

TryHackMe: Offensive Security Intro — Writeup


Name : Nandana Silju

Room : Offensive Security Intro

✓ Task 1: What is Offensive Security?

This task introduces the concept of **Offensive Security**, which refers to the proactive approach in cybersecurity to simulate attacks on systems to identify vulnerabilities before real attackers do.

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

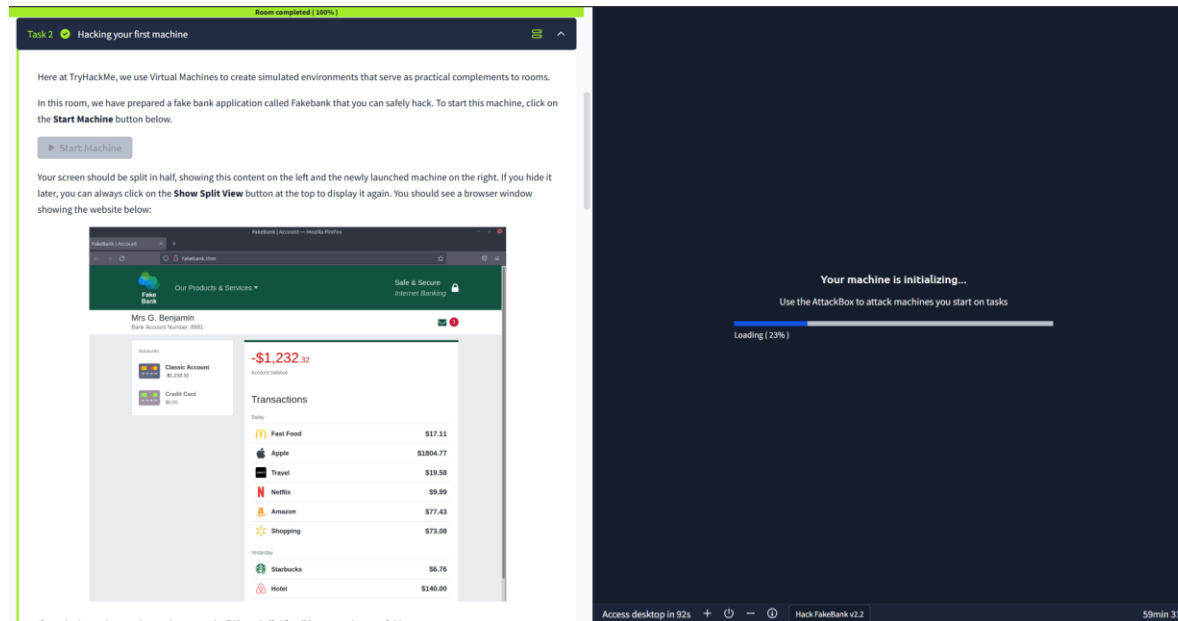
🔍 Hint

✓ Task 2: Hacking Your First Machine

In this task, we interact with a simulated vulnerable website. The goal is to practice exploiting a basic **web vulnerability**.

■ Step 1: Starting the Machine and Exploring the Target

Once the TryHackMe room launched, I clicked **Start Machine**, which opened a **split-view screen** with the browser showing the FakeBank website. This simulated a real-world environment for ethical hacking.



■ Step 2: Finding Hidden Directories Using Gobuster

I opened the terminal in the virtual machine and ran the following command:

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

The screenshot displays a virtual machine environment. On the left, a terminal window shows the execution of the Gobuster command. The output indicates that Gobuster v2.0.1 is running with the following configuration: Mode: dir, Url/Domain: http://fakebank.thm/, Threads: 10, Wordlist: wordlist.txt, Status codes: 200,204,301,302,307,403, and Timeout: 10s. The command starts at 2024/05/21 10:04:38 and finishes at 2024/05/21 10:04:44. The output shows that Gobuster found hidden directories: /images (Status: 301) and /bank-transfer (Status: 200).

On the right, a web browser window shows the FakeBank application interface. The account balance is -\$1,232.32, and the credit card balance is \$0.00. The transactions list for today includes:

Transaction	Amount
Fast Food	\$17.11
Apple	\$1804.77
Travel	\$19.58
Netflix	\$9.99
Amazon	\$77.43

The bottom status bar of the virtual machine shows 'Access desktop in 20s', 'Hack FakeBank v2.2', and '58min 19s'.

■ Step 3: Exploiting the Bank Transfer Functionality

I visited the hidden path:

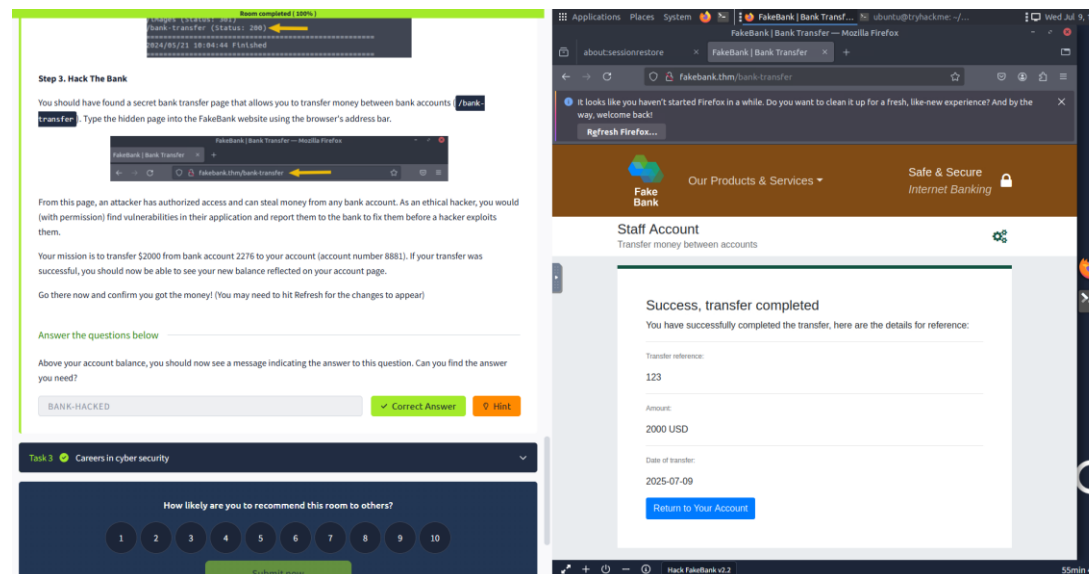
`http://fakebank.thm/bank-transfer`

This page allowed me to initiate a bank transfer. Following the instructions:

- From: 2276
- To: 8881
- Amount: 2000

After completing the transfer and refreshing the account page, I saw my new balance reflected and a confirmation message:

BANK-HACKED



✓ Task 3: Careers in Cybersecurity

This task gives insight into different roles in cybersecurity, especially focusing on offensive roles.

Offensive Roles Discussed:

- Penetration Tester: Simulates attacks to find vulnerabilities.
- Red Teamer: Tests overall security using adversary emulation.
- Bug Bounty Hunter: Finds and reports bugs in return for rewards.

The screenshot shows a web interface for a task titled "Task 3: Careers in cyber security". At the top, a green bar indicates "Room completed (100%)". The task title is displayed in a dark blue header. The main content area has a light green background and contains the following text:

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!

Below the text, there is a green button labeled "Correct Answer" and a grey button labeled "No answer needed".

At the bottom, there is a dark blue section with the question "How likely are you to recommend this room to others?". It features a row of 10 circular buttons numbered 1 to 10, with button 5 selected. A green "Submit now" button is located below the row.