

Pre Security > Introduction to Cyber Security > Offensive Security Intro


Offensive Security Intro

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

Easy 15 min

Share your achievement Help Save Room 68608 Options

Task 1 What is Offensive Security?



"To outsmart a hacker, you need to think like one."

This is the core of "Offensive Security." It involves breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access. The goal is to understand hacker tactics and enhance our system defences.

Beginning Your Learning Journey

In this TryHackMe room, you will be guided through hacking your first website in a legal and safe environment. The goal is to show you how an ethical hacker operates.

But before we do that, let's review by answering the questions below. Type your answer in the text box after the question and click the "Submit" button. When you're done, proceed to Task 2.

Answer the questions below

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

Offensive Security ✓ Correct Answer Hint

Task 1: What is Offensive Security?

Learned the fundamentals of Offensive Security, which involves simulating hacker tactics to uncover vulnerabilities in systems before malicious actors can.

Understood the difference between Offensive Security and Defensive Security.

Answered the question correctly:

Which process simulates a hacker's actions to find vulnerabilities?

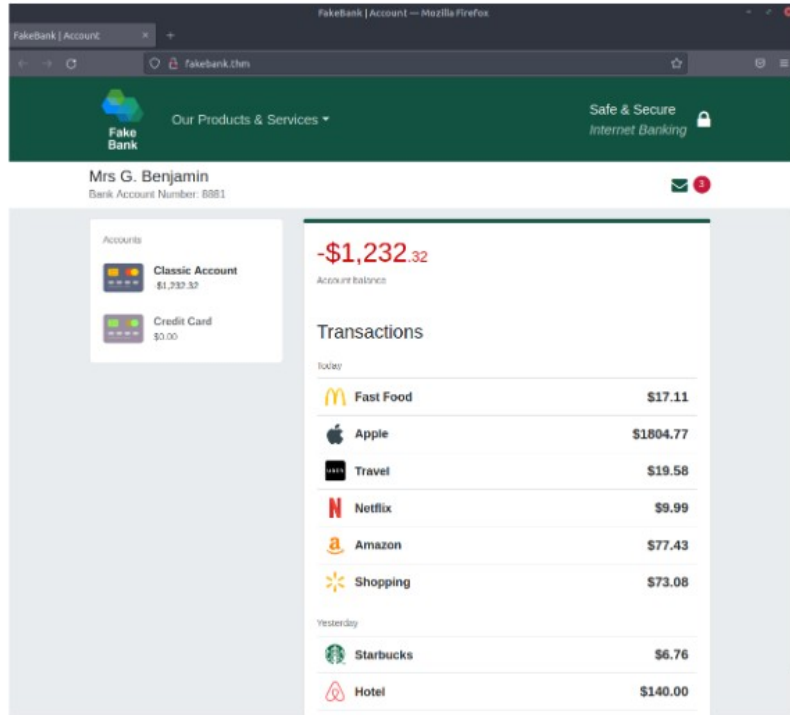
Answer: Offensive Security

Here at TryHackMe, we use Virtual Machines to create simulated environments that serve as practical complements to rooms.

In this room, we have prepared a fake bank application called Fakebank that you can safely hack. To start this machine, click on the **Start Machine** button below.

[▶ Start Machine](#)

Your screen should be split in half, showing this content on the left and the newly launched machine on the right. If you hide it later, you can always click on the **Show Split View** button at the top to display it again. You should see a browser window showing the website below:



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.

To begin, type the following command into the terminal to find potentially hidden pages on FakeBank's website using Gobuster (a command-line security application).

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

The command will run and show you an output similar to this:

```
=====
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
=====
```

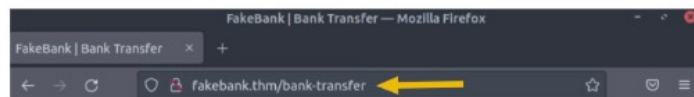
In the command above, `-u` is used to state the website we're scanning, `-w` takes a list of words to iterate through to find hidden pages.

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).

```
=====
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
=====
```

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)

Answer the questions below

Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED

✓ Correct Answer

🔒 Hint

Task 2: Hacking Your First Machine

Started a Virtual Machine (VM) from TryHackMe's platform that launched a fake online banking website called FakeBank.

Gained access to a user's account showing their balance and recent transactions.

Step 1: Open a Terminal

Accessed the terminal in the VM environment to interact with the system via the command line.

Directory Brute-Forcing with Gobuster

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

Gobuster scanned the target URL and identified a hidden endpoint:
/bank-transfer (HTTP status code: 200)

Step 2 : Exploiting the Vulnerability – Bank Transfer Access

Navigated to <http://fakebank.thm/bank-transfer>, a hidden bank transfer page that lacked proper access control.

Used this page to simulate unauthorized transfers between bank accounts:

Transferred \$2000 from account 2276 to my account 8881. After refreshing the account page, I saw a new balance update confirming the successful transaction.

A hidden message appeared indicating the correct completion of the task:
BANK-HACKED