

Offensive Security Intro Room Completion Report

This document contains screenshots and completion proof for the TryHackMe 'Offensive Security Intro Room'. Each screenshot corresponds to a task completed successfully.

Author: Dhaniyal Jose

Date: 2025-08-09

Target IP: 10.201.95.73

Room Link: <https://tryhackme.com/room/offensivesecurityintro>

1. Introduction

The Offensive Security Intro room is a beginner-friendly lab that introduces core concepts in ethical hacking.

It guides the user through reconnaissance, enumeration, exploitation, and privilege escalation against a simulated banking website called **FakeBank**.

2. Tools Used

- **AttackBox** (TryHackMe's browser-based Kali Linux)
- `nmap` – network scanning
- `dirb` – directory brute forcing
- Firefox – browsing target pages
- Linux terminal utilities

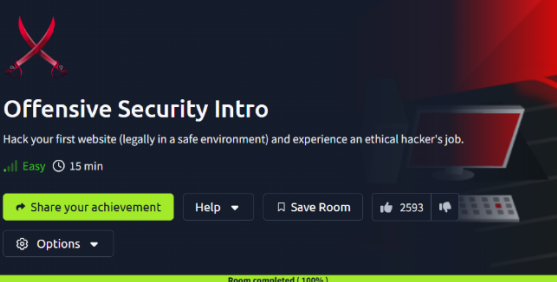
3. Steps Taken

Step 1 – Starting the Machine

- Started the TryHackMe machine and noted the target IP: `10.201.95.73`.
- Launched the AttackBox for easy, VPN-free access.

Task 1 Screen shot:

Learn > 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 👍 2593 🗨️

⚙️ Options ▾

Room completed (100%)

Target Machine Information

Title	Target IP Address	Expires
Hack FakeBank v2.5	10.201.95.73 📶 🌐	50min 14s

Add 1 hourTerminate

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.

Our labs can also be reverted to their initial state, so don't be afraid to break the machine. Experiment as much as you like, we got you covered!

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 Screen shot:

Task 2 🟢 Starting the Lab

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. The virtual machine with the application should start automatically for you. If it doesn't, 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:

🔒 FakeBank

Our Products & Services +

Safe & Secure internet banking

Mrs G. Bergamin

Bank Account Number: 8881

Accounts

Classic Account

£1,232.32

Credit Card

£0.00

Transactions

Today

Fast Food

£17.11

Apple

\$184.77

Internet

\$19.58

Netflix

\$9.99

Amazon

\$77.43

Shopping

\$73.08

Yesterday

Starbucks

\$6.76

Hotel

\$140.00

👉 Let's see the virtual machine! Click here for help!

Answer the questions below

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

8881

✓ Correct Answer

🔒 FakeBank

Our Products & Services +

Safe & Secure internet banking

Mrs G. Bergamin

Bank Account Number: 8881

Accounts

Classic Account

£1,232.32

Credit Card

£0.00

Transactions

Today

Fast Food

£17.11

Apple

\$184.77

Internet

\$19.58

Netflix

\$9.99

Amazon

\$77.43

Shopping

\$73.08

Yesterday

Starbucks

\$6.76

Hotel

\$140.00

Task 3 Screen shot:

Task 3

Your First Hack

Briefing

Our goal is to find a way to hack the FakeBank application to steal money. For that purpose, they have provided us with an account in the bank, just as if we were a regular user.

One of the easiest ways we can try to hack the application is by finding hidden features in the application. Sometimes, applications will expose sensitive functionality to users via secret URLs. If we can find such URLs, we might be able to perform actions that a regular user is not supposed to do.

To find hidden URLs, we will use a tool called `dirb`. This tool uses a **brute-force** approach, by taking a **list of potential page names** and testing one by one if they exist in your website. This approach works because people use predictable names a lot of times.

Opening A Terminal

A terminal, also known as the command line, is a program that allows us to send text-based commands to the computer. A lot of hacking tools, including `dirb`, need to be executed from a terminal.

On the machine, open the terminal by clicking on the Terminal icon on the right of the screen.



Using dirb To Find Hidden Website Pages

Using `dirb` is quite simple. Using the terminal, write the `dirb` command followed by the URL of the website you want to brute-force. Be sure to press `enter` in your keyboard to execute the command:

```
dirb http://fakebank.thm
```

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

```
ubunt@tryhackme:~/Desktop$ dirb http://fakebank.thm

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Apr 17 16:29:52 2025
URL_BASE: http://fakebank.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4638

---- Scanning URL: http://fakebank.thm/ ----
+ http://fakebank.thm/bank-deposit (CODE:200|SIZE:4663)
+ http://fakebank.thm/images (CODE:301|SIZE:179)

-----
END_TIME: Thu Apr 17 16:29:59 2025
DOWNLOADED: 4638 - FOUND: 2
```

The output of the command might look a bit intimidating, but here's a simple breakdown of what is reported:

- The first section of the output tells us the URL_BASE we scanned, which is just the URL we gave the tool. It also shows the location of the wordlist file used by the tool, which contains common page names that will be tested during the brute-force attack. In this case, the tool uses the default wordlist included with the tool, located at `/usr/share/dirb/wordlists/common.txt`. There's a copy of the `common.txt` file in your desktop as well, if you want to explore it.
- The lines starting with `+` sign are the results of the scan. In this case, `dirb` was able to find two URLs for you. Try opening them in the machine's browser! You might find something interesting.

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

0 HINT

```
Terminal
File Edit View Search Terminal Help
ubunt@tryhackme:~/Desktop$ dirb http://fakebank.thm

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat Aug 9 17:52:37 2025
URL_BASE: http://fakebank.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4609

---- Scanning URL: http://fakebank.thm/ ----
+ http://fakebank.thm/bank-deposit (CODE:200|SIZE:4663)
+ http://fakebank.thm/images (CODE:301|SIZE:179)

-----
END_TIME: Sat Aug 9 17:52:44 2025
DOWNLOADED: 4609 - FOUND: 2
ubunt@tryhackme:~/Desktop$
```

Task 4 Screen shot:

