

Room 1: Offensive Security Intro.

Summary:

- This room entails an offensive security simulation. It demonstrates how hackers can manipulate hidden, vulnerable pages for their gain – prompting the need for a Red Team.

Objective:

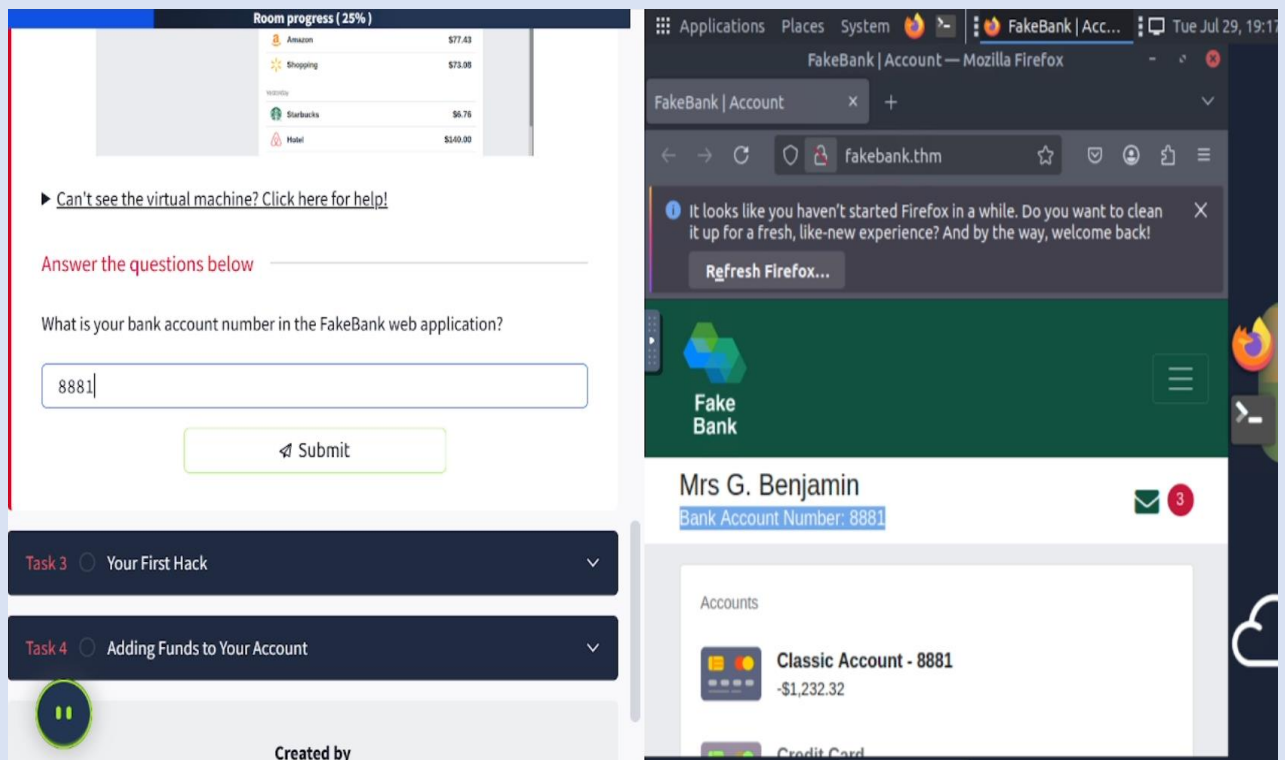
- To hack an online banking web application (legally in a safe environment), to mimic ethical hackers

Tools Used:

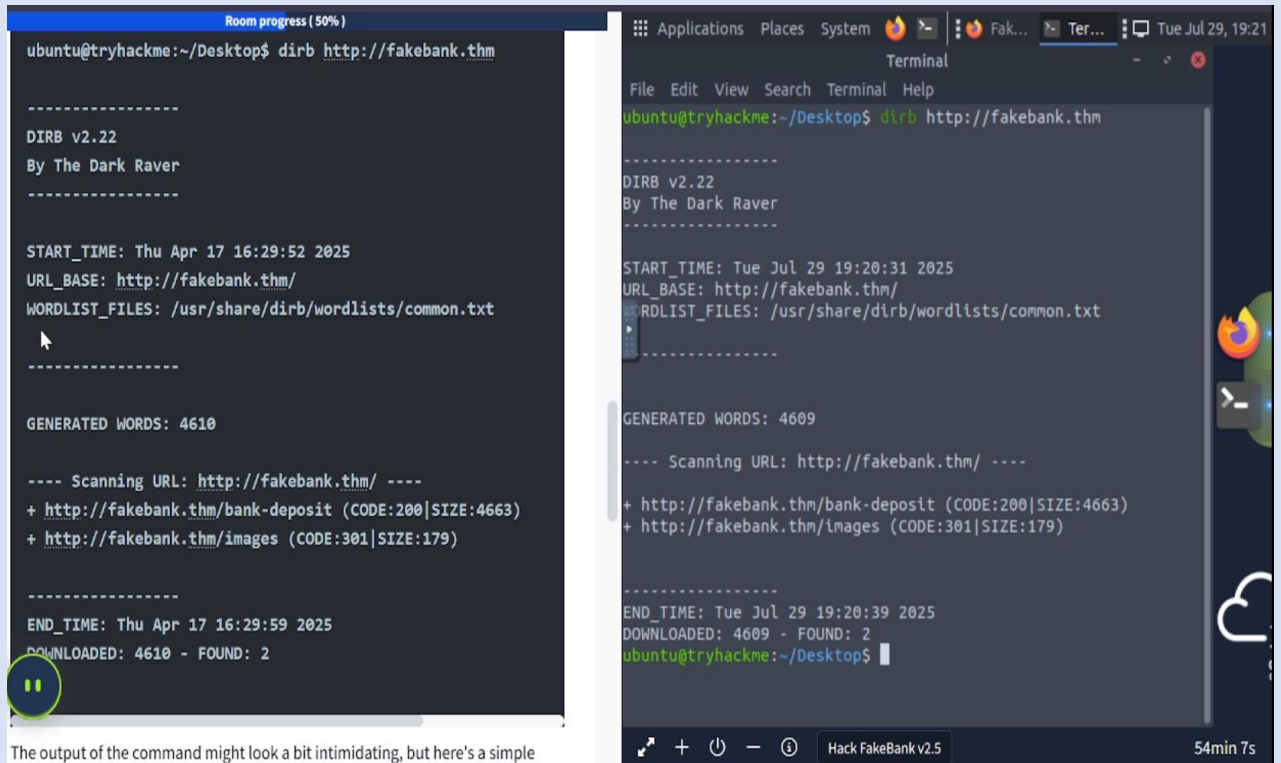
- TryHackMe Linux Terminal
- dirb command
- Fakebank Web application

Steps Taken:

- Identified the Fakebank website application vulnerable page



- Brute-forced the Fakebank website page URL



```
Room progress (50%)
ubuntu@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: 4610

---- 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: 4610 - FOUND: 2

The output of the command might look a bit intimidating, but here's a simple
```

```
Applications Places System Fak... Ter... Tue Jul 29, 19:21
Terminal
File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop$ dirb http://fakebank.thm

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

START_TIME: Tue Jul 29 19:20:31 2025
URL_BASE: http://fakebank.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

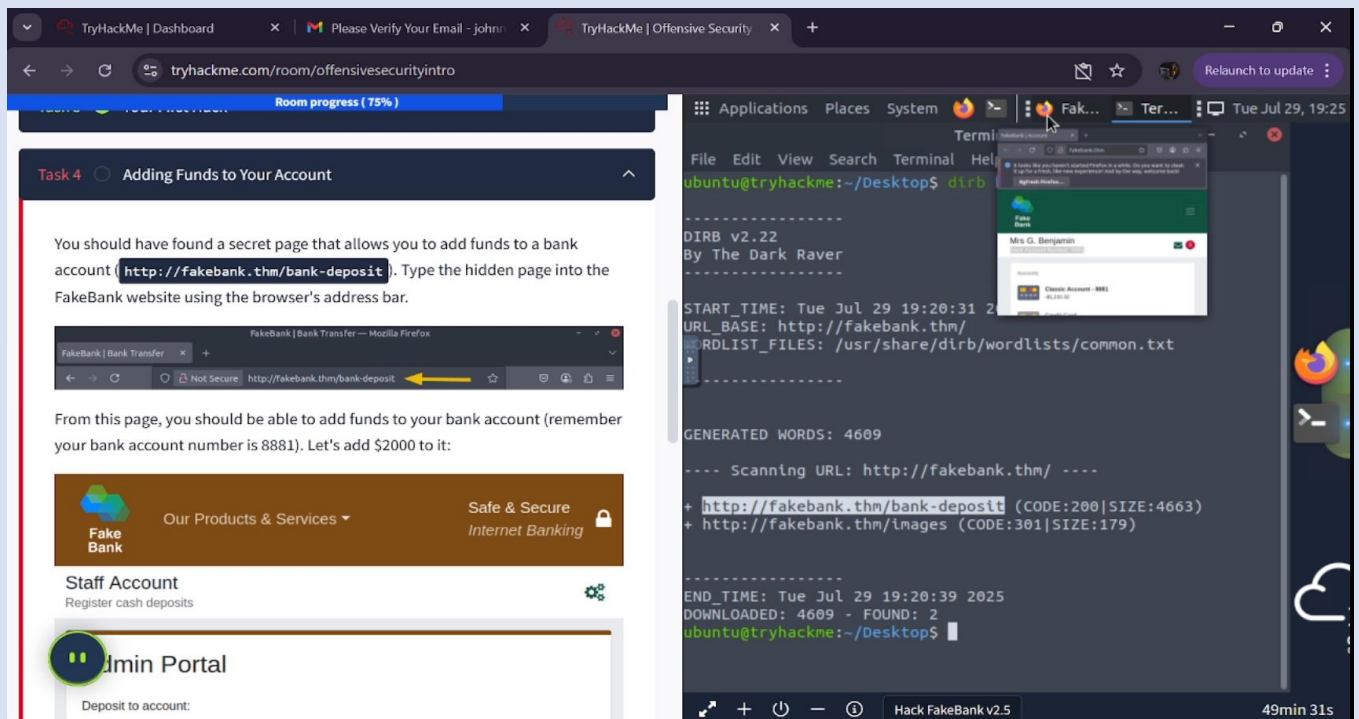
GENERATED WORDS: 4609

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

-----

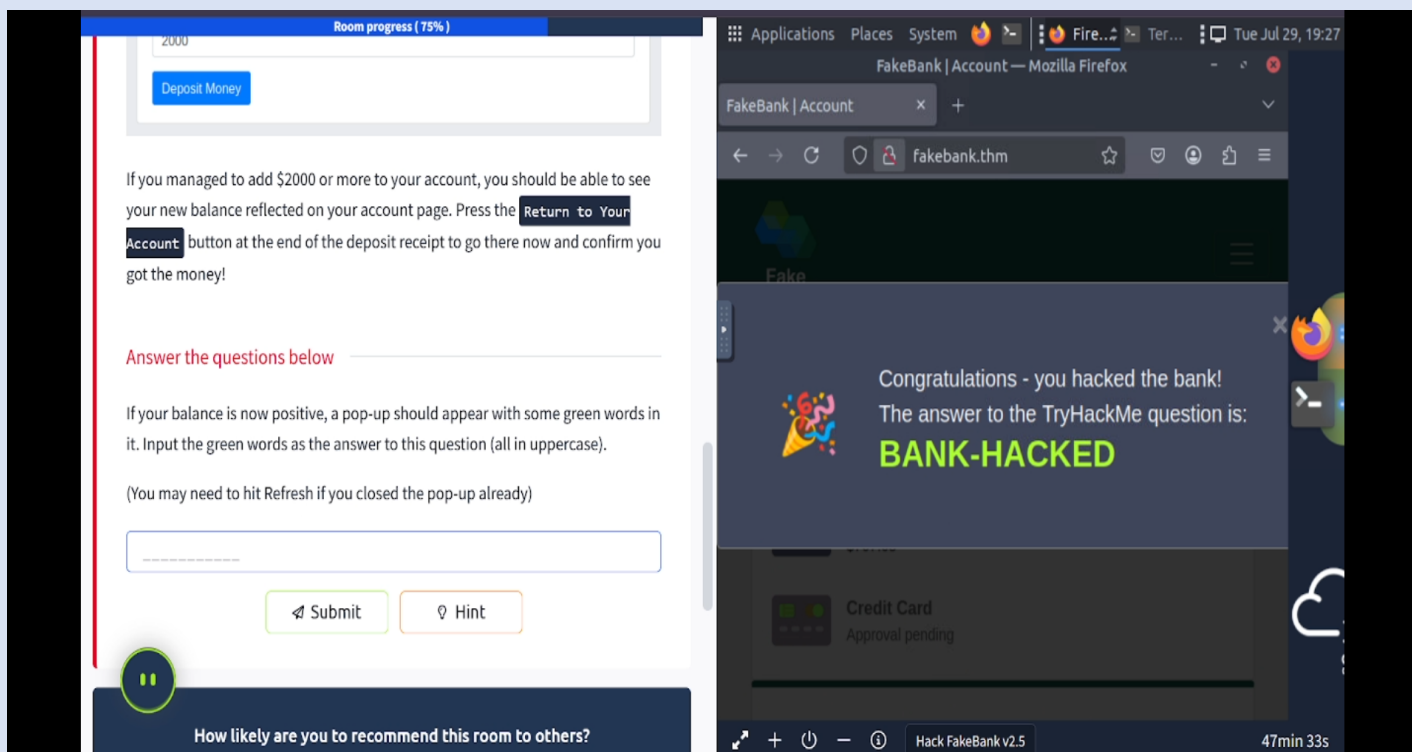
END_TIME: Tue Jul 29 19:20:39 2025
DOWNLOADED: 4609 - FOUND: 2
ubuntu@tryhackme:~/Desktop$
```

- Identified the hidden 'bank-deposit' page and transferred 2000 USD to my bank account



Flag(s):

- BANCK – HACKED



Lessons Learned:

- I successfully identified hidden vulnerable pages and demonstrated how they can be exploited, hence prompting the need to strengthen the web app security.

Room 2: Defensive Security Intro.

Summary:

- This room entails defensive security. It demonstrates how a special security team (Special Operations Center) can handle advances from malicious hackers.

Objective:

- To simulate defensive security through Security Information & Event Management (SIEM)

Tools Used:

- SIEM

Steps Taken:

- Used SIEM to demonstrate defensive security

The screenshot displays the TryHackMe interface for the 'Defensive Security Intro' room. The browser address bar shows the URL `tryhackme.com/room/defensivesecurityintro`. The room progress is indicated as 80% complete. On the left, there is a 'View Site' button and instructional text about navigating through the simulation. The right side of the interface features a dashboard with a pie chart showing 40% for 'Operations: Information', a bar chart comparing various countries (UK, US, Brazil, China, Russia, N. Korea), and an 'Alert Log' table.

Alert Log

Date	Message
undefined 7th 2025, 09:38:29:068	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
undefined 7th 2025, 09:35:12:103	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
undefined 7th 2025, 07:18:55:283	The user John Doe logged in successfully (Event ID 4624)
undefined 7th 2025, 07:18:30:223	Multiple failed login attempts from John Doe
undefined 7th 2025, 07:08:46:226	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

TryHackMe | Dashboard

Please Verify Your Email - johnn

TryHackMe | Defensive Security

tryhackme.com/room/defensivesecurityintro

Relaunch to update

Room progress (80%)

What's next?

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

Answer the questions below


What is the flag that you obtained by following along?

Submit

How likely are you to recommend this room to others?

you can proceed and implement the block rule. Block the malicious IP address on the firewall and find out what message they left for you.

https://firewall.internal



Firewall Block List

Block List	
Date	IP Address
July 2nd 2021, 13:27:00:948	101.34.37.231
June 30th 2021, 09:12:11:857	212.38.99.12
June 23rd 2021, 23:56:28:370	213.106.84.35

Block IP Address

Defensive Security

Flag(s):

- THM {THREAT – BLOCKED}

TryHackMe | Dashboard

Please Verify Your Email - johnn

TryHackMe | Defensive Security

tryhackme.com/room/defensivesecurityintro

Relaunch to update

Room progress (80%)

What's next?

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

Answer the questions below

What is the flag that you obtained by following along?

Submit

How likely are you to recommend this room to others?

A Day In the Life of a Junior (Associate) Security Analyst

Challenge Complete

You blocked the malicious IP address!

THM{THREAT-BLOCKED}

Defensive Security

Lessons Learned:

- I was able to enforce defensive security via SIEM

Room 3: Careers in Cyber

Summary:

This room entails a wide range of careers in Cybersecurity. In detail, a variety of scopes are outlined, and a personality-based quiz is included, which helps determine the appropriate career.

Objective:

- To explore cybersecurity career scopes and determine the best scope to venture into.

Tools Used:

- No tool(s) used

Steps Taken:

Security Analysts

Answer the questions below

Read about what a security analyst does.

No answer needed

🚩 Complete

Definition:

- These are professionals who are responsible for maintaining the overall security of an organization

Roles:

- They explore network systems to uncover and provide recommendations to security engineers
- They collaborate with a variety of stakeholders to conduct a holistic cybersecurity analysis in a given organization
- They develop actionable security plans and research zero-day attacks, tools, and trends to provide insights across all security teams

Security Engineers

Answer the questions below

Read about what a security engineer does.

No answer needed

🚩 Complete

Definition:

- These are professionals who are responsible for designing, monitoring, and maintaining security controls, networks, and systems to prevent cyberattacks

Roles:

- They test and screen security measures across systems, controls, and networks
- They monitor networks and update systems to lessen the potential impact of vulnerabilities
- They identify and implement systems needed for optimal security

Incident Responders

Answer the questions below

Read about what an incident responder does.

No answer needed

🚩 Complete

Definition:

- These are professionals who identify and mitigate risks while the attackers' operations are still unfolding.

Roles:

- They provide a thorough, actionable response plan
- They maintain robust security best practices and uphold incident response measures
- After the incident, they report and prepare for future attacks

Digital Forensic Examiners

Answer the questions below

Read about what a digital forensics examiner does.

No answer needed

🚩 Complete

Definition:

- These are professionals who are responsible for using digital forensics to investigate incidents and crimes.

Roles:

- They collect digital evidence while observing legal procedures
- They analyze evidence to find answers related to the case
- They document and file their findings

Malware Analysts

Answer the questions below

Read about what a malware analyst does.

No answer needed

🚩 Complete

Definition:

- These are professionals who analyze malware types to learn how they work and what they do.

Roles:

- They carry out static analyses of malicious programs, which are based on reverse engineering
- They conduct dynamic analyses of malware samples by observing their activities in a controlled environment
- They document and report all the findings

Penetration Testers

Answer the questions below

Read about what a penetration tester does.

No answer needed

🚩 Complete

Definition:

- These are professionals who are responsible for testing technology products for security loopholes.

Roles:

- They conduct tests on computer systems, networks, and web-based applications
- They perform security assessments, audits, and analyze policies
- They evaluate and report on insights, recommending actionable preventive steps

Red -Teamers

Answer the questions below

Read about what a red teamer does.

No answer needed

🚩 Complete

Definition:

- These are professionals who play the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.

Roles:

- They evaluate the role of a threat actor to uncover exploitable vulnerabilities, maintain access, and avoid detection
- They assess an organization's security controls, threat intelligence, and incident response procedures
- They evaluate and report on insights with actionable data for companies to avoid real-world instances

Career Quiz

The screenshot shows the TryHackMe website interface for a career quiz. The left sidebar lists tasks 1 through 9, with Task 9 'Quiz' selected. The main content area displays the quiz questions and a list of career roles: Penetration Tester, Security Analyst, Incident Responder, Red Teamer, and Security Engineer. The right sidebar provides detailed information for each role, including responsibilities and learning paths.

Task 1 Introduction

Task 2 Security Analyst

Task 3 Security Engineer

Task 4 Incident Responder

Task 5 Digital Forensics Examiner

Task 6 Malware Analyst

Task 7 Penetration Tester

Task 8 Red Teamer

Task 9 Quiz

This room has provided you with a general overview of the different careers in cyber security. Don't forget that you can [leverage online training to land your dream job](#) in cyber security. To find out which cyber security role suits you best, try our fun quiz, which you can access by clicking the "View Site" button on the right.

[View Site](#)

Answer the questions below

Complete the careers quiz and share your chosen job!

No answer needed [Correct Answer](#)

Created by tryhackme strategos

Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)

Users in Room 949,648

Created 1205 days ago

Penetration Tester

Responsible for testing technology products for security loopholes.

Security Analyst

You may see penetration testing referred to as pentesting and ethical hacking. A penetration tester's job role is to test the security of the systems and software within a company - through attempts to uncover flaws and vulnerabilities through systemised hacking. Penetration testers exploit these vulnerabilities to evaluate the risk in each instance. The company can then take these insights to rectify issues to prevent a real-world cyber attack.

Incident Responder

Red Teamer

Security Engineer

PRE SECURITY

JR PENETRATION TESTER

OFFENSIVE PENTESTING

Flag(s):

- No Flag(s) captured

Lessons Learned:

- I successfully explored cybersecurity careers and discovered that I can pursue the Pentester scope.