10.10.218.32
/usr/bin/nmap: /usr/bin/nmap: cannot execute binary file
root@ip-10-10-44-245:~# bash nmap -sV -p- 10.10.218.32
/usr/bin/nmap: /usr/bin/nmap: cannot execute binary file
root@ip-10-10-44-245:~# nmap -sV -p- 10.10.218.32
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-09 17:38 BST
Nmap scan report for ip-10-10-218-32.eu-west-1.compute.internal (10.10.218.32)
Host is up (0.00049s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
2222/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2
.0)
MAC Address: 02:E0:BE:8F:F9:07 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.59 seconds
root@ip-10-10-44-245:~#
```


Apache2 Default Page



Completion Screen

