TASK1 REPORT

Task: On tryhackme, select a simple CTF room of your choosing, and complete it. Make a writeup and take screenshots of the procedure of completing the CTF, in the form of a MarkDown file or PDF or similar.

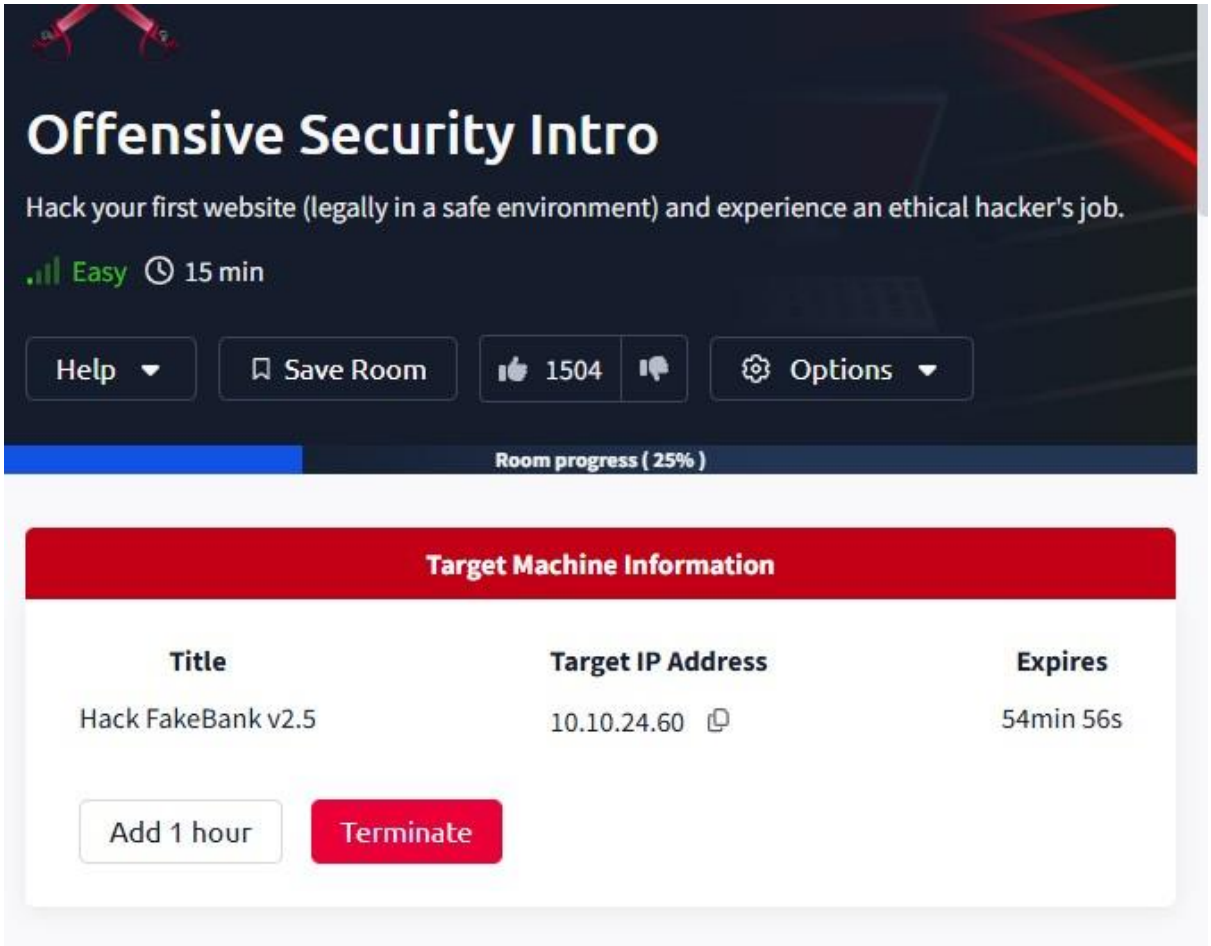
As a complete beginner to ethical hacking and CTF-style exercises, I chose to complete the **Offensive Security Intro** room on TryHackMe. While it is designed primarily as a learning resource rather than a formal CTF room, it includes realistic steps and flag-capturing tasks that simulate a Capture The Flag experience.

This exercise allowed me to get hands-on practice with:

- Network scanning using `nmap`

- Basic web enumeration

- Simulated exploitation of a vulnerable fake banking site



Commands Used:

1. nmap -sC -sV -T4 [IP]

- `-sC`: runs default scripts
- `-sV`: detects service versions
- `-T4`: sets faster timing for quicker scan

`nmap` was used to **scan that IP address** to identify:

- Open ports (e.g., 80 for HTTP)

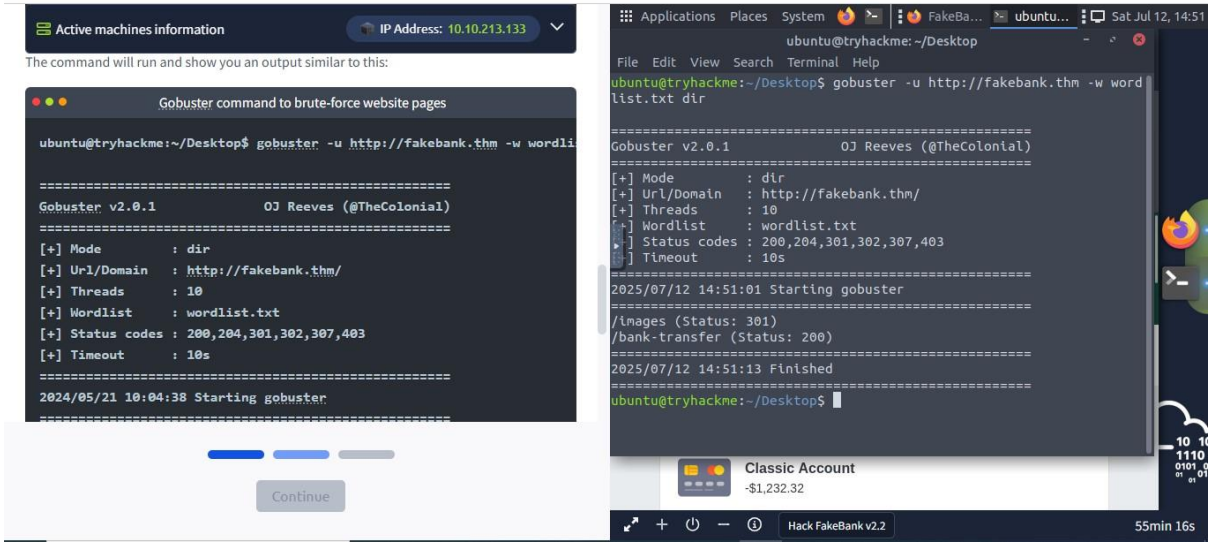
- Running services (e.g., Apache or SSH)

- Service versions that may reveal vulnerabilities

2. gobuster –u http://fakebank.thm –w wordlist.txt dir

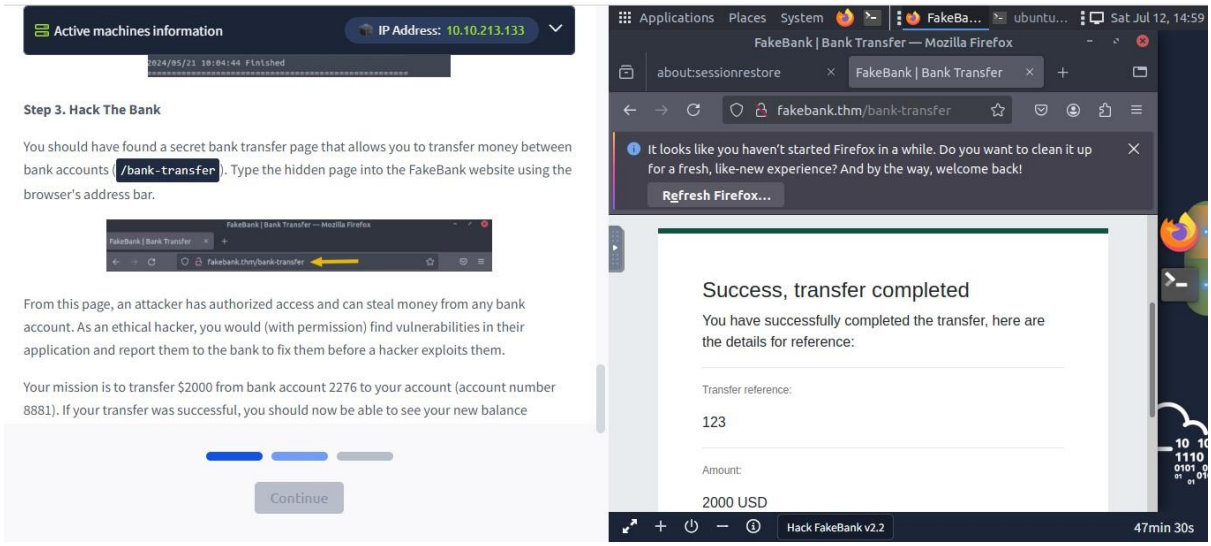
This command is used for **directory brute-forcing** a website — meaning, it tries to discover **hidden folders or files** on a web server that are not linked anywhere.

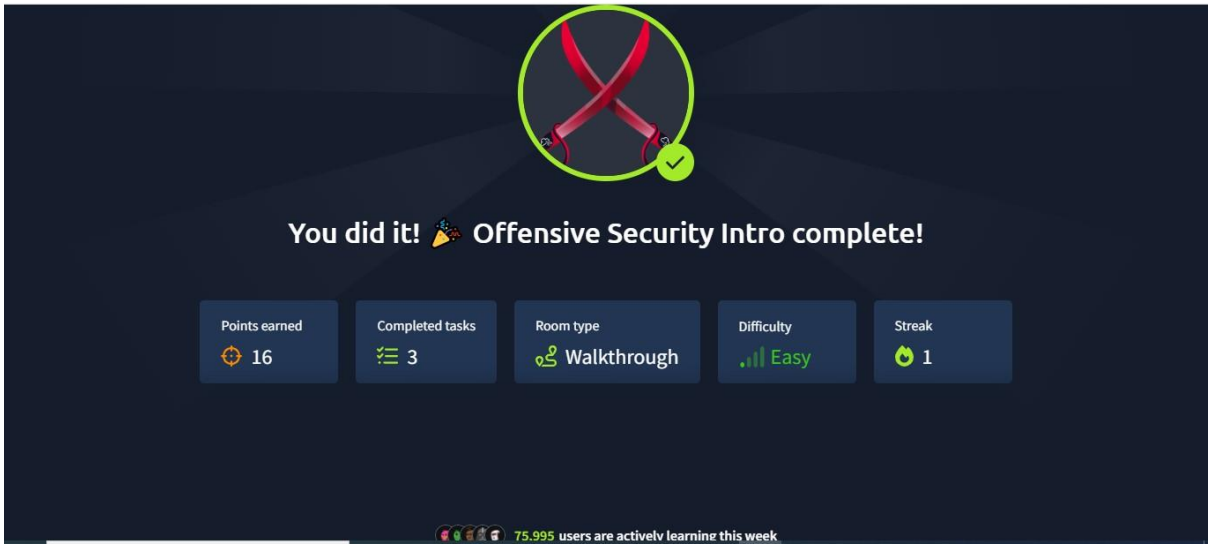
- `gobuster`: the tool used for brute-forcing URLs and directories.
- `dir`: tells Gobuster you're doing **directory enumeration**.
- `-u http://fakebank.thm`: the **target URL**.
- `-w wordlist.txt`: the **wordlist** to use (a list of common folder/file names to try).



Found the hidden page /bank-transfer which allows to transfer money between bank accounts.

Type the hidden page into the fakebank website using the browser's address bar.





This TryHackMe room introduced me to the basics of offensive security through a simulated Capture The Flag (CTF) challenge. Although it was designed for learning rather than competition, it helped me understand and apply core hacking steps, including:

- **Information gathering** using `nmap` and `gobuster`
- **Web enumeration** to find hidden files and login portals