

TryHackme Offensive Security Introduction – writeup

Room : Offensive Security Intro

Name : Gokul B

Introduction to Offensive Security – TryHackMe


Task 1: What is Offensive Security?

Offensive Security involves simulating the actions of malicious hackers to uncover vulnerabilities in systems and applications. The goal is to understand attacker behavior to improve defenses. Ethical hackers legally use these techniques to identify and fix weaknesses.

Key Points:

- - Focuses on proactive testing.
- - Simulated attacks enhance system security.
- - Legal hacking with permission to strengthen systems.

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 2: Hacking Your First Machine

A virtual environment was launched with a fake banking website (fakebank.thm). The objective was to simulate an attack and gain unauthorized access.

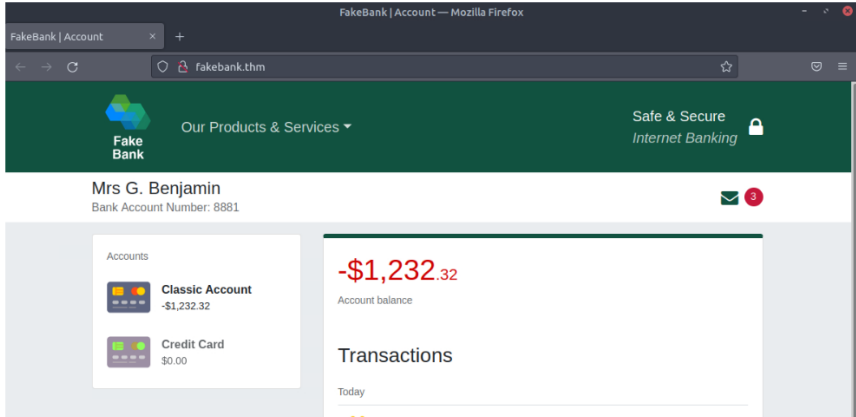
Task 2 Hacking your first machine

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:



Task 1 What is Offensive Security?

Task 2 Hacking Your First Machine

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 at the top right of this task. Your screen should be split in half, showing this content on the left and the newly launched machine on the right. You should see a browser window showing the website below:

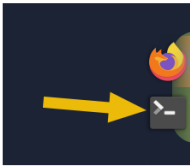
▶ Start Machine

Your First Hack

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.



Steps:

- - Started the virtual machine and accessed the fake bank interface.
- - Used Gobuster to discover hidden directories.
- - Found and accessed the /bank-transfer page.
- - Transferred funds between accounts to simulate a successful hack.

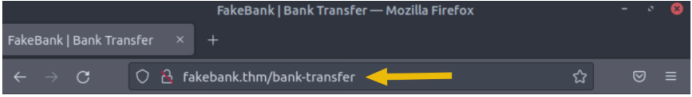
=====

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?

✓ Correct Answer

🔍 Hint

Task 3: Careers in Cyber Security

Offensive Security is a subset of the broader cybersecurity field. This section covered career paths and learning strategies.

Getting Started:

- - Learn networking, operating systems, and security basics.
- - Practice on platforms like TryHackMe.
- - Engage in hands-on labs regularly.

Career Roles:

- - Penetration Tester: Identifies and reports system vulnerabilities.
- - Red Teamer: Simulates real-world attacks to test defenses.
- - Security Engineer: Designs and maintains secure systems.

Task 3

Careers in cyber security

How can I start learning?

People often wonder how others become hackers (security consultants) or defenders (security analysts fighting cybercrime), and the answer is simple. Break it down, learn an area of cyber security you're interested in, and regularly practice using hands-on exercises. Build a habit of learning a little bit each day on TryHackMe, and you'll acquire the knowledge to get your first job in the industry.

Trust us; you can do it! Just take a look at some people who have used TryHackMe to get their first security job:

- Paul went from a construction worker to a security engineer. [Read more](#)
- Kassandra went from a music teacher to a security professional. [Read more](#)
- Brandon used TryHackMe while at school to get his first job in cyber. [Read more](#)

What careers are there?

The cyber careers room goes into more depth about the different careers in cyber. However, here is a short description of a few offensive security roles:

- Penetration Tester - Responsible for testing technology products for finding exploitable security vulnerabilities.
- Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

Answer the questions below

Read the above, and continue with the next room!

No answer needed

✓ Correct Answer

Summary

This TryHackMe room introduced the fundamentals of Offensive Security. It emphasized practical learning and demonstrated a basic ethical hacking workflow:

- - Reconnaissance using tools.
- - Discovering vulnerabilities via brute force.
- - Exploiting weaknesses to simulate attacks.

Ethical hacking plays a vital role in enhancing digital security.