Introduction to Cyber Security – Offensive Security Intro – TryHackMe Walkthrough

Table of Contents

Task 1 – What is Offensive Security?

Offensive Security is defined as a type of cyber security that is responsible for gaining unauthorised access into a computer system and its applications. One of the key features of this cyber security type is to **understand** the thinking process of the attacker and improve the defense mechanism inside a computer system and/or application.

Question:

Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

- Offensive Security
- Defensive Security

Answer:

Offensive Security

Explanation:

Offensive Security is a type of cyber security that simulates an action of a hacker to find vulnerabilities inside a particular system. Defensive Security is a type of cyber security that protects any threat and/or risks inside a particular system from the attacker.

Task 2 – Hacking your First Machine

This task is a hands-on lab.

Scenario:
There is an application that is prepared by TryHackMe to hack safely inside the lab environment.

Task:
Transfer the money from the bank account of another client to your bank account.

Action/Process:

1. **Open the terminal App**

   It requires a terminal or Command Line Interface because it does not require any Graphical User Interface (GUI) to interact with the computer. The interface would be most likely displayed below:

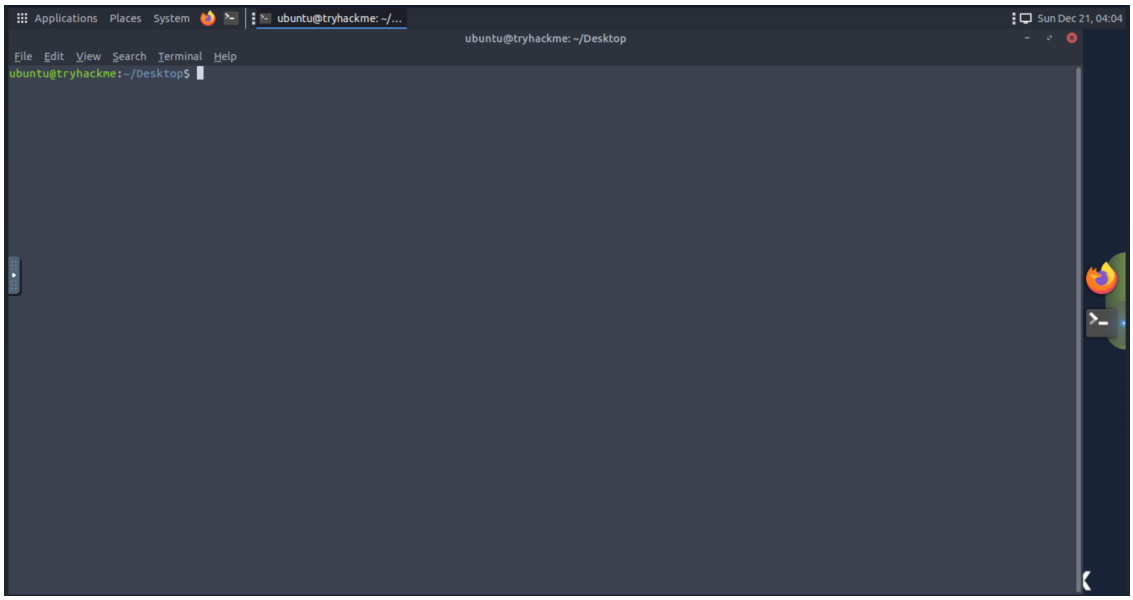

Image 1: Terminal Application after being launched.

2. **Use GoBuster to find directories of the bank web application**

   TryHackMe suggested to run this command:

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

   However, the question arises:

   - **What does `-u` and `-w` actually mean?**
   - **Can I decompose what this command is actually doing?**

   These questions will be answered in the **Result & Reflection** section. We will come back to this later.

As this command is being ran, the result in the terminal shows the output below:

```
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
===============================================================
2025/12/21 05:41:38 Starting gobuster
===============================================================
/images (Status: 301)
/bank-transfer (Status: 200)
===============================================================
2025/12/21 05:41:49 Finished
===============================================================
ubuntu@tryhackme:~/Desktop$
```

Image 2: Output after running the GoBuster tool.

3. Hack the Bank

There are 2 directories that are available on the website provided above after the scan is performed. HTTP Status 301 means the site is being redirected to a different website (Moved Permanently), while 200 indicates that the site is available to access for all clients. When it is visited on the web browser, the UI of the website is given below:

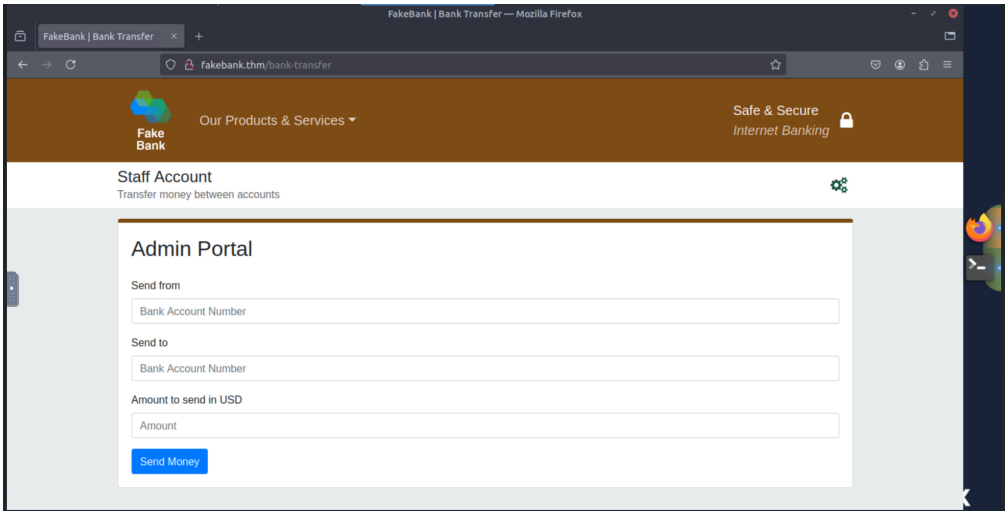

Image 3: The hidden directory found while scanning.

This site is displaying the Admin portal, which consists of the Bank Account Number from one recipient and the other as well as the amount that the money needs to be sent. TryHackMe provides the information to send $2000 with the bank account number 2276 to 8881. Here is what I provided:

Image 4: Details about sending the money.

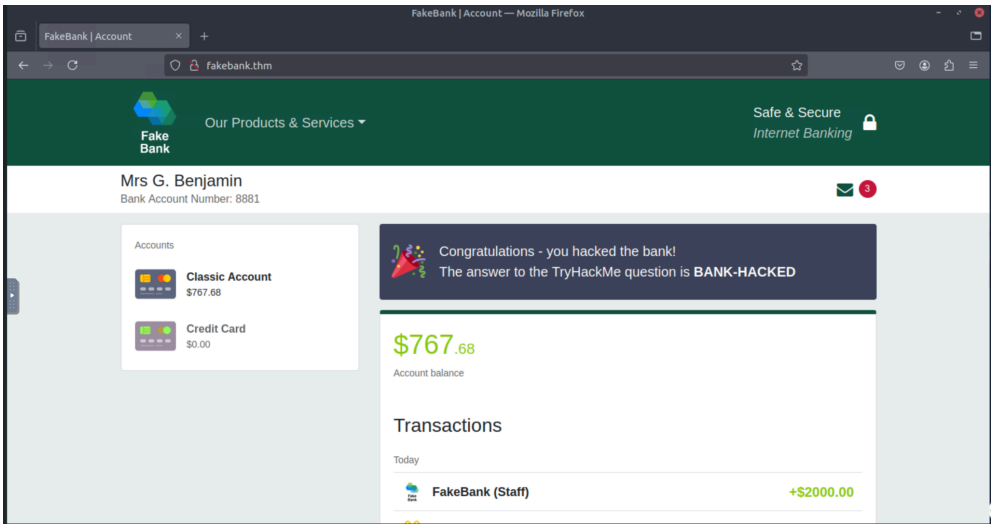

Image 5: Result after sending the money.

Question:

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

Result & Reflection:

Referring back to the questions on the **Actions/Processes**:

- **What does `-u` and `-w` actually mean?**
- **Can I decompose what this command is actually doing?**

The first question can be answered by typing `man gobuster` or `gobuster -h` which loads the manual of the name and the functions of the tool itself. Based on the results, here is what it meant:

- `-u` refers to the target URL or the domain, which in this case is `http://fakebank.thm`
- `-w` refers to path of the wordlist, which in this case is `wordlist.txt`

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

This command is running the tool called gobuster, with the URL located at http://fakebank.thm and wordlist inputted into wordlist.txt. In addition, the `dir` specifies the mode of the tool itself, which in this case is directory mode, searching for directories available in the web server located at http://fakebank.thm. The detailed guide can be found at this github repository:

https://github.com/OJ/gobuster – GoBuster tool

Task 3 – Careers in cyber security

There are a number of different careers in Cyber Security, not limited to offensive security. These are the some of the wide options for cyber security careers in offensive security:

- Penetration Tester (Pentester) – Responsible for testing technology products to find any vulnerabilities inside the product itself.
- Red Teamer – Plays a role in adversary, perform an attack to the company and provide feedback based on the perspective of a threat actor.
- Security Engineer – Design, monitor, and maintain security controls, systems, and networks to prevent any possible cyberattacks.

Question:
Read the above, and continue to the next room!

Answer:
None.

Explanation:
There are a lot of cyber security jobs other than offensive security, this room specifies some of the examples of possible cyber security roles, specifically in Offensive Security.