Cybersecurity Hackathon Week 1 – Write up

Name : Hiran Nath K B
Event : OWASP Kerala × MuLearn Cybersecurity Hackathon

Task : Complete a TryHackMe CTF room

- Task 1: What is Offensive Security?

Offensive Security refers to a proactive approach to cybersecurity where the goal is to identify and exploit vulnerabilities in systems, networks, or applications **before malicious hackers do.** It involves **simulating real-world cyberattacks** to assess the security posture of an organization and uncover weaknesses.
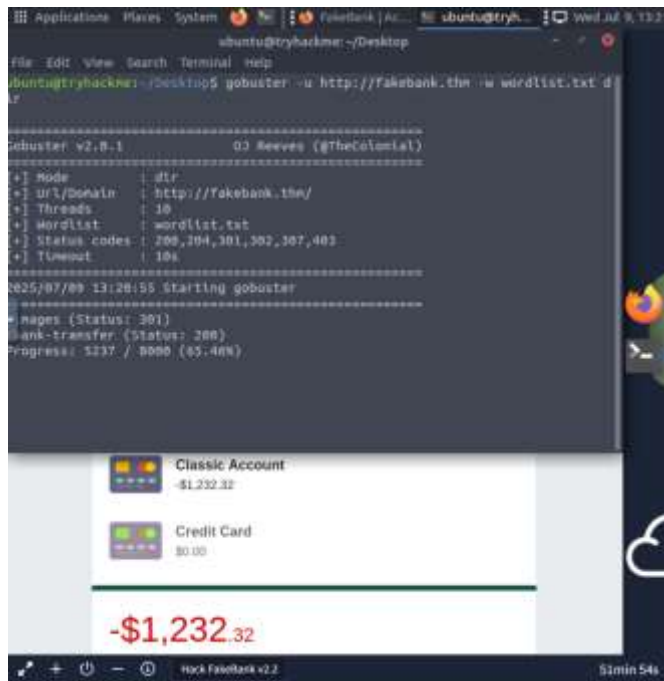
✦ Task 2: Hacking a machine

- TryHackMe uses virtual machines to simulate hacking environments. Here, we have launched the 'FakeBank' virtual machine to begin exploring its vulnerabilities in a safe and legal setup. The system showed a browser window on the right displaying FakeBank's customer dashboard.
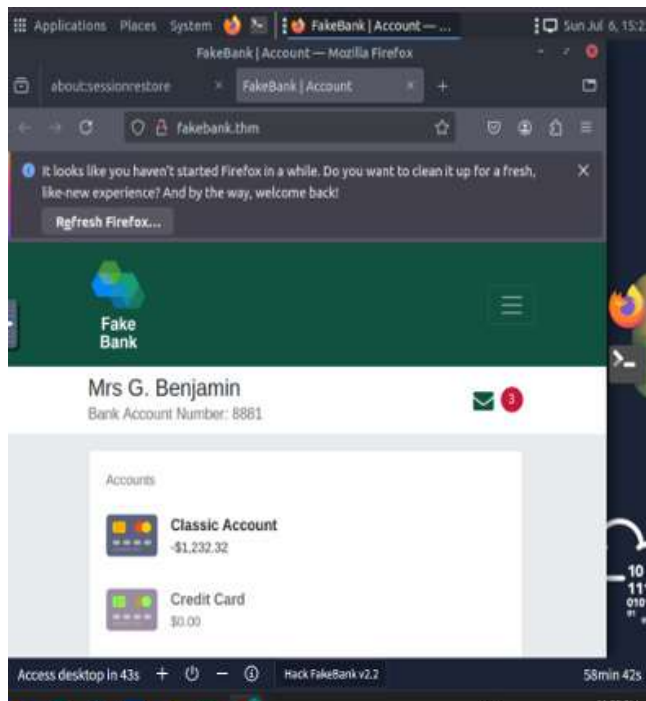
- Step 1: Usage of Gobuster

- We used the terminal command: **gobuster -u http://fakebank.thm -w wordlist.txt dir** This attempts to discover hidden or private admin pages.
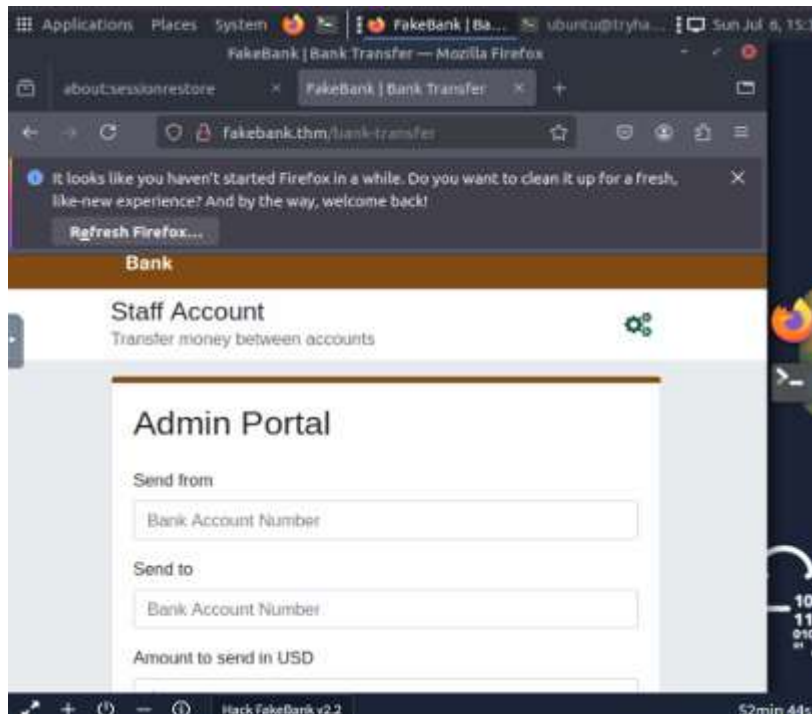
▪Step 2: Hack the Bank

- Accessing /bank-transfer

Gobuster helped discover a hidden page: /bank-transfer. Navigating to this URL revealed an admin portal for transferring money between bank accounts. This represents a critical vulnerability.

- Transferring Funds

- On the /bank-transfer page, we are told to initiate a transfer of $2000 from account 2276 to my own account 8881. The application returned a confirmation message stating "Success, transfer completed," with reference ID and transfer details – proving the operation was executed without any authentication barrier.
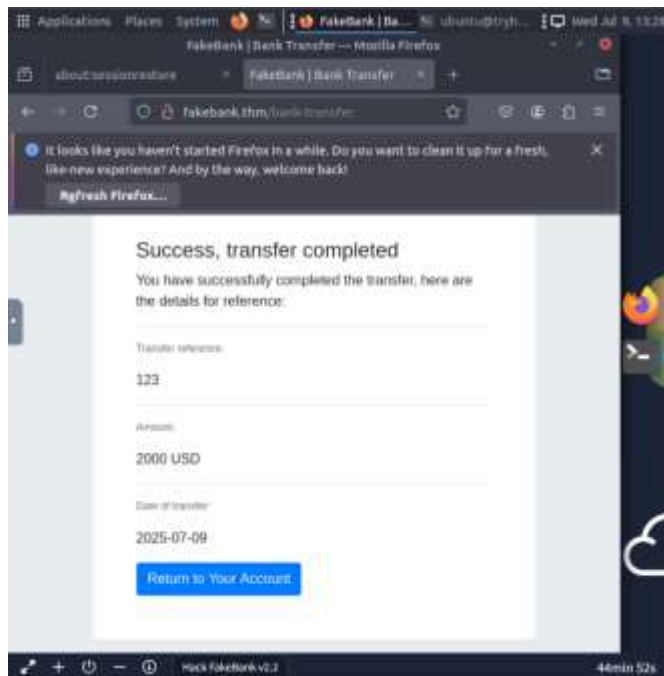
- Verifying the Result

- After the transfer, revisiting the account page confirmed the new balance and showed a congratulatory banner: "Congratulations - you hacked the bank! The answer to the TryHackMe question is BANK-HACKED." This marks the completion of the task and highlights the seriousness of exposed admin panels in real-world application.