Owasp x mulearn bootcamp Task 1

🛡️ TryHackMe Report: Intro to Offensive Security CTF

Name: Ajay M Nambiar
Date: 02/08/2025
Platform: TryHackMe
Room Name: Intro to Offensive Security
CTF Type: Beginner-friendly, Learning-based

🔍 Objective

The objective of this room was to introduce basic offensive security concepts, specifically directory enumeration, using a fake bank website as the target. The goal was to find hidden URLs and retrieve the flag.

🧰 Tool Used

- dirb – Web directory brute-forcing

🧪 Tasks Completed

Task 1: Access the Initial Page

Visited the fake banking site at:
http://[Target IP]/bank
Discovered a login page with no obvious flaws.

Task 2: Find Hidden URL

Ran dirb against the root directory:

dirb http://[Target IP] /usr/share/wordlists/dirb/common.txt

Discovered a hidden endpoint:
http://[Target IP]/secure

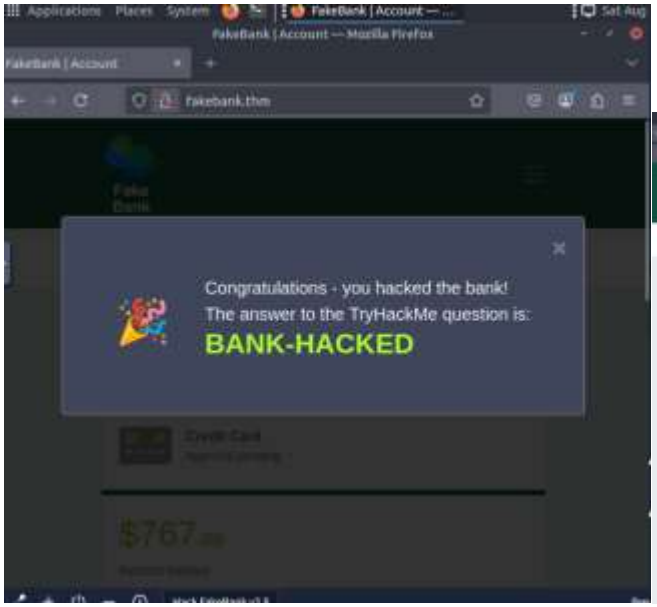
Task 3: Capture the Flag

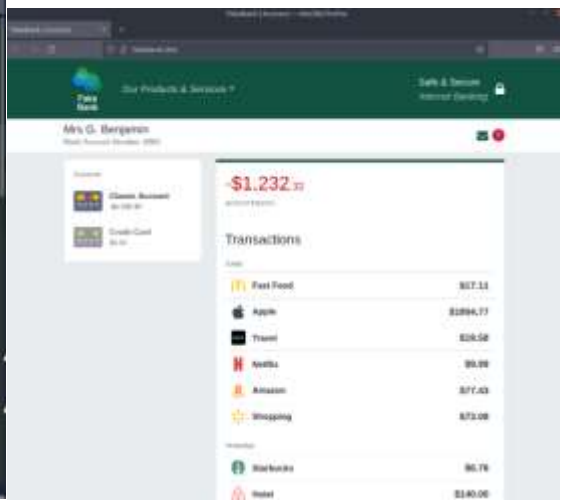
Accessed the /secure directory and followed the in-room instructions.
Successfully completed the steps to "hack" the fake bank account and retrieve the flag.

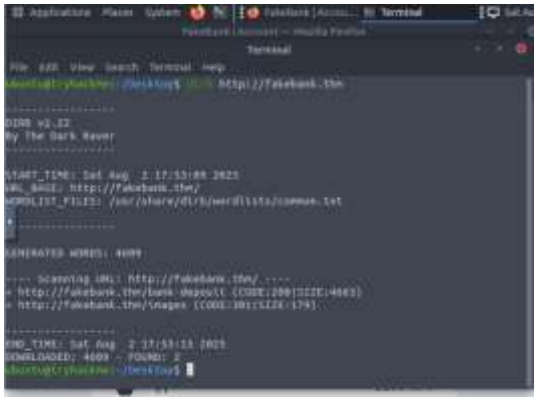
🏁 Flag

Flag captured at the end of the CTF challenge (hidden in /secure section).

📸 Screenshots







Challenge Completion

✅ Conclusion

The challenge showed how basic enumeration using a single tool like dirb can uncover sensitive and hidden paths. Despite being beginner-focused, it mimicked real-world logic flaws that attackers might exploit.
