TryhackMe write-Up

Hack your first website (legally in a safe environment) and experience an ethical hacker's job.

Completed on
Nov 30, 2024

Prepared by
Gajanan Tayde

Room Title: Offensive Security Introduction

Learning Path: Introduction to Cyber Security | Pre Security

Room Difficulty: Easy

Introduction

The **Offensive Security** path on TryHackMe is designed to introduce participants to the core concepts, tools, and methodologies used in ethical hacking and penetration testing. It serves as a stepping stone for beginners and intermediate learners to understand the offensive side of cybersecurity, focusing on identifying, exploiting, and mitigating vulnerabilities in real-world scenarios.

This path emphasizes practical, hands-on learning through a series of guided labs, challenges, and writeups. These exercises simulate real-world attacks, allowing you to develop the skills necessary to think like an attacker while reinforcing defensive strategies.

Overview of the Room: Offensive Security Intro

This room introduces the foundational knowledge required to dive into offensive security. It covers the basics of penetration testing methodologies, including:

- **Reconnaissance**: Gathering information about a target system.
- **Scanning**: Identifying live hosts, open ports, and services.
- **Exploitation**: Leveraging vulnerabilities to gain unauthorized access.
- **Post-Exploitation**: Understanding what to do after gaining access

Task- 01

What is Offensive Security?

- Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system? Offensive Security OR Defensive Security
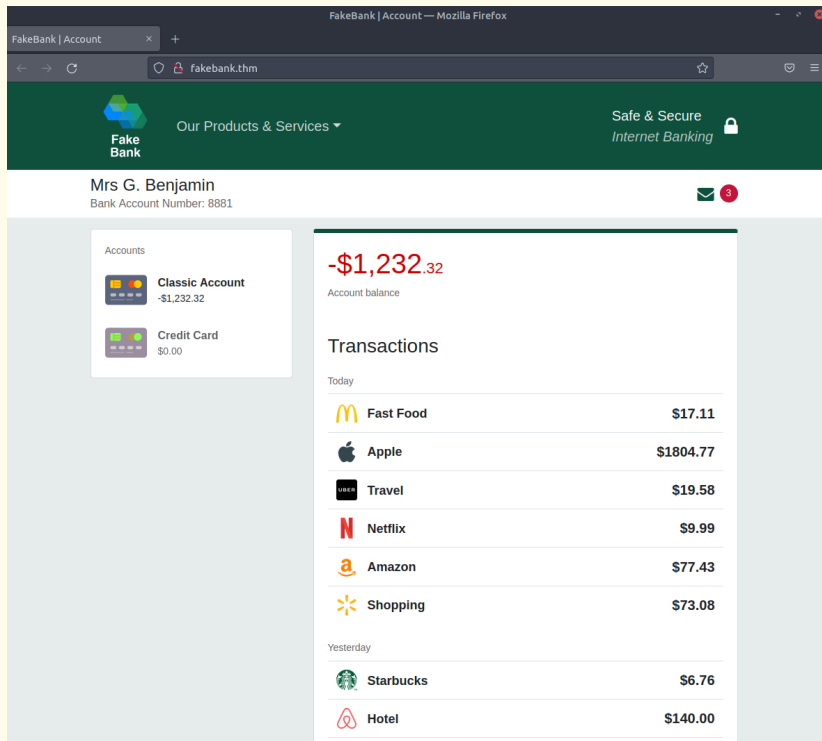
- Answer: Offensive Security

Task-02

Hacking your first machine

We will use a command-line application called "Gobuster" to brute-force FakeBank's website to find hidden directories and pages. Gobuster will take a list of potential page or directory names and try accessing a website with each of them; if the page exists, it tells you.

Step 1. Open A Terminal

A terminal, also known as the command line, allows us to interact with a computer without using a graphical user interface. On the machine, open the terminal by clicking on the Terminal icon on the right of the screen.
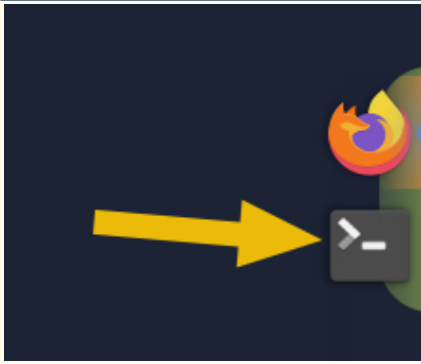
Step 2. Use Gobuster To Find Hidden Website Pages

Most companies have an admin portal page, giving their staff access to basic admin controls for day-to-day operations. For a bank, an employee might need to transfer money to and from client accounts. Due to human error or negligence, there may be instances when these pages are not made private, allowing attackers to find hidden pages that show or give access to admin controls or sensitive data.

```
gobuster -u http://fakebank.thm -w wordlist.txt dir
```

```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.thm -w wordlist.txt dir


======================================================
Gobuster v2.0.1                  OJ Reeves (@TheColonial)
======================================================
[+] Mode         : dir
[+] Url/Domain   : http://fakebank.thm/
[+] Threads      : 10
[+] Wordlist     : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
======================================================
2024/05/21 10:04:38 Starting gobuster
======================================================
/images (Status: 301)
/bank-transfer (Status: 200)
======================================================
2024/05/21 10:04:44 Finished
======================================================
```

You will see that Gobuster scans the website with each word in the list, finding pages that exist on the site. Gobuster will have told you the pages in the list of page/directory names (indicated by Status: 200).

Step 3. Hack The Bank

You should have found a secret bank transfer page that allows you to transfer money between bank accounts (/bank-transfer). Type the hidden page into the FakeBank website using the browser's address bar.
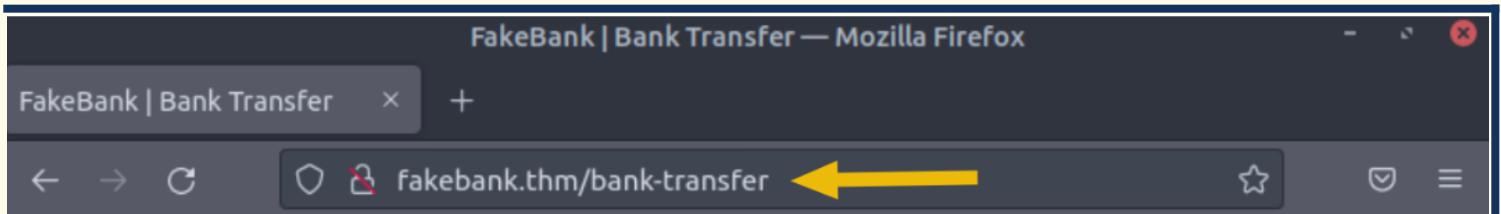
From this page, an attacker has authorized access and can steal money from any bank account. As an ethical hacker, you would (with permission) find vulnerabilities in their application and report them to the bank to fix them before a hacker exploits them.

Your mission is to transfer $2000 from bank account 2276 to your account (account number 8881). If your transfer was successful, you should now be able to see your new balance reflected on your account page.

Go there now and confirm you got the money! (You may need to hit Refresh for the changes to appear)

Please press "Return to Your Account" to find the answer of the first question in this task i.e. **BANK-HACKED**
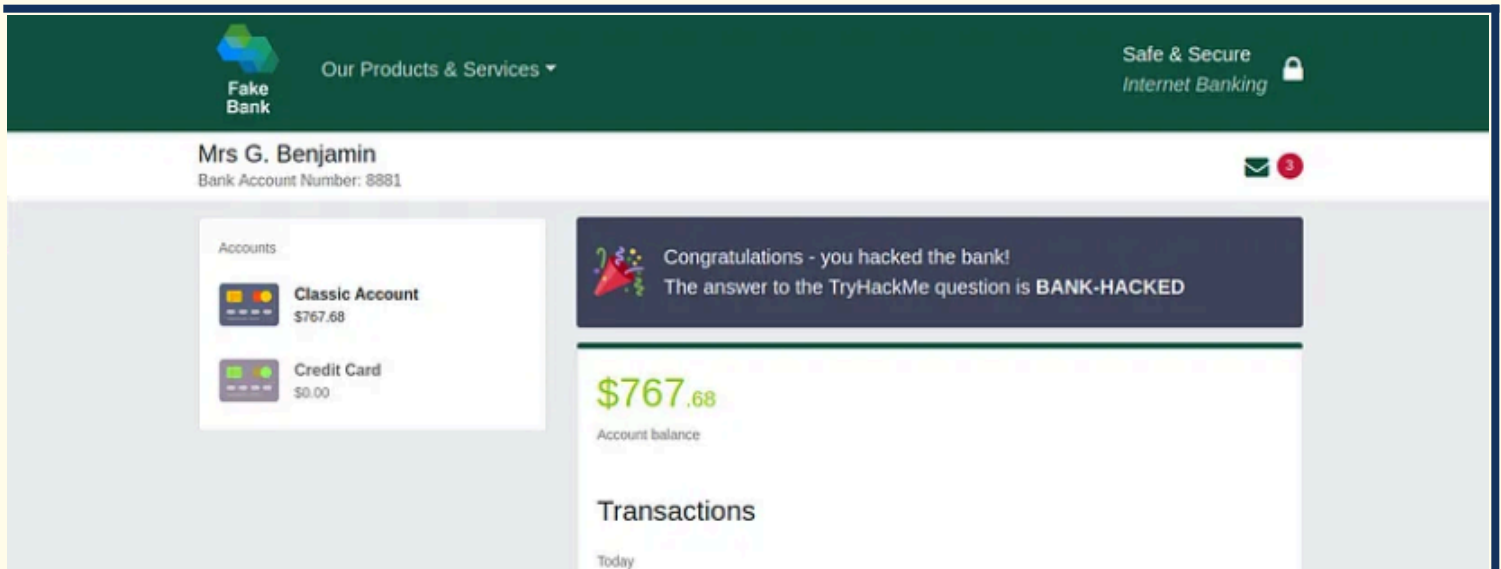
- Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

- Answer:**BANK-HACKED**

- No Answer Needed for other Questions Just marked them as complete.

Task-03

Careers in Cyber Security

In this task, we are introduced to several offensive security roles, including Penetration Tester, Red Teamer, and Security Engineer.Read through the information provided and proceed to the next room!

No answer is required—just click "Completed."

Conclusion

Today, we successfully hacked into our first website (legally and within a safe environment) and gained a glimpse into the role of an ethical hacker.

If you enjoy my content, feel free to follow me on other social media platforms. You can find all my links here. Should you have any questions or spot any errors in my content, please email me at gajanan1303@gmail.com I'm always happy to learn and improve!

Supplementary:

TryHackMe Profile: TryHackME
GitHub Portfolio: GitHub

LinkedIn: [LinkedIN](#)
[GItHub_Notes](#)