YoungDev Interns

YoungDevInterns

Internship Tasks Report

Part of : **Cyber Security Internship**

Prepared By

Muhammad Izaz Haider

~Sudo-Master~~Izaz

Paper Due Date

15 April 2025

Table of Contents

1: Introduction

Cybersecurity begins with mastering foundational practices that protect systems from potential threats. This report presents a detailed walkthrough of three essential tasks that are part of my internship under the *YoungDevInterns_Cyber Security* program. Each task contributes to building core cybersecurity habits from configuring firewalls to using secure password management tools, and identifying phishing attempts.

Throughout these tasks, I engaged in hands-on activities to enhance my understanding of practical security implementations. Whether it was blocking unwanted ports with a firewall, managing credentials securely, or spotting suspicious email indicators, each task reinforced real-world cybersecurity skills. This experience not only improved my technical capabilities but also highlighted the importance of documentation, reporting, and awareness in professional environments.

2. Lab Objectives

This Basic Tasks ab focused on achieving the following objectives:

- **Task 1:** Configure a Basic Firewall
- **Task 2:** Implement a Password Manager
- **Task 3**: Recognize and Handle Phishing Emails

5. Tools and Environment

To perform and complete the assigned tasks successfully, I utilized the following tools and platforms:

- **Laptop/PC**
  For performing all the tasks and configurations.
- **Internet Access**
  Required for tool installations, research, and uploading reports.
- **Web Browser**
  Used to access GitHub, install extensions, and explore phishing examples.
- **Windows Defender Firewall**
  To configure and test firewall rules.
- **Bitwarden (Password Manager)**
  For storing and generating strong passwords securely.
- **Email**

  To identify and analyze phishing email.
- **Note-taking Application (e.g., Notepad or Word)**
  For documentation and preparing the final report.

Part 1: Set Up Basic Firewall Rules

In this task, I focused on configuring firewall rules to enhance security on a personal computer. Specifically, I utilized **Windows Defender Firewall** to control incoming and outgoing network traffic based on predefined security rules. Setting up these rules helps in protecting the computer from unauthorized access and attacks.

Step 1: Open Windows Defender Firewall

- To begin, I opened the **Control Panel** and clicked on **Windows Defender Firewall**.
- From the left panel, I selected **Advanced Settings** to configure inbound and outbound rules.

Step 2: Create a New Firewall Rule

- Under **Inbound Rules**, I clicked on **New Rule** to create a custom rule.
- I selected **Program** and browsed to the executable file (e.g., notepad.exe) to block access.
- For **Outbound Rules**, I followed the same steps to set up restrictions for outgoing traffic.

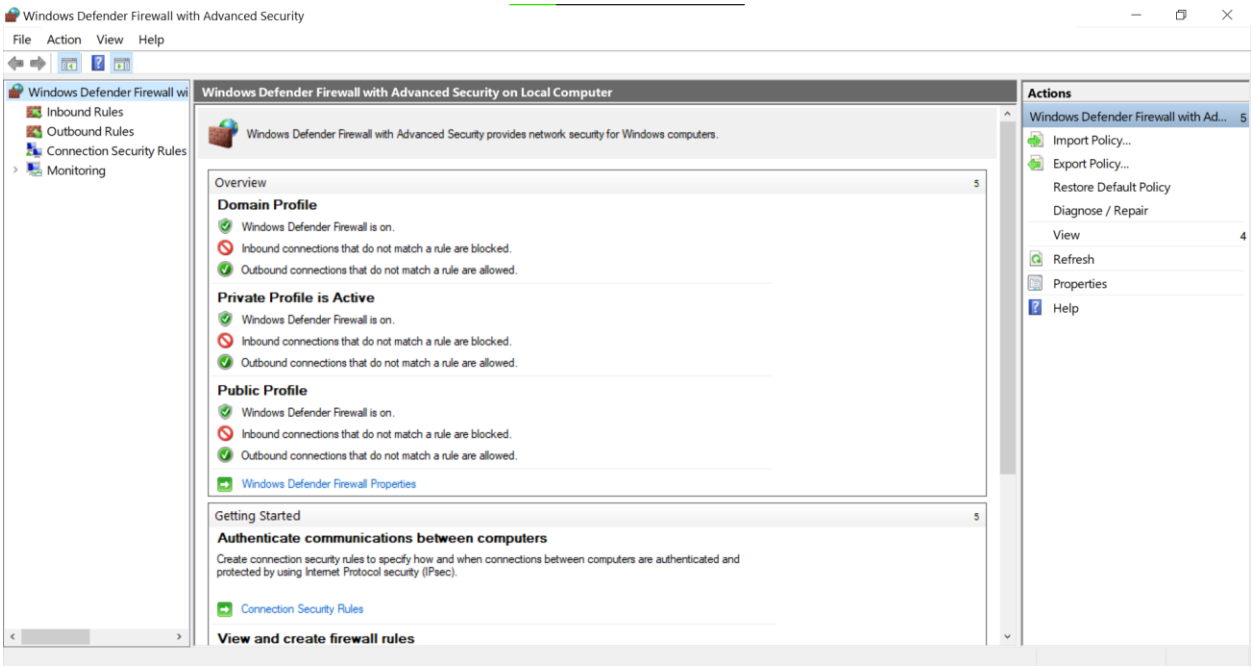
Step 3: Blocking Specific Ports

- In the **New Rule** wizard, I selected **Port** and specified a port number (e.g., 80 for HTTP).
- I chose to **Block the connection** for this specific port to prevent unauthorized access.
-

Step 4: Save and Test the Rules

- After creating the rules, I saved the configurations and tested them by attempting to access the blocked program or port.

Screenshot:



Summary

Through this task, I successfully set up basic firewall rules on a personal computer using Windows Defender Firewall. This task provided me with a hands-on understanding of configuring rules to block or allow specific applications or ports, which is a fundamental aspect of network security.

Task 2: Use a Password Manager

In this task, I focused on setting up and using a **password manager** to securely store and manage passwords. Password managers help ensure that passwords are complex, unique, and stored securely, which is crucial for maintaining privacy and security in the digital world.

Step 1: Install a Password Manager

- First, I selected **Bitwarden** as my password manager and installed it on my computer by visiting their official website.
- I followed the simple installation process for **Windows**, which involved downloading the installer and running it.

Step 2: Set Up and Create an Account

- After installation, I created an account on Bitwarden by providing an email address and a strong master password.
- This master password will be the only one I need to remember, and it will unlock access to all the other stored passwords.

Step 3: Add Passwords to the Manager

- I started adding passwords to my Bitwarden vault by clicking the **Add Item** button and inputting login details for various accounts.

Step 4: Generate Strong Passwords

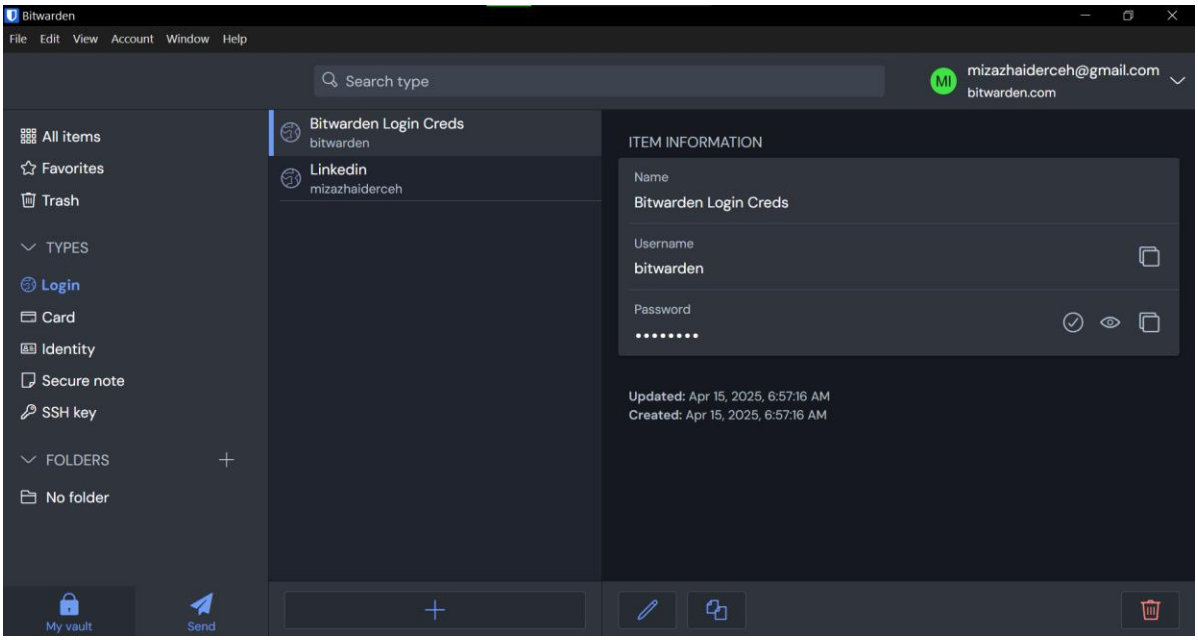
- Using the password generator feature of Bitwarden, I created strong, random passwords for my accounts.

- These passwords are complex, containing a mix of uppercase and lowercase letters, numbers, and special characters.

Step 5: Use Autofill for Password Management

- I enabled the **Autofill** feature in Bitwarden's browser extension, which allows the manager to automatically fill in login details for websites and apps.
- This saves time and ensures that I am always using the correct password without manually typing it.

Screenshot:



Summary

This task was a valuable learning experience, as it showed me how to securely store and manage passwords using a password manager. By using **Bitwarden**, I ensured that my passwords are complex, unique, and stored securely. The ability to generate strong passwords and autofill login details helps streamline my online security and makes password management much easier.

Task 3: Identify Phishing Emails

In this task, I learned how to recognize and handle **phishing emails**, which are deceptive attempts to obtain sensitive information, such as login credentials or personal data, by pretending to be from a trusted source. Identifying phishing emails is crucial in preventing security breaches and protecting personal and organizational data.

Step 1: Understand the Common Signs of Phishing Emails

- **Suspicious Links**: Phishing emails often contain links that look legitimate at first glance but actually redirect you to fraudulent websites. I learned to hover over links before clicking them to check the actual URL.
- **Urgent Requests**: Phishing emails frequently use urgent language, pressuring the recipient to act quickly, such as claiming that your account will be locked unless you immediately reset your password.
- **Strange Email Address**: The sender's email address might look similar to a legitimate one, but it usually contains small discrepancies, such as missing letters or additional characters.
- **Grammatical Errors**: Many phishing emails contain poor grammar, spelling mistakes, and awkward sentence structures. This is a key indicator of fraudulent communication.

Step 2: Examine a Sample Phishing Email

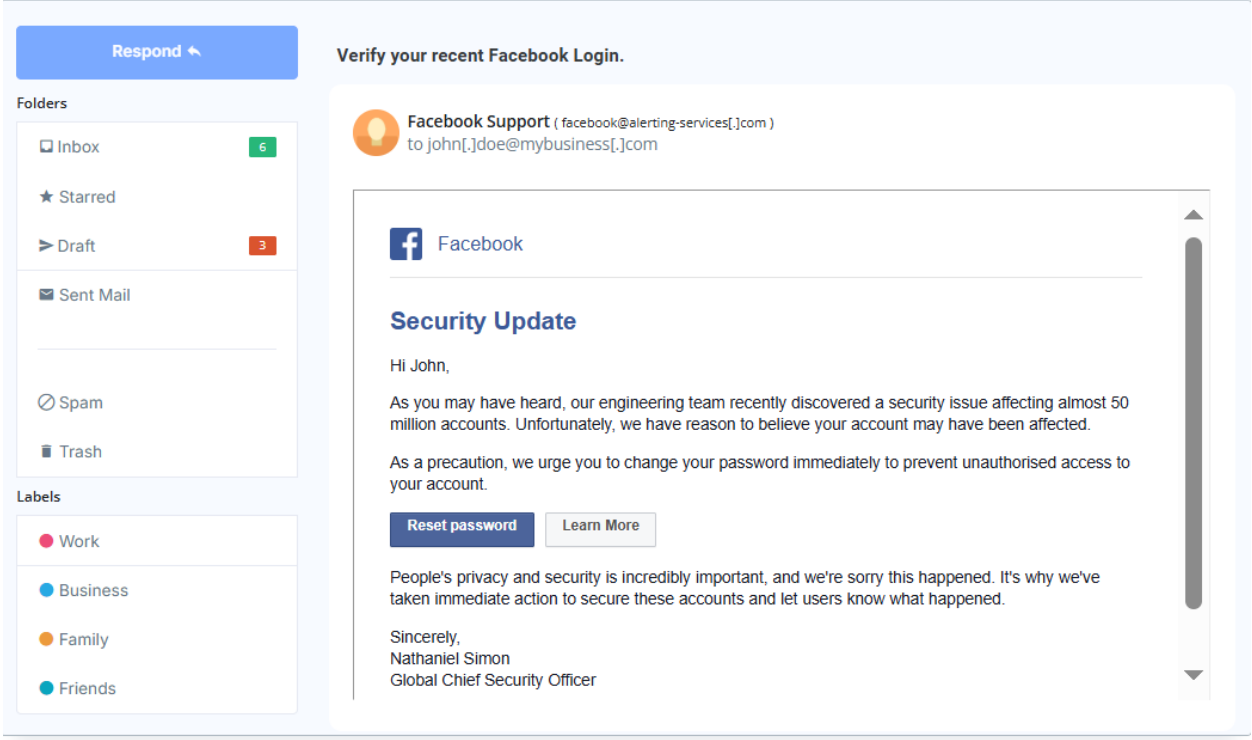
- I reviewed a sample phishing email to apply the signs of phishing that I had learned. The email contained the following characteristics:

- A fake request for login credentials, claiming to be from Facebook’s security team.
- A link that appeared legitimate at first glance (e.g., "Reset password"), but upon hovering over it, redirected to a suspicious domain.
- The email used a generic greeting ("Hi John") rather than a personalized one, making it less authentic.
- Urgent language requesting immediate action ("change your password immediately to prevent unauthorized access to your account"), creating a sense of panic.
- A signature from a supposed security officer ("Nathaniel Simon, Global Chief Security Officer") to make the email appear more credible. account suspension.

Step 3: Report the Phishing Attempt

- Upon identifying the phishing email, I reported it to my email provider and moved it to the **Spam** or **Junk** folder.
- I also ensured to delete any email that attempted to harvest sensitive information, ensuring my device remained secure.

Screenshot:



Summary

This task taught me to recognize the various signs of phishing attempts and how to handle them appropriately. By carefully examining email content, links, and sender information, I can prevent falling victim to these malicious tactics. In this digital age, it's essential to stay vigilant and be cautious when handling emails, especially when they involve sensitive information.

Key Learnings and Observations from All Tasks

Throughout the completion of these tasks, I have gained valuable knowledge and practical experience in core cybersecurity practices, which will help in both personal and professional growth in the cybersecurity field. Here are the key learnings and observations from each task:

Task 1: Set Up Basic Firewall Rules

- **Learning Outcome**: Configuring firewall settings is a fundamental task in protecting personal computers from unauthorized access. I learned how to enable and configure Windows Defender Firewall and set custom rules to allow or block specific applications or ports.
- **Real-World Application**: Understanding firewall rules is crucial for preventing unauthorized network traffic and defending against external attacks.
- **Observation**: The process is relatively straightforward, but it requires attention to detail, especially when configuring rules for specific applications or ports.

Task 2: Use a Password Manager

- **Learning Outcome**: I learned the importance of using a password manager to store and generate strong, unique passwords for various accounts. Installing tools like LastPass

or Bitwarden helped me realize the value of keeping sensitive information secure and easily accessible.

- **Real-World Application**: Password managers are essential in reducing the risk of password reuse and improving overall account security. This is a critical practice, especially as we manage more accounts online.
- **Observation**: Using a password manager significantly reduces the stress of remembering multiple passwords, and it also ensures that passwords are strong and encrypted.

Task 3: Identify Phishing Emails

- **Learning Outcome**: This task taught me how to identify common signs of phishing emails, such as suspicious links, urgent requests, and email address discrepancies. By understanding these signs, I can prevent myself from falling victim to phishing attacks.
- **Real-World Application**: Phishing remains one of the most common cybersecurity threats, and being able to identify phishing attempts is essential for protecting personal and organizational data.
- **Observation**: The key takeaway from this task is the importance of vigilance when reading emails and always verifying sources before interacting with any links or attachments.

My Reflections and Experience from the Internship

This internship has been an incredible learning experience, providing me with hands-on tasks that deepened my understanding of cybersecurity. From configuring firewall rules to identifying phishing emails, I gained practical skills that I can apply in real-world situations.

Key Learnings:

- **Real-World Applications**: I gained valuable experience using tools like Windows Defender Firewall, LastPass, and Bitwarden, which enhanced my technical skills and confidence.
- **Cyber Hygiene**: Tasks like password management and phishing email identification emphasized the importance of personal cybersecurity practices.
- **Problem-Solving**: While some tasks were challenging, they helped me develop a critical thinking approach and attention to detail.

This internship not only boosted my technical knowledge but also improved my communication and reporting skills. It has solidified my passion for cybersecurity, and I look forward to applying what I've learned in my future career.

Conclusion

In conclusion, this internship has been a valuable journey in strengthening my understanding of fundamental cybersecurity practices. By completing tasks like setting up firewall rules, using a password manager, and identifying phishing attempts, I've gained practical skills that are essential for any cybersecurity professional. These experiences have not only deepened my technical expertise but have also emphasized the importance of maintaining a proactive approach to digital security.

As I move forward in my career, I will continue to build on these foundations, applying the knowledge and skills I've acquired to real-world scenarios and further advancing in the field of cybersecurity.