Intro to Offensive Security

Stanisław Ciszkiewicz

April 6, 2024

Contents

1 Introduction

This document concerns the exercise Intro to Offensive Security published on TryHackMe platform. TryHackMe platform provides a chance to improve knowledge connected with cybersecurity by facing users with diversified cyber problems. The main purpose of this excercise was to introduce offensive security as one of the most important parts of cybersecurity industry. Whats's more, it gives us a chance to practice, by trying to ethically hack fake bank account. Next sections of this document contains brief description of tasks to do in this TryHackMe room:https://tryhackme.com/room/introtooffensivesecurity.

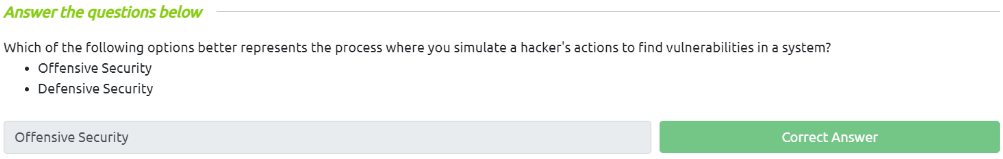
2 Task 1 - What is the Offensive Security?

In this part we can see description of the Offensive Security. It is presented as one of the way, how cybersecurity workers can find loopholes and vulnerabilities in their systems. They behave somehow like the real hackers, but the goal of their job is to find the problems and then report to the people responsible for vulnerability elimination in a company. Furthermore, in the last paragraph we can read about Deffensive Security - other cyber role, in which we try to understand how our systems were infected and how to improve our resources from future attacks.

There was only one question in this part. Our task was to answer the question: 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

As we said before the proccess in which we behave similarly to hackers (respecting ethical rules) is connected with 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

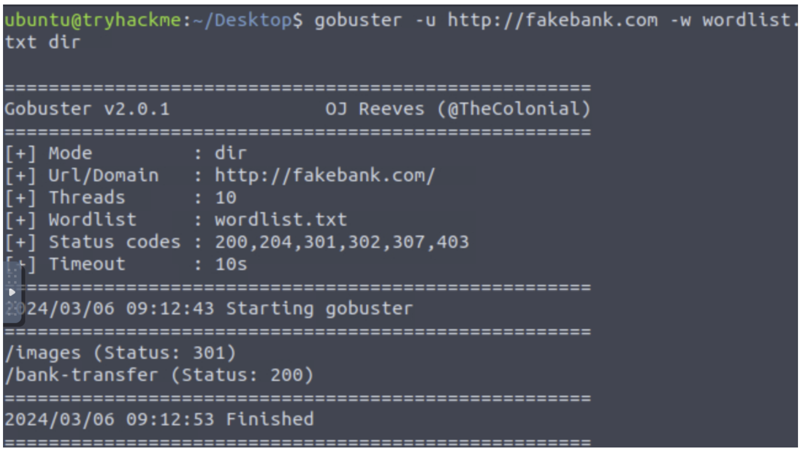
Figure 1: Task 1 answer

3 Task 2 - Hacking your first machine

This exercise provides the first chance to try what offensive security term means in practice. The purpose of this part was to hack Fake Bank's website using command line application called GoBuster. After turning on a machine, we were said to open a command line on it. Our goal is to find potentially hidden pages on Fake Bank's website which could probably lead us to some sensitive data. We begin from typing command:

```
$ gobuster —u http://fakebank.com —w wordlist.txt dir
```

-u → selecting the website to scan, -w → selecting a list of words which will be used to find hidden pages.

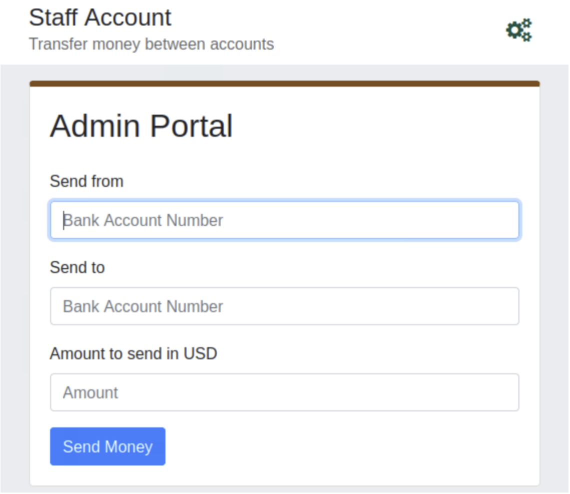


```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordlist.
txt dir

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://fakebank.com/
[+] Threads      : 10
[+] Wordlist     : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2024/03/06 09:12:43 Starting gobuster
=====================================================
/images (Status: 301)
/bank-transfer (Status: 200)
=====================================================
2024/03/06 09:12:53 Finished
=====================================================
```

Figure 2: Gobuster output

As we can see on Figure 2 application found two hidden websites: /images and /bank-transfer. Now it's time to discover what data is stored on them. First of all we start from page fakebank.com/bank-transfer. It led us to admin portal webpage on which we can order a transfer from any account we want.



Staff Account

Transfer money between accounts

Admin Portal

Send from

Bank Account Number

Send to

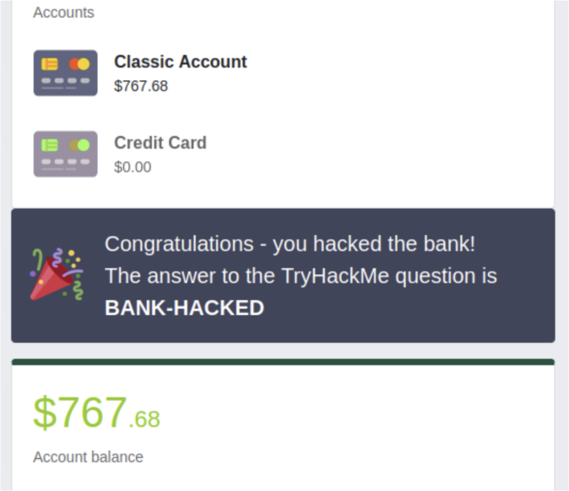
Bank Account Number

Amount to send in USD

Amount

Figure 3: bank-transfer page

Our job was to send 2000 $ from the account 2276 to our account 8881. After coming back to our account page we see that the balance has changed and our transfer was successful. Above our account balance we can see the message containing answer to the question from a task.



Accounts

Classic Account
$767.68

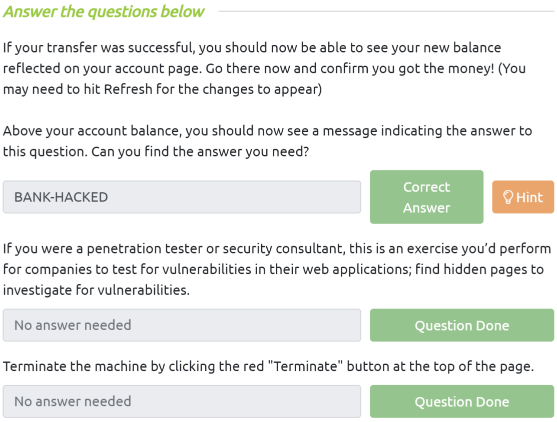
Credit Card
$0.00

Congratulations - you hacked the bank!
The answer to the TryHackMe question is
BANK-HACKED

$767.68
Account balance

Figure 4: Account balance and message

We type the answer on Tryhackme page to see if the exercise was done correctly. Other exercises from this part didn't have any practical knowledge (were just informational).



Answer the questions below

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)

Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED

If you were a penetration tester or security consultant, this is an exercise you'd perform for companies to test for vulnerabilities in their web applications; find hidden pages to investigate for vulnerabilities.

No answer needed

Terminate the machine by clicking the red "Terminate" button at the top of the page.

No answer needed

Figure 5: Task 2

4 Task 3 - Carrers in cybersecurity

This task was more informational, it included brief overview on how to start learning offensive security and what can we do being an offensive security expert. Tryhackme provides some examples of people, who had started from Tryhackme and the became a professional security workers. In the end, there is a short description of Penetration Tester, red Teamer and Security Engineer main duties in companies.

5 Summary

This room gave us a quick entry to offensive security. In the beginning we got to know the definition of offensive security, then used the basic knowledge in practice, using GoBuster application, to finish with describing potential careers in offensive security.