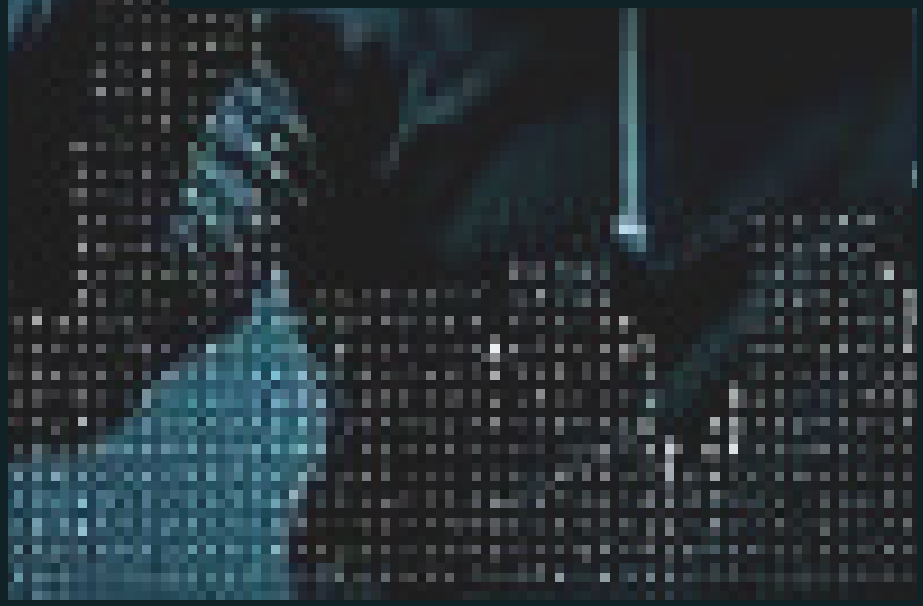
Vijay B & Swathi

Overall Report

# Cyber Security



2023

UNDER THE GUIDENCE OF

eduphoniex solution

# Table of content



- **Hackers breached almost 4 million records in March 2022. (Source: IT Governance) As of March 2022, there were 88 publicly disclosed cybersecurity cases. This resulted in 3,987,593 breached records. For the entire first quarter of 2022, a total of 75,099,482 records were breached.**

PHOENIX SOLUTIONS
LET'S SHINE TOGETHER


# BRUTE FORCE ATTACK

Brute force attacks represent a significant threat to the security of digital systems and networks in the realm of cybersecurity. These attacks involve the systematic and exhaustive trial of all possible combinations to gain unauthorized access to protected information, systems, or encrypted data. By leveraging computational power and automation, attackers aim to exploit vulnerabilities in passwords, encryption keys, or authentication mechanisms.

This report provides an overview of brute force attacks, including their methods, implications, and countermeasures. By gaining insight into these aspects, individuals and organizations can strengthen their defenses, safeguard their sensitive information, and prevent unauthorized access.

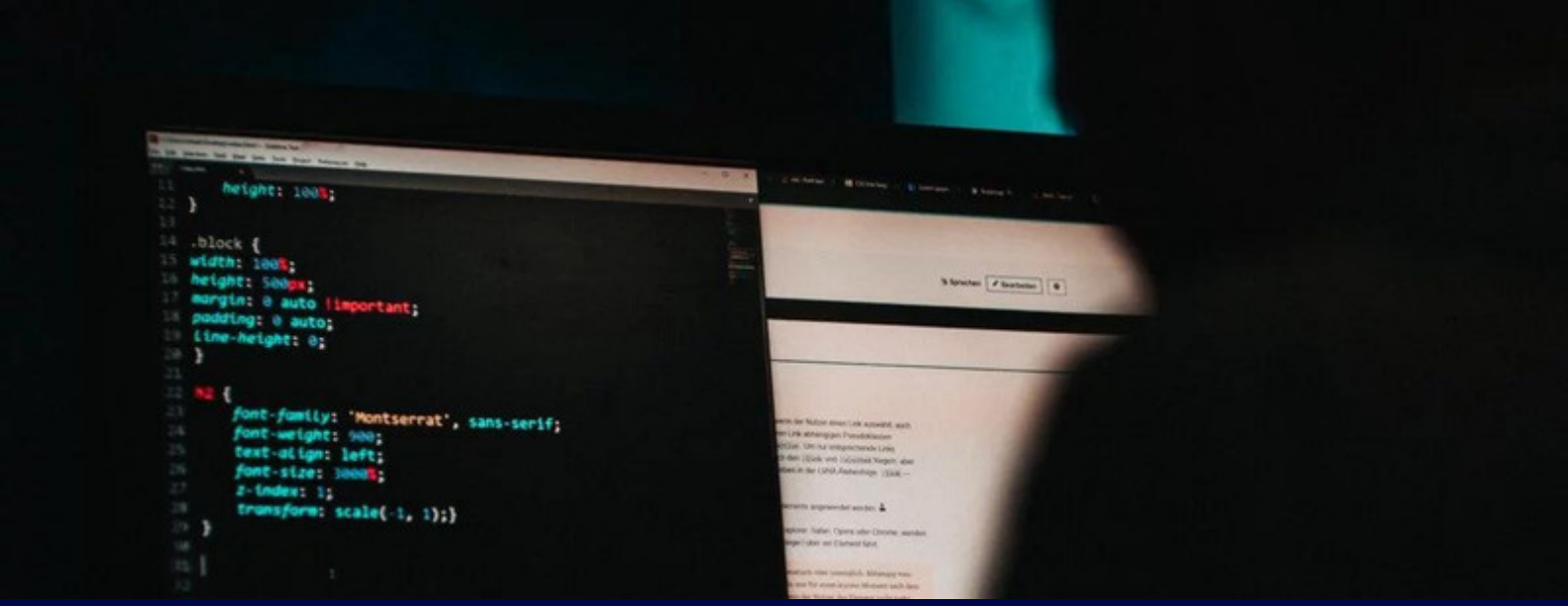
# Understanding Brute Force Attacks

Understanding brute force attacks is essential in the realm of cybersecurity to effectively protect systems, networks, and sensitive information. Brute force attacks are a method employed by malicious actors to gain unauthorized access by systematically trying all possible combinations until the correct solution is discovered.

The fundamental concept of a brute force attack involves exhaustive trial-and-error attempts. Attackers systematically generate and test different combinations, such as passwords or encryption keys, until they find the correct one. This method relies on the assumption that the correct solution exists within the search space and can be found through systematic enumeration.

Brute force attacks can target various security mechanisms, including passwords, encryption algorithms, or authentication systems. Attackers exploit vulnerabilities in these mechanisms, aiming to breach the defenses of a target and gain unauthorized access.

## How a Basic Brute Force Attack Works



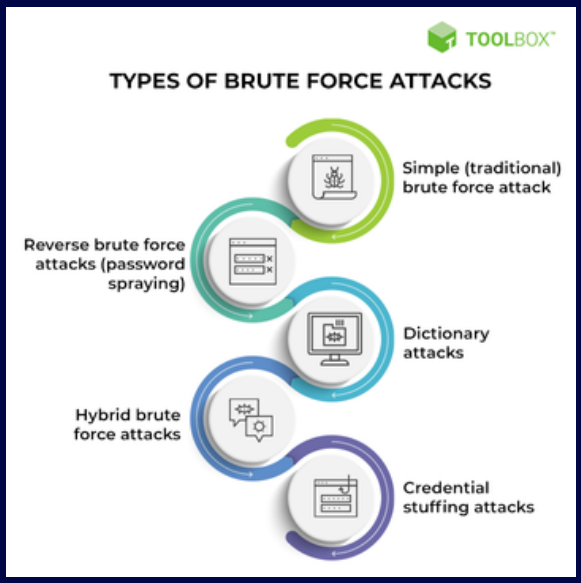
# Types of Brute Force Attacks:

- Password Cracking: Attackers attempt to guess passwords by systematically trying different combinations until they find the correct one. They exploit weak or poorly protected passwords to gain unauthorized access to user accounts or systems.

- Cryptanalysis: Brute force attacks can be used to break encryption by trying all possible keys until the correct one is discovered. This method aims to compromise the confidentiality and integrity of encrypted data.

- Network Attacks: Attackers may target network protocols and services by attempting various username and password combinations. They exploit weaknesses in network authentication mechanisms to gain unauthorized access to network devices or sensitive information.

- Application Attacks: Brute force techniques can be employed to target web applications or software with authentication mechanisms. Attackers systematically test different login credentials to gain unauthorized access or exploit vulnerabilities in the application.



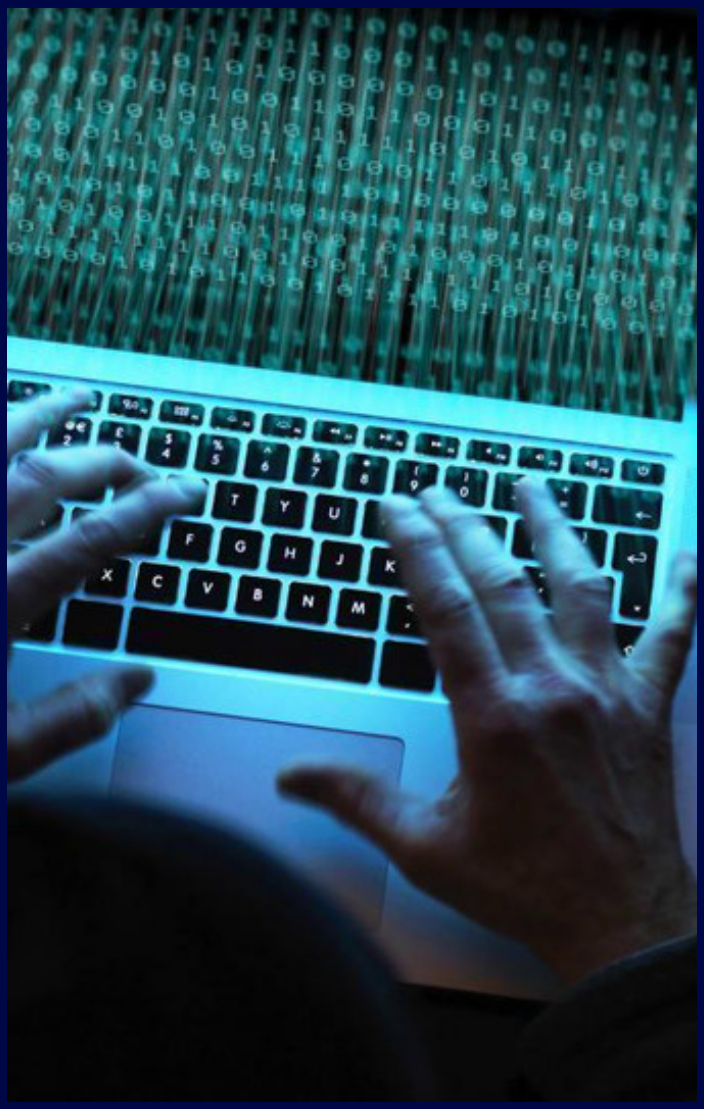

Brute force attacks utilize various techniques and tools to systematically try all possible combinations and gain unauthorized access. Here are some common techniques and tools employed in brute force attacks:

# Techniques and Tools

1. Exhaustive Search
2. Dictionary Attacks
3. Hybrid Attacks:
4. Rainbow Tables:
5. Specialized Tools and Software:

# Fake Banking using Brute Force

It's important to note that fake banking systems themselves are illegal and unethical. Engaging in such activities, whether it involves brute force attacks or any other means, is against the law and can lead to severe legal consequences.



Fake banking using brute force would refer to a scenario where an attacker employs brute force techniques to gain unauthorized access to a fraudulent or fake banking system. In this context, the attacker would systematically try various combinations of usernames and passwords until they find the correct credentials to access the fake banking platform

# Steps to hack a fake bank

we were given a task to hack a fictious/fake bank it was controlled exercise in a simulated environment with the intention of testing cybersecurity defenses, then it can be considered a legitimate and educational activity.

---

Click the "Start Machine" button. Once loaded in Split View in your browser, you will have access to a machine you'll use to hack a fake bank application called FakeBank.

# 1.STEP

## Open a terminal

A terminal, also known as the command-line, allows us to interact with a computer without using a graphical user interface. On the machine, open the terminal using the Terminal icon:

# 2.STEP

## Find hidden website pages

Most companies will have an admin portal page, giving their staff access to basic admin controls for day-to-day operations. For a bank, an employee might need to transfer money to and from client accounts. Often these pages are not made private, allowing attackers to find hidden pages that show, or give access to, admin controls or sensitive data.

Type the following command into the terminal to find potentially hidden pages on FakeBank's website using GoBuster (a command-line security application).

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

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

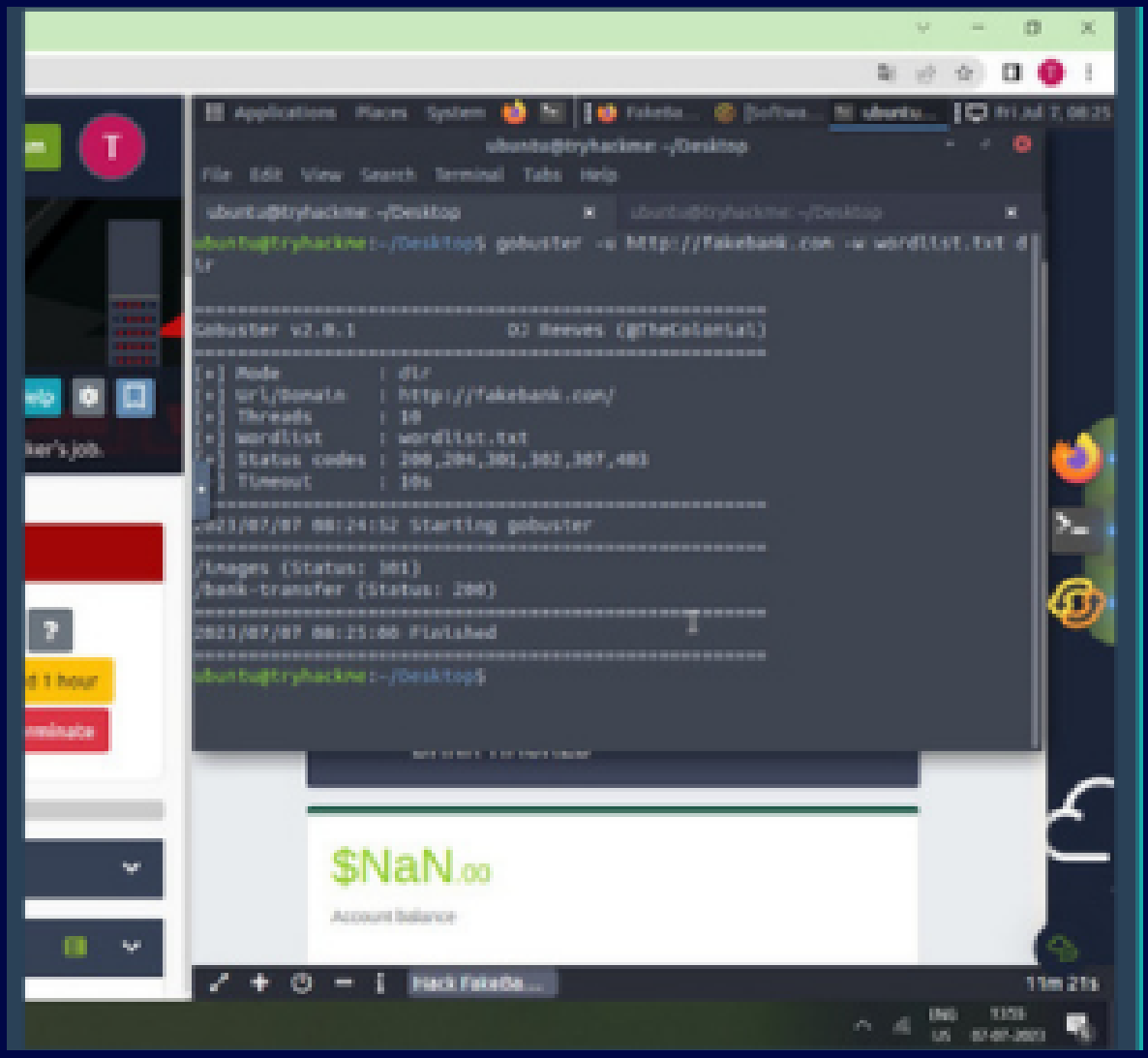
```
  -x string
        File extension(s) to search for (dir mode only)
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordl
ist.txt dir

===============================================================
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
===============================================================
2023/07/07 07:42:12 Starting gobuster
===============================================================
/images (Status: 301)
/bank-transfer (Status: 200)
===============================================================
2023/07/07 07:42:21 Finished
===============================================================
ubuntu@tryhackme:~/Desktop$ ^C
ubuntu@tryhackme:~/Desktop$
```

# 3.Step

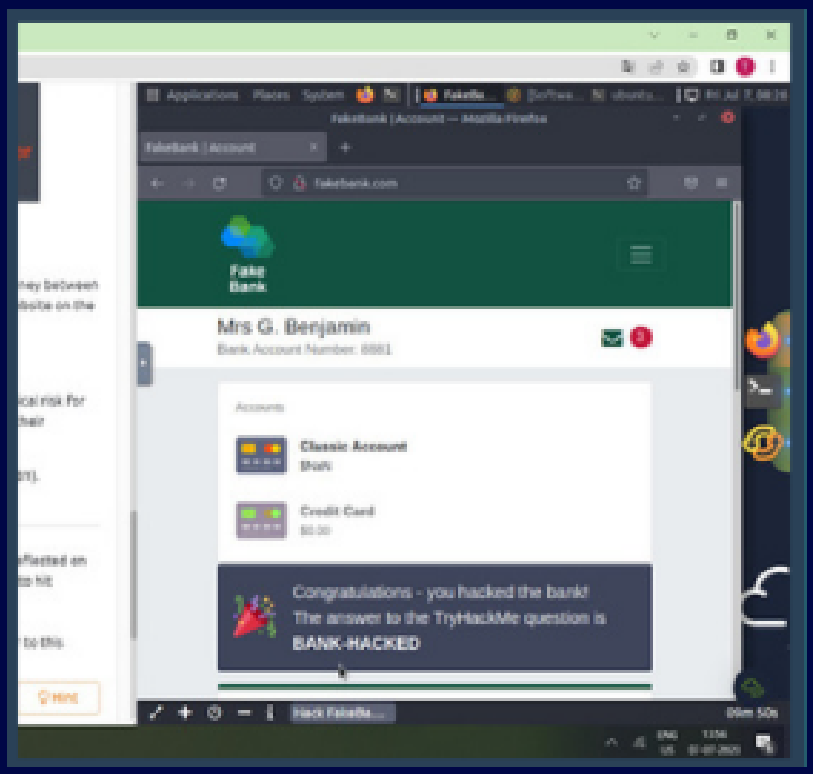
## Hack the bank

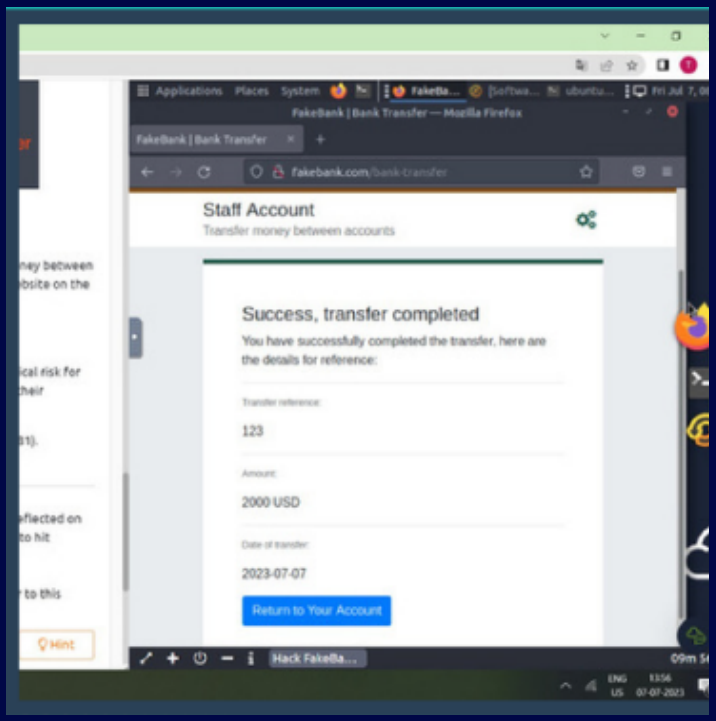
**You should have found a secret bank transfer page that allows you to transfer money between accounts at the bank (/bank-transfer). Type the hidden page into the FakeBank website on the machine.**

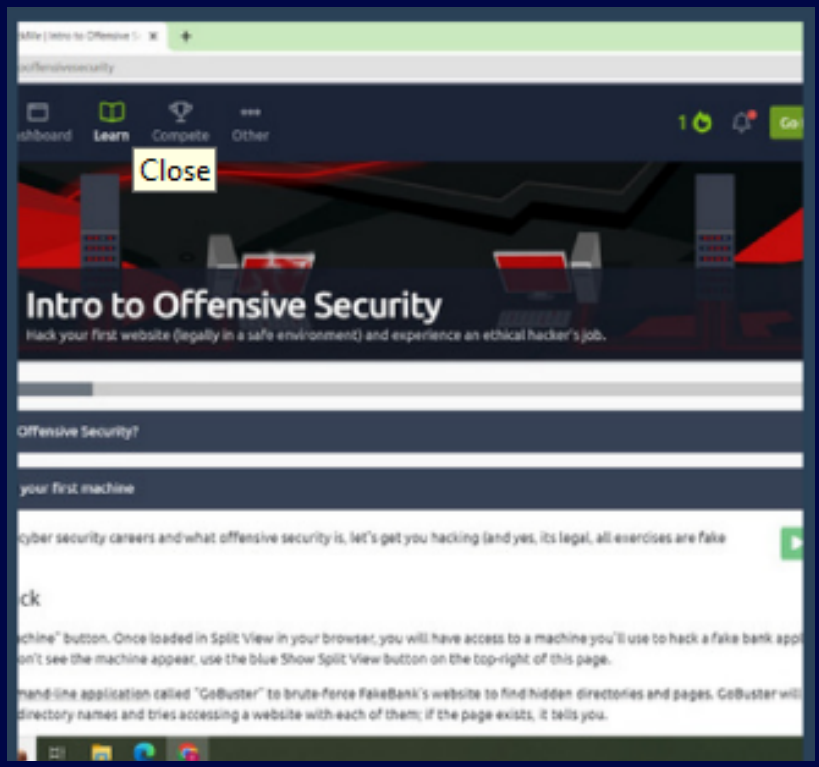



Having found a hidden page on the FakeBank website, specifically for bank transfers (/bank transfer), we were able to initiate a transfer of $2000 from account 2276 to my account 8881. It is important to note that these actions were conducted for demonstration purposes within the context of uncovering vulnerabilities and should not be replicated in real-life situations without proper authorization and legal consent.

# SCREENSHOTS



# OVERVIEW

During my internship, I had the chance to deepen my understanding of various concepts and principles in cyber security. Through training sessions, workshops, and hands-on projects, I learned about topics such as network security, cryptography, ethical hacking, risk assessment, and incident response. This knowledge enhancement has provided me with a strong foundation in cyber security practices.

Guidance and Mentorship:
I greatly appreciate the guidance and mentorship provided during my internship. The experienced professionals in the organization were readily available to answer my questions, provide feedback, and offer valuable insights. Their expertise and willingness to share their knowledge significantly contributed to my learning and professional growth.

The internship provided a valuable glimpse into the industry's current trends, challenges, and best practices in cyber security.

# CONCLUSION

I am grateful for the guidance and mentorship provided by experienced professionals in Eduphoenix Solutions who were always willing to support and share their expertise. Their advices  and feedback have been helpful in my learning and professional growth.

In conclusion, my internship experience in the field of cyber security has been extremely valuable and rewarding. I had the opportunity to acquire knowledge and practical skills that are highly relevant in the ever-evolving landscape of cyber security.