YoungDev Interns

Internship Tasks Report

- **Prepared By:** Muhammad Izaz Haider
- **Assigned by:** YoungDev Interns
- **Given Tasks:** 3
- **Part of :** Information Security Intern
- **Date :** 15 April 2025

~Sudo-Master~㉿~Izaz

Table of Contents

1. Introduction to Intermediate Cybersecurity Tasks

Cybersecurity is an ever-evolving field that requires continuous learning and practical engagement with real-world scenarios. This report highlights the intermediate-level tasks undertaken as part of my internship with the **YoungDevInterns_Cyber Security** program. These tasks represent the next step beyond foundational skills, focusing on more hands-on experience with tools and strategies used by professionals to secure systems and networks.

During this phase of the internship, I worked on conducting vulnerability scans, implementing two-factor authentication (2FA), and analyzing network traffic. Each task provided valuable insights into how real-world cybersecurity operations are carried out. From identifying system weaknesses to observing the flow of data through a network, these activities helped sharpen both my technical and analytical skills.

2. Internship Objectives – Intermediate Level

This phase of the internship aimed to deepen technical proficiency and cybersecurity awareness through practical, tool-based activities. The specific objectives of the Intermediate Level tasks included:

- **Task 1:** Perform a Basic Vulnerability Scan using tools like Nmap or OpenVAS.
- **Task 2:** Implement Two-Factor Authentication (2FA) across personal or test accounts.
- **Task 3:** Analyze Network Traffic using packet analysis tools such as Wireshark.

3. Tools, Platforms, and Environment

To successfully complete the intermediate-level tasks assigned during my internship, I used the following tools, platforms, and resources. Each played an essential role in performing the tasks efficiently and gaining hands-on experience with real-world cybersecurity practices

- **Laptop/PC**
  Used for running security tools, analyzing network traffic, and documenting findings.
- **Stable Internet Connection**
  Essential for downloading tools, researching vulnerabilities, and uploading reports to GitHub and social media platforms.
- **Web Browser**
  Accessed for setting up 2FA, exploring tutorials, and managing online platforms such as LinkedIn, Facebook, and GitHub.
- **Nmap**

  Used for performing vulnerability scans to identify weaknesses in systems and networks.
- **Wireshark**
  Employed to capture and analyze network packets and study traffic patterns.
- **Note-taking Application (e.g., Notepad, Word, or Google Docs)**
  Used to maintain task logs, write reflections, and prepare the final report.

Task 1: Perform a Basic Vulnerability Scan

In this task, I focused on scanning a target system to detect known vulnerabilities using Nmap, a powerful and widely-used network scanning tool. This type of scan helps identify potential security issues, such as outdated software, exposed services, and misconfigurations, which could be exploited by attackers.

Step 1: Install Nmap

- I downloaded and installed **Nmap** from the official website: https://nmap.org.
- Optionally, I also installed **Zenmap**, the graphical interface for Nmap, for a more user-friendly experience.

Step 2: Identify Target IP Address

- I selected a target system within my own network (e.g., metaspoitable 2) to scan.
- I ensured I had full permission to scan this system, respecting ethical hacking principles.

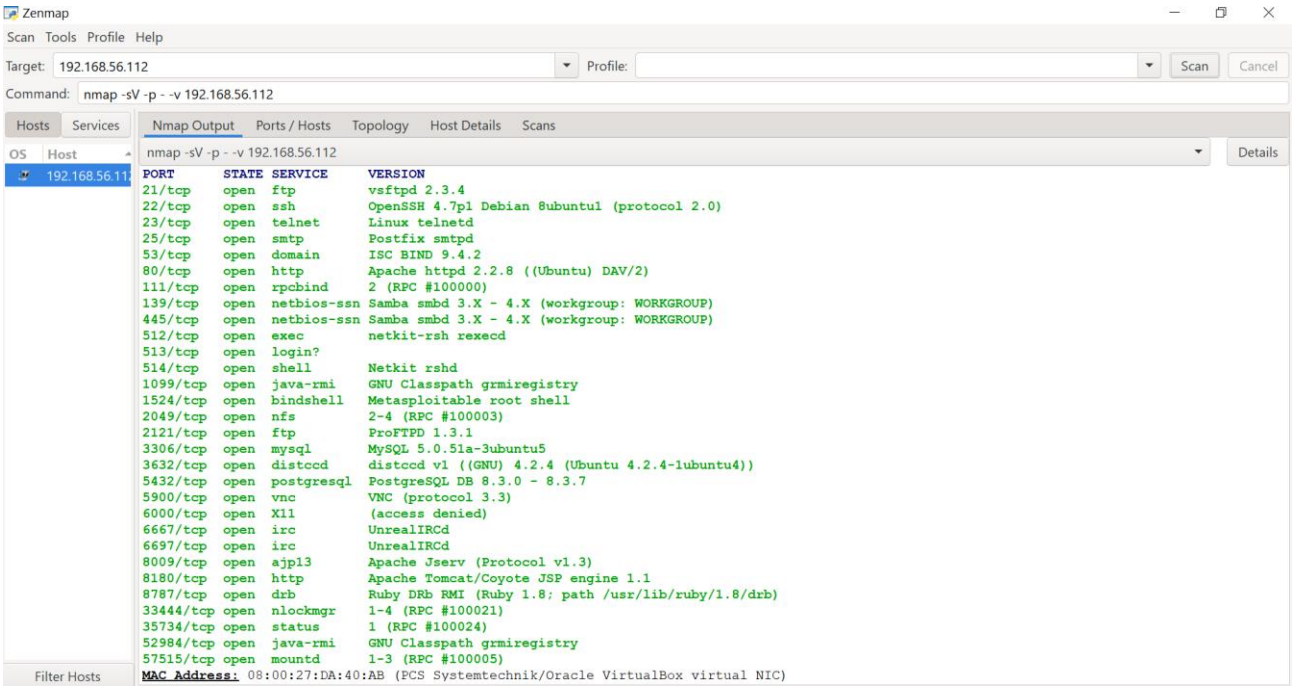
Step 3: Perform a Basic Port and Service Scan

- I started with a simple port scan to discover all open ports and services:

Command: nmap -p- -sV 192.168.56.112 -v

  - -p- performs full ports scan.
  - -sV enables service and version detection.

- -v enables to see live what's going on

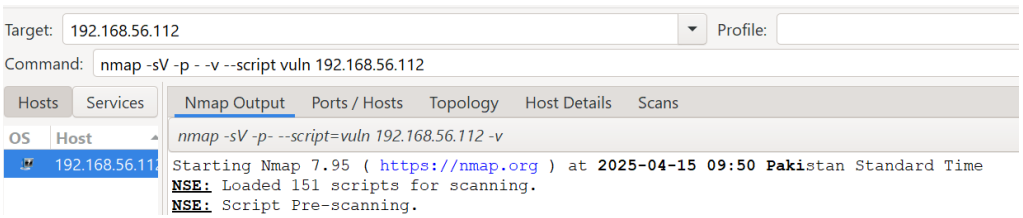


Step 4: Perform a Vulnerability Scan Using NSE Scripts

- To detect vulnerabilities, I used Nmap's scripting engine (NSE) with the following command:

Command: nmap -sV -p- --script=vuln 192.168.56.112 -v

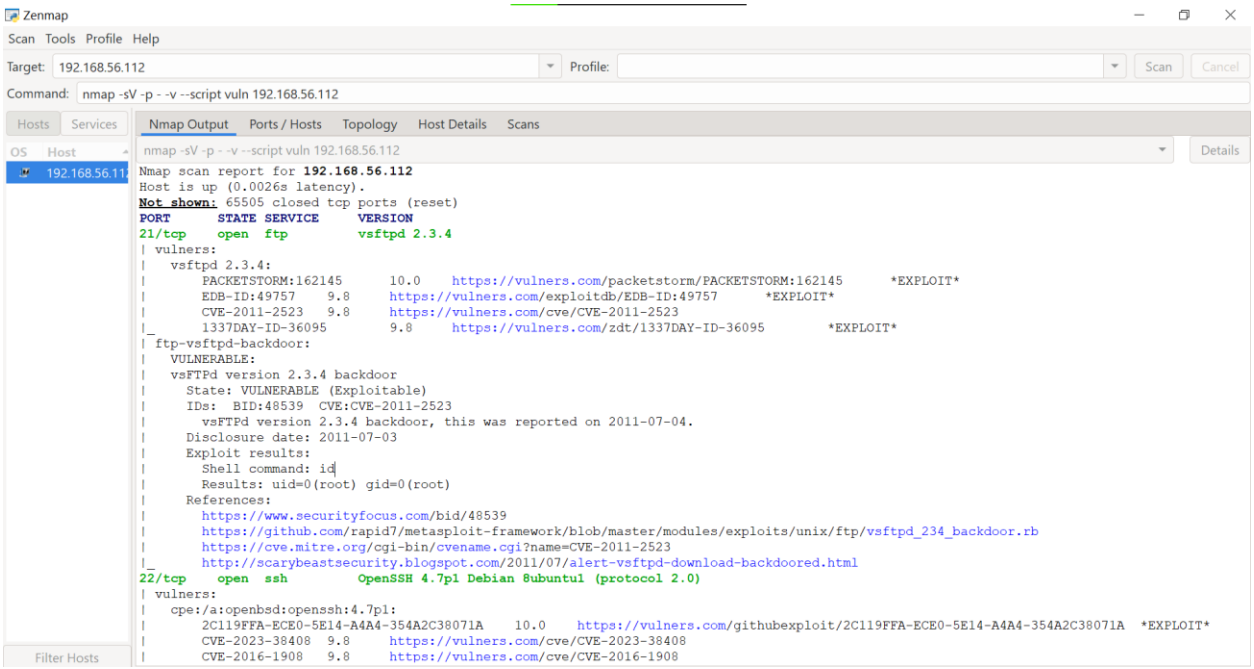
- This runs all vulnerability-related scripts available in Nmap's library.
- It checks for issues like CVEs, weak configurations, and outdated services.
- –script=vuln scan and find vulnerbailites
- - v enables to see live what's going on



Step 5: Review and Analyze Results

- I carefully read through the scan report generated by Nmap.
- Each vulnerability result included a **risk summary**, possible **CVEs**, and **remediation advice**.
- I documented any critical or high-risk findings for further study and learning.

Screenshot:



Summary

Through this task, I successfully conducted a basic vulnerability scan using **Nmap** and its scripting engine. This helped me understand how security professionals identify risks in networks before attackers can exploit them. It improved my knowledge of:

- Port scanning
- Service enumeration
- Vulnerability detection

- Ethical hacking methodology

This task gave me hands-on experience in using one of the most essential tools in the cybersecurity toolkit, and reinforced the importance of **continuous scanning and assessment** in maintaining a secure network environment.

Task 2: Implement Two-Factor Authentication (2FA)

In this task, I focused on enhancing the security of my personal accounts by setting up **Two-Factor Authentication (2FA)**. 2FA provides an extra layer of protection by requiring both something I know (password) and something I have (authentication code from a device or app) to access accounts. This process greatly reduces the risk of unauthorized access even if my password is compromised.

Step 1: Choose and Install an Authenticator App

- To begin, I selected **Google Authenticator** as my 2FA app. Other popular options like **Authy** or **Microsoft Authenticator** can also be used.
- I downloaded the app from the App Store (iOS) or Google Play Store (Android) and installed it on my smartphone.

Step 2: Enable 2FA on My Accounts

- I chose a few critical accounts for 2FA setup, including my **email** and **social media** accounts.
- For each account, I navigated to the **Security Settings** or **Account Settings** and selected the **Enable Two-Factor Authentication** option.

Step 3: Scan QR Code and Link Account

- I was presented with a **QR code** for each account.
- Using my **Google Authenticator** app, I scanned the QR code to link the account with the app.
- Once linked, the app generated a **time-based 6-digit code** that changes every 30 seconds.

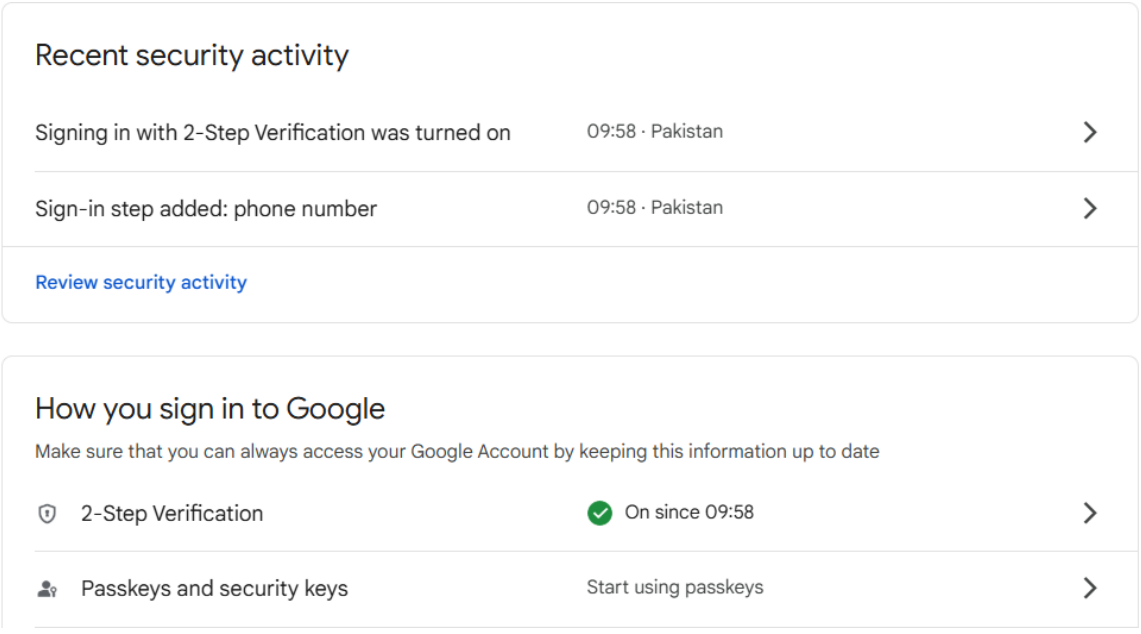
Step 4: Backup Codes and Recovery Options

- I ensured to **write down backup codes** or save recovery options provided by the service in case I lose access to the authenticator app.
- This was important to avoid getting locked out of my accounts in the future.

Step 5: Test 2FA Functionality

- After completing the setup, I logged out of my account and tried to log back in to ensure that 2FA was working correctly.
- When logging in, I was prompted to enter the 6-digit code generated by the authenticator app in addition to my password.

Screenshot:



Summary

Through this task, I successfully implemented **Two-Factor Authentication (2FA)** on my personal accounts, adding a significant layer of security. This process helped me understand how 2FA works in practice and why it's a critical feature in modern cybersecurity to protect sensitive data from unauthorized access.

2FA reduces the risk of account compromise from various attack vectors, such as **phishing** and **password breaches**, by ensuring that even if a password is stolen, access cannot be gained without the second factor.

Task 3: Analyze Network Traffic

In this task, I focused on monitoring and analyzing network traffic to understand the flow of data across a network and identify potential security issues. Network traffic analysis is a vital part of cybersecurity, as it helps detect unusual activities, data leaks, and potential attacks such as **Man-in-the-Middle (MitM)** or **Denial of Service (DoS)**.

To perform this task, I used **Wireshark**, a widely-used network protocol analyzer that captures and inspects packets traveling through a network.

Step 1: Install Wireshark

- I downloaded and installed **Wireshark** from the official website: https://www.wireshark.org.
- I ensured that my system had the necessary **network drivers** installed for Wireshark to capture packets.

Step 2: Capture Network Traffic

- I launched Wireshark and selected the **network interface** (Wi-Fi or Ethernet) to start capturing packets.

- I applied a basic filter to capture all traffic on the network using the display filter: ip.addr == <your_ip_address>.
    - This allowed me to focus on traffic related to my device.
- I captured packets for a set amount of time (5-10 minutes) to gather sufficient data for analysis.

Step 3: Analyze the Traffic

- Once the capture started, I observed the packets flowing across the network.
- I filtered the results to focus on specific protocols, such as:
    - **HTTP**: To view unencrypted web traffic.
    - **DNS**: To observe domain name resolutions.
    - **TCP** and **UDP** packets: To analyze basic communication protocols.
- I examined packet details such as:
    - **Source and destination IP addresses**
    - **Port numbers**
    - **Protocol types**
    - **Packet size and payload**

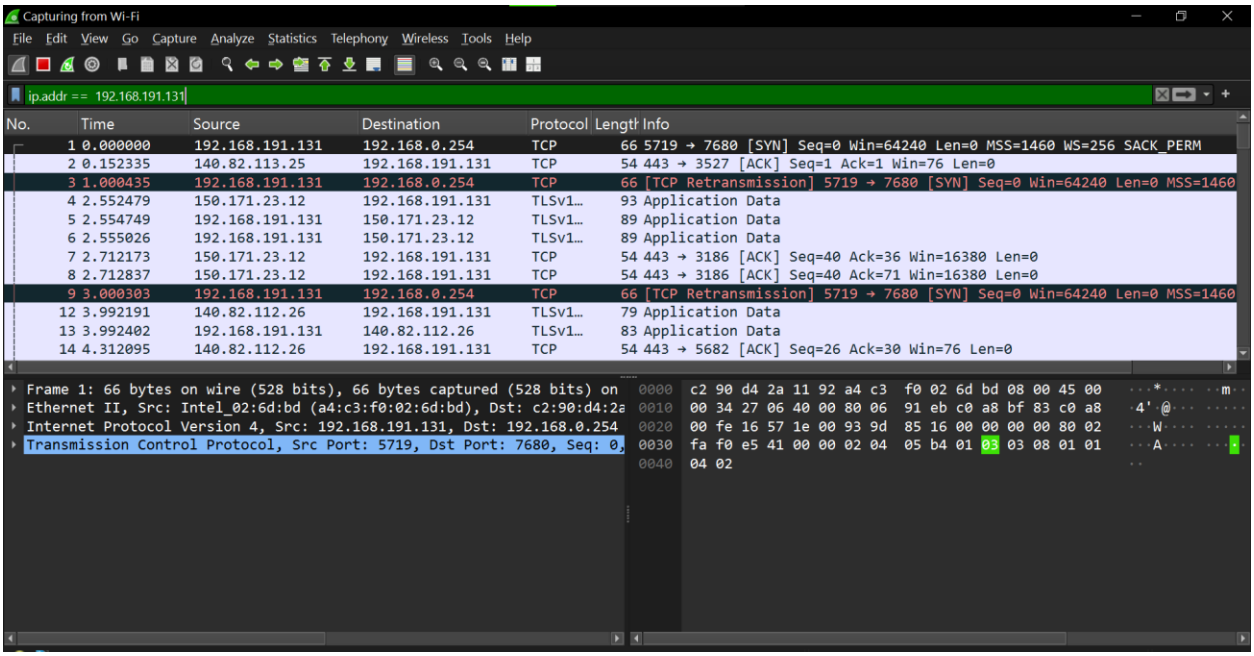
Step 4: Identify Suspicious or Unusual Activity

- While analyzing, I looked for unusual patterns, such as:
    - **Large volumes of traffic to unknown destinations**
    - **Repeated failed connection attempts** (possible brute force attack indicators)
    - **Unencrypted traffic** on sensitive services (e.g., HTTP instead of HTTPS)
- I also used **Wireshark's built-in analysis tools** to detect common network issues, such as **TCP retransmissions** or **out-of-order packets**.

Step 5: Save and Document the Results

- I saved the captured traffic as a **.pcap** file for future reference or further analysis.
- I documented key observations, such as any suspicious traffic or vulnerabilities that could be addressed.

Screenshot:



Summary

Through this task, I gained practical experience in **network traffic analysis** using **Wireshark**. I learned how to:

- Capture and filter network packets.
- Analyze common protocols and their behaviors.
- Identify potential vulnerabilities and security risks based on traffic patterns.

Traffic analysis is an essential skill for identifying malicious activity, ensuring secure network communication, and troubleshooting network-related issues.

7. Insights and Interpretations from Vulnerability Scanning

During the vulnerability scanning task, I identified a variety of vulnerabilities that could be exploited if not addressed promptly. The scan revealed weaknesses in common services and protocols, including **FTP**, **SSH**, **Apache**, **Apache Tomcat**, and **HTTP**. These vulnerabilities are potential entry points for attackers, highlighting the critical importance of regular vulnerability assessments. Many of the identified vulnerabilities were deemed **exploitable**, underlining the need for constant monitoring, patching, and securing of systems to prevent unauthorized access and cyberattacks.

8. Importance of 2FA in Modern Cybersecurity Practices

Two-Factor Authentication (2FA) is a vital security measure for protecting online accounts and systems. In this task, I implemented 2FA on several of my personal accounts, such as email and social media, to enhance their security. By requiring two forms of verification something you know (a password) and something you have (a one-time code from an app or device) 2FA makes it significantly harder for unauthorized users to access accounts, even if they know the password. This task reinforced the critical role of 2FA in defending against unauthorized access, phishing attacks, and brute force attempts. As a result, it's clear that enabling 2FA should be a standard practice for securing personal and professional accounts in today's digital landscape.

9. Observations from Network Traffic Monitoring

During network traffic monitoring with **Wireshark**, I analyzed the flow of various network protocols such as **HTTP**, **DNS**, and **FTP**. One significant

observation was the presence of unencrypted communication, particularly with **HTTP**, which could expose sensitive data to potential interception. This highlighted the importance of using secure protocols like **HTTPS** to ensure data privacy. By closely monitoring the traffic, I gained valuable insights into how data flows within a network and the security implications of unprotected communications. This task reinforced the need for encryption and constant vigilance to maintain secure network environments.

10. Key Learnings and Takeaways from Intermediate Tasks

Throughout the completion of these intermediate cybersecurity tasks, I gained valuable insights and hands-on experience that significantly contributed to my understanding of security practices. From performing vulnerability scans with tools like **Nmap** to setting up **Two-Factor Authentication (2FA)** and monitoring network traffic with **Wireshark**, each task offered a unique learning opportunity.

I learned the importance of **proactive security measures** such as regular vulnerability scanning and the implementation of 2FA to prevent unauthorized access. Additionally, I understood how **network traffic analysis** can help detect potential security risks and how crucial it is to secure communication channels. These tasks not only helped me improve my technical skills but also emphasized the need for continuous monitoring and adapting to new cybersecurity threats. Overall, the experience provided a solid foundation for practical, real-world cybersecurity practices that are essential for securing systems and networks.

11. My Reflections and Growth Through These Activities

These tasks have been an eye-opening experience, providing a deeper understanding of the practical aspects of cybersecurity. The hands-on nature

of each task helped me to not only apply theoretical knowledge but also develop essential problem-solving skills. Working with tools like **Nmap**, **Wireshark**, and implementing **2FA** on my personal accounts helped me build confidence in applying cybersecurity measures to real-world scenarios.

Throughout these activities, I realized the significance of attention to detail, as small vulnerabilities or misconfigurations can lead to larger security risks. Additionally, I learned that cybersecurity is an ongoing process that requires constant vigilance and adaptation to new threats. This journey has not only enhanced my technical capabilities but has also reinforced my passion for pursuing a career in cybersecurity, where continual learning and growth are crucial.

12. Conclusion

In conclusion, the tasks I completed during this internship have significantly strengthened my understanding of core cybersecurity principles and practical applications. From performing vulnerability scans to implementing **Two-Factor Authentication (2FA)** and analyzing network traffic, I've developed crucial skills that are essential for protecting systems and networks. Each task provided me with valuable insights into the importance of securing digital environments against various threats.

Through these activities, I've learned that cybersecurity is not just about using the right tools, but also about adopting a proactive mindset, continually assessing risks, and implementing protective measures. The experience has reinforced my commitment to cybersecurity and has prepared me for the challenges I will face in the industry. I look forward to further expanding my skills and contributing to the ongoing effort of securing digital space