

TryHackMe CTF Write-Up

Task 1 - TryHackMe Room: Offensive Security Intro

Objective:

Explore the basics of offensive security through a simple CTF exercise where we:

- Scan for hidden directories on a fake banking website.
- Exploit vulnerabilities to perform unauthorized fund transfers.
- Simulate how ethical hackers assess security flaws.

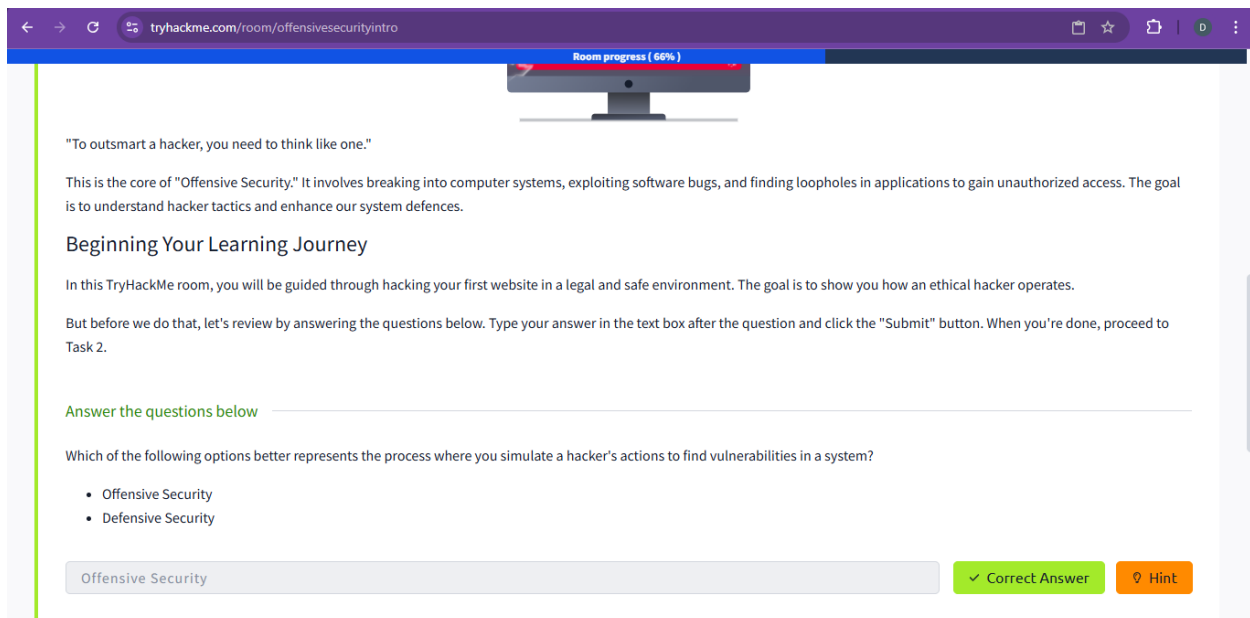
Tools Used:

- **Gobuster:** For directory brute forcing.
- **Firefox Browser:** To access and manipulate the web application.
- **Linux Terminal:** For running enumeration commands.

Task 1: 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?

Answer: Offensive Security



The screenshot shows a web browser window with the URL `tryhackme.com/room/offensivesecurityintro`. At the top, a blue progress bar indicates "Room progress (66%)". Below the browser, a computer monitor icon displays the room's content. The text on the screen reads: "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

 At the bottom, there is a text input field containing "Offensive Security", a green "Correct Answer" button, and an orange "Hint" button.

Task 2: Hacking Your First Machine

Step-by-Step Walkthrough

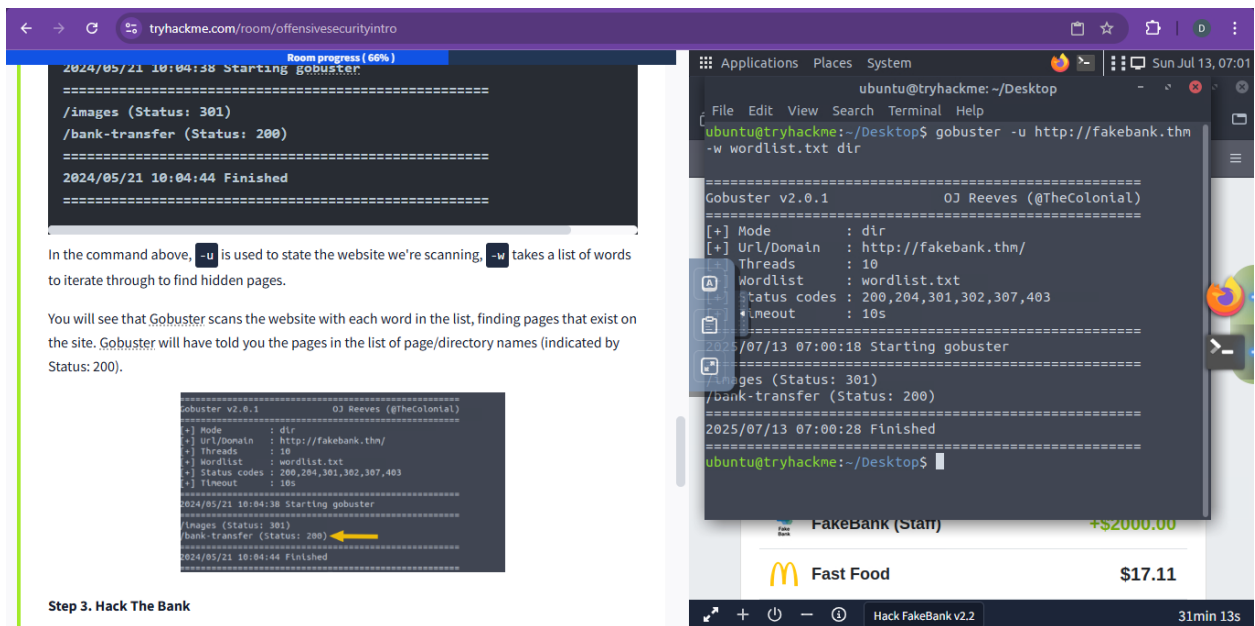
Step 1: Enumerate Hidden Pages Using Gobuster

We started by running Gobuster on the target URL:

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

This revealed two directories:

- /images (Status: 301)
- /bank-transfer (Status: 200)



Step 2: Access the Hidden Transfer Page

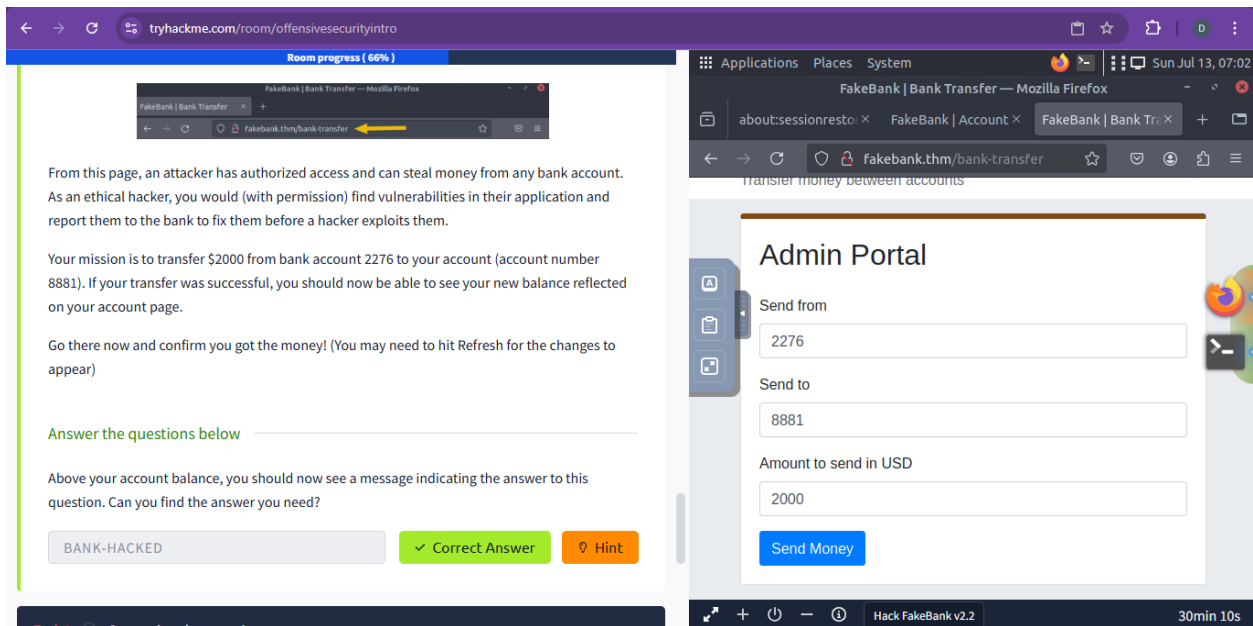
By visiting <http://fakebank.thm/bank-transfer>, we found an Admin Portal allowing unauthorized bank transfers.

Step 3: Exploit the Vulnerability

We transferred \$2000 from account 2276 to account 8881 using the exposed admin form.

Details entered:

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



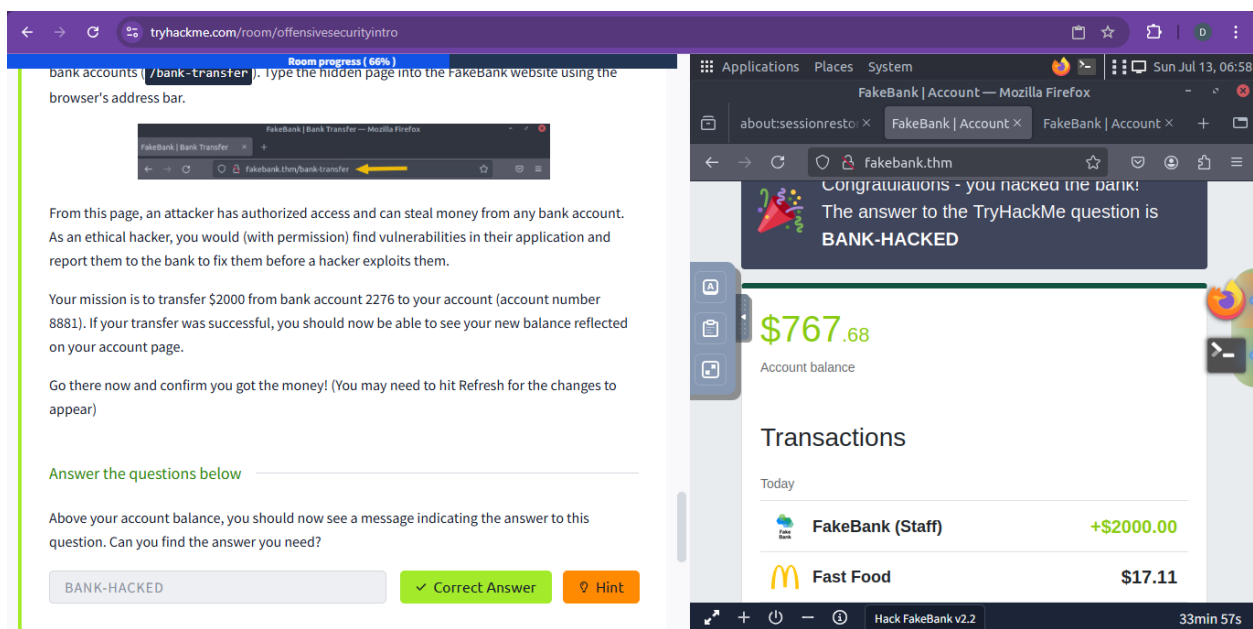
Step 4: Confirm the Exploit Worked

Navigated to the account page to check the balance and validate the transfer.

Message seen:

Congratulations - you hacked the bank!

The answer to the TryHackMe question is: BANK-HACKED



After transaction, message appeared:

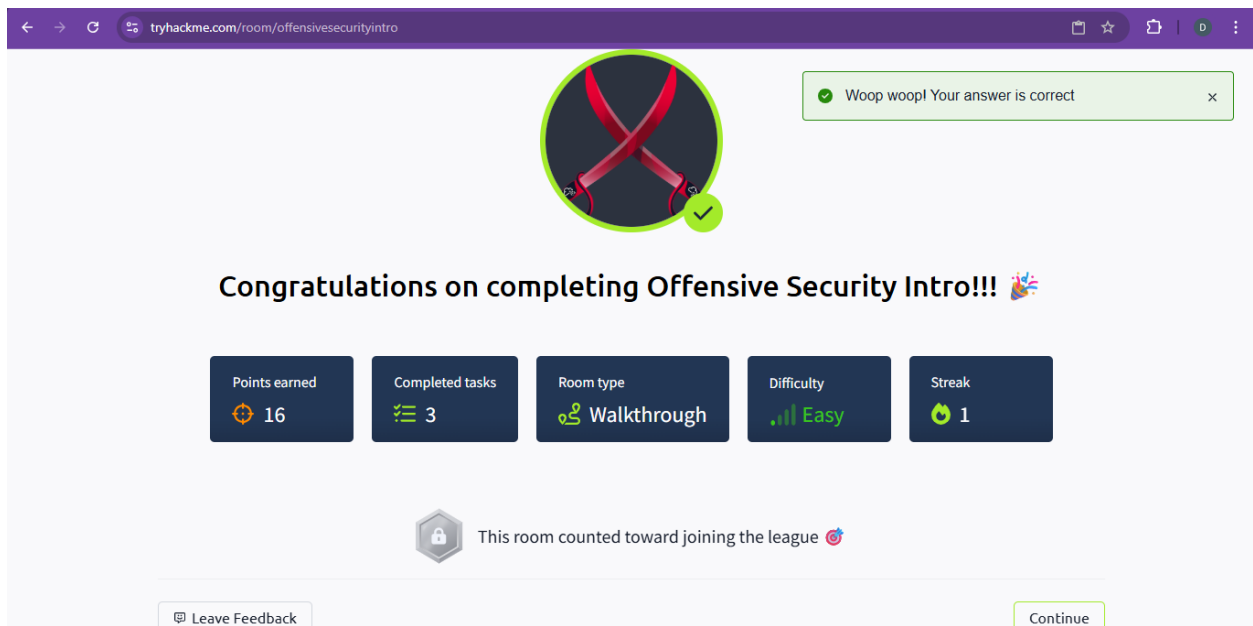
Answer: BANK-HACKED

Task 3: Careers in Cyber Security

Clicked the complete button to finish the task.

Room Completion

Successfully completed all tasks and questions in the TryHackMe room.



The screenshot shows the TryHackMe room completion page for 'Offensive Security Intro'. At the top, a green notification bubble says 'Woop woop! Your answer is correct'. Below this is a large circular icon with a red 'X' and a green checkmark. The main heading reads 'Congratulations on completing Offensive Security Intro!!!' with a party popper emoji. Below the heading are five statistics cards: 'Points earned' (16), 'Completed tasks' (3), 'Room type' (Walkthrough), 'Difficulty' (Easy), and 'Streak' (1). A message states 'This room counted toward joining the league'. At the bottom, there are 'Leave Feedback' and 'Continue' buttons.

Points earned	Completed tasks	Room type	Difficulty	Streak
16	3	Walkthrough	Easy	1

Author:

Dennis Jacob

Cyber Security Bootcamp Participant

OWASP Kerala x µLearn