

TryHackMe CTF Writeup

This report summarizes the progress and findings of Task in the TryHackMe room "Offensive Security". The room simulates ethical hacking against a fake banking application called FakeBank. The objective is to understand how hackers operate and how to identify system vulnerabilities safely using hands-on tools.

This contains the detailed walkthrough of the 'Offensive Security' room on TryHackMe. The room walks users through the core ideas of ethical hacking using banking platform.



Offensive Security Intro

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

Task 1

What is offensive security

1. Which of the following option better represents the process where you simulate a hacker's action to find vulnerabilities in a system?

Answer: Offensive Security

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

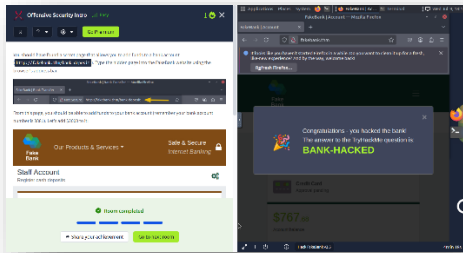
✓ Correct Answer

💡 Hint

Task 2

Hacking your first machine

In this room, we can see a fake bank application called FakeBank that we can safely hack. The virtual machine with the application should start automatically. Screen should be split in half, showing this content on the left and the newly launched machine on the right.



After that, we can see the information about account holder

1. What is your bank account number in the 'FakeBank' web application?

Answer: 8881

Answer the questions below

What is your bank account number in the FakeBank web application?

8881

✓ Correct Answer

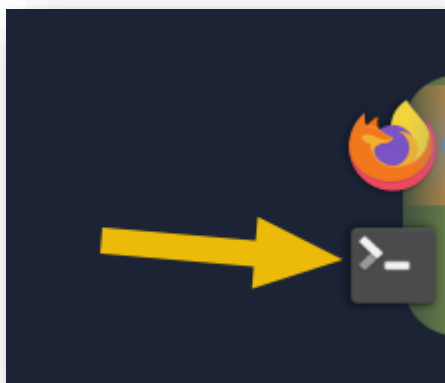
Task 3

Your First Hack

After the machine started, the FakeBank application loaded. It shows the account details for "Mrs. G. Benjamin," just like a real user would when logged in.

Step1

Open terminal and using the icon



Using the terminal, write the dirb command followed by the URL of the website you want to brute-force. Then run it using enter key

Dirb should have found 2 hidden URLs. One of them is `http://fakebank.thm/images`. What is the other one?

Answer: <http://fakebank.thm/bank-deposit>

Answer the questions below

Dirb should have found 2 hidden URLs. One of them is `http://fakebank.thm/images`. What is the other one?

✓ Correct Answer

💡 Hint

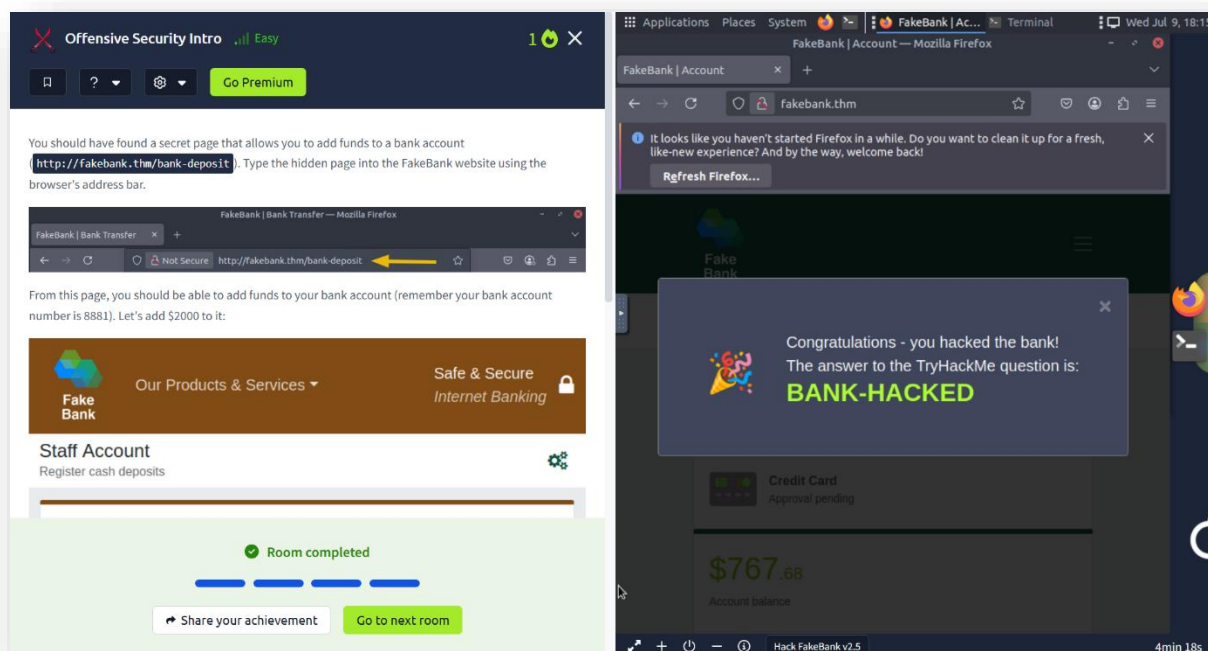
Task 4

Adding Funds to Your Account

Gobuster helped discover a hidden page: `/bank-transfer`. Navigating to this URL revealed an admin portal for transferring money between bank accounts

Adding funds

I add \$2000 to my account 8881.



2. If your balance is now positive, a pop-up should appear with some green words in it. Input the green words as the answer to this question (all in uppercase).

Answer: BANK-HACKED

Answer the questions below

If your balance is now positive, a pop-up should appear with some green words in it. Input the green words as the answer to this question (all in uppercase).

(You may need to hit Refresh if you closed the pop-up already)

BANK-HACKED

✓ Correct Answer

🔍 Hint

Conclusion

This task introduces key concepts in offensive security, such as directory brute-forcing, hidden URL discovery, and web application exploitation. By interacting with a simulated banking environment, the learner gains practical experience in identifying vulnerabilities and understanding attacker behaviour. This hands-on approach builds foundational knowledge essential for ethical hacking and penetration testing.

SUBMITTED BY:
SREEHARI VINOD