Internship Report

NAME: SUVHANKAR DUTTA

TRACK: CYBER SECURITY

DURATION: 1 MONTH

1. Introduction

My internship experience has been an invaluable stepping stone in my journey toward a career in cybersecurity. Over the course of the program, I was exposed to a variety of tools and methodologies that deepened my understanding of real-world security practices. From exploring web application vulnerabilities with OWASP ZAP to analyzing network traffic using Wireshark, I gained practical skills that complemented my academic learning. This summary outlines the key lessons I learned, how the experience contributed to my professional growth, and suggestions that could enhance the internship experience for future participants.

2. Task Overview

2.1 Task 1: Introduction to Network Security Basics

NETWORK SECURITY CONCEPTS:

- ***Objectives:***

Understand the basics of network security by learning about different types of network threats and how to implement basic security measures. This task will introduce you to the foundational concepts of securing a small network.

- Understanding different types of network threats, including viruses, worms,

trojans, and phishing attacks.

- Understanding basic security concepts like firewalls, encryption, and secure network

- Setting up a simple network environment, such as your home network or a virtual lab with a router and one or two connected devices.
- Enabling and configuring a basic firewall (e.g., Windows Defender Firewall) to block
- unauthorized access.
- Setting up basic security configurations, such as changing default passwords and enabling network encryption
- Using Wireshark to capture and analyze network traffic.
- Identify different types of traffic, such as HTTP, DNS, and others, and understand them.

Understanding different types of network threats, including viruses, worms, trojans, and phishing attacks:

1. Viruses

- Malicious code that attaches itself to legitimate files or programs and spreads when executed.
- Threat: Corrupts, deletes, or modifies files; slows down systems.
- Example: File-infector virus, Macro virus.

2. Trojan Horses

- Malicious programs disguised as legitimate software.
- Threat: Creates backdoors, steals data, allows remote access.
- Example: Remote Access Trojans (RATs), Banker Trojans.

3. Worms

- Self-replicating malware that spreads through networks without human action.
- Threat: Consumes bandwidth, slows down networks, causes system crashes.

- Example: SQL Slammer, WannaCry worm.

4. Man-in-the-Middle Attacks

- Attacker intercepts communication between two parties.
- Threat: Steals or alters data being transmitted.
- Example: Eavesdropping on login credentials over unsecured Wi-Fi.

5. Phishing Attacks

- Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity via email, message, or website.
- Threat: Data theft (passwords, credit card details), identity theft.
- Example: Fake bank login pages, fraudulent emails asking for personal info.

6. Denial of Service (DoS) / Distributed DoS (DDoS)

- Overwhelms a server or network with traffic to make it unavailable.
- Threat: Disrupts service for users and businesses.
- Example: Flooding a website with millions of requests to crash it.

7. Insider Threats

- Security risks originating from employees or others with access.
- Threat: Data theft, system sabotage, accidental breaches.
- Example: An employee stealing confidential company data.

8. Ransomware

- Malware that encrypts user data and demands payment to restore access.
- Threat: Data loss, financial damage, downtime.
- Example: WannaCry, Locky.

9. Spyware

- Software that secretly monitors user activity and sends data to attackers.
- Threat: Theft of credentials, surveillance.
- Example: Key loggers, tracking cookies.

10. Adware

- Unwanted software that displays ads and may track user activity.
- Threat: Privacy invasion, slows down devices.
- Example: Pop-ups, browser redirects.

Understanding basic security concepts like firewalls, encryption, and secure network:

1. **Firewalls**

- A firewall is a security device (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Purpose: Blocks unauthorized access while permitting legitimate communication.
- Types:
  Packet-filtering firewall
  Stateful inspection firewall
  Next-generation firewall (NGFW)
- Example: Preventing unknown IP addresses from accessing your computer or server.

2. **Encryption**

- The process of converting data into a coded format (ciphertext) so only authorized parties can understand it.
- Purpose: Protects data confidentiality during storage and transmission.
- Types:
  Symmetric encryption (same key for encryption/decryption) – e.g., AES
  Asymmetric encryption (public and private keys) – e.g., RSA
- Example: HTTPS uses encryption to protect data exchanged between your browser and websites.

3. **Secure Network Configurations**

- The practice of setting up and maintaining network systems in a secure manner to minimize vulnerabilities.
- Key Practices:
- Disabling unused ports and services
- Changing default passwords
- Implementing strong access control
- Regular patching and updating
- Using secure protocols (like SSH instead of Telnet)
- Purpose: Reduces the attack surface and prevents unauthorized access.
- Example: Configuring a router to block unused ports and enable WPA3 encryption for Wi-Fi.

Summary Table:

Concept	**Purpose**	**Example**
Firewall IPs	Control network traffic	Block traffic from suspicious sources
Encrypting emails	Protect data confidentiality	HTTPS, VPN
Secure configuration default logins	Network security	Disable unused port change

Instructions are provided for creating a virtual network in Oracle VM VirtualBox. The process includes setting up a host-only adapter, configuring DHCP settings, and connecting virtual machines (Ubuntu and Kali Linux) to the same subnet. Verification steps ensure both machines can communicate effectively through ping tests.

Highlights: Creating a virtual network in Oracle VM VirtualBox allows multiple virtual machines to communicate within the same subnet. This setup enhances network management and testing capabilities for users. -Setting up a host-only network adapter is crucial for isolating communication between virtual machines. This ensures that the VMs can interact without external network interference. -Configuring the DHCP server enables automatic IP address assignment within the specified subnet. This simplifies the network setup process and minimizes manual configuration errors. -Disabling the default network adapter on each VM ensures that they only connect through the newly created network. This step is important to maintain the virtual network's integrity. Creating and configuring a virtual network in Oracle VirtualBox allows multiple virtual machines to communicate effectively.

This process involves assigning IP addresses and verifying connectivity between hosts. -To begin, power on a Linux virtual machine and run the command 'ip addr' to check the assigned IP address from the created subnet range. -After verifying the first machine's IP address, repeat the process on a second Linux machine to ensure it also receives an IP from the same subnet. -Finally, use the ping command to test connectivity between the two hosts, confirming they can communicate as expected within the same subnet.

Windows Firewall can be enhanced to block malicious IPs through automation. By using a script, users can regularly update a blacklist of harmful IP addresses, ensuring better protection against hackers and malware. The video also promotes a Discord workshop for community engagement and further learning about network security.

Highlights: Windows Firewall is not just a passive protector; it actively filters traffic and can be customized to enhance security. Users can create specific rules to block malicious IP addresses effectively. -Many users are unaware of the extensive rules that Windows Firewall operates with, which filter incoming and outgoing traffic. Understanding these rules is crucial for better security management. -The importance of creating exceptions for applications that connect in non-standard ways emphasizes the need for user awareness. Users often overlook this aspect until prompted by alerts. -Using automation and scripts can simplify the process of updating and managing firewall rules. This allows users to block multiple malicious IPs efficiently instead of doing it manually. Automating the process of blocking malicious IPs is essential for cybersecurity. This video demonstrates how to efficiently retrieve and manage a list of harmful IP addresses. -Using resources like abuse.ch and URLhaus, users can find lists of malicious servers and domains. These lists help in blocking potential malware threats effectively. -The video showcases a simple script that automates the updating of blocked IP lists. This ensures that the firewall settings remain current and effective against new threats. -Understanding the format of the IP lists is crucial for the automation process. The video explains how to convert CSV data into a usable format for firewall rules.

Dynamic IP management is crucial for cybersecurity, as IP addresses can change and become malicious over time. Implementing scripts that adaptively block these IPs is essential for effective network protection. -The process begins by deleting existing rules to ensure that new scripts operate on a fresh set of parameters, preventing outdated rules from interfering. -Using a CSV reader and Lambda filter allows the script to exclude comment lines, focusing solely on the valid IP addresses that need to be processed. -The script generates commands to block specific IPs, illustrating how automation can enhance firewall management and safeguard against threats like DDoS attacks. Utilizing scripts to add rules for IP addresses is an effective method for enhancing network security. This process can be applied across various firewall software solutions for better protection. -The script displays the added IP addresses in real-time, showcasing how rules can be integrated into the system seamlessly. This visual feedback is crucial for monitoring. CrowdSec is introduced as an open-source intrusion detection system, providing users with an automated way to manage block lists. This system simplifies the security process significantly. CrowdSec allows users to add custom rules and implement captchas for certain IPs, enhancing user interactions while maintaining security. This feature adds flexibility to the blocking process. Crowdsourced security tools are becoming more accessible for home users, allowing them to enhance their protection against malicious threats. These tools leverage community input to identify and classify security risks effectively. -Community involvement plays a crucial role in identifying false positives and confirming malware, empowering users to contribute to their own security. This collaborative approach enhances overall protection. -The ease of deploying these security tools makes them ideal for home servers and personal use, providing a low barrier to entry for users. They are user-friendly and continuously updated. -Participating in events like Discord discussions can foster community engagement and provide users with detailed guidance on network security practices. These interactions promote learning and collaboration.

- **Tools and methods used**: *Firewall (Windows Defender Firewall or a basic hardware firewall), Wireshark*

- **Steps taken to complete the task:**

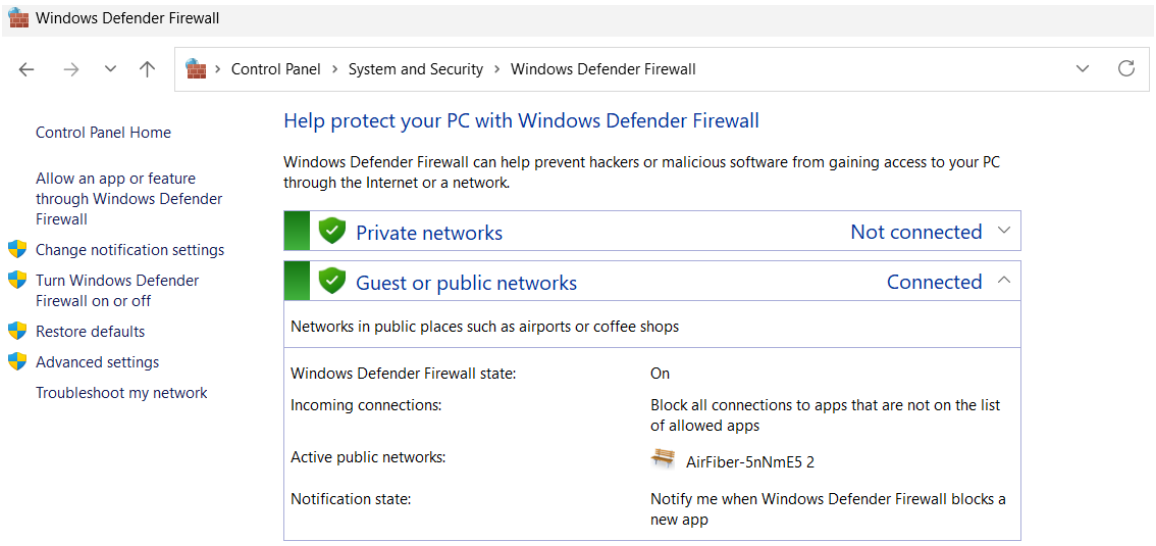
- Setting up a simple network environment, such as your home network or a virtual lab with a router and one or two connected devices.
- Enabling and configuring a basic firewall (e.g., Windows Defender Firewall) to block
- unauthorized access.
- Setting up basic security configurations, such as changing default passwords and enabling network encryption
- Using Wireshark to capture and analyze network traffic.
- Identify different types of traffic, such as HTTP, DNS, and others, and understand them using Wireshark.

- **Challenges faced and how they were overcome**:

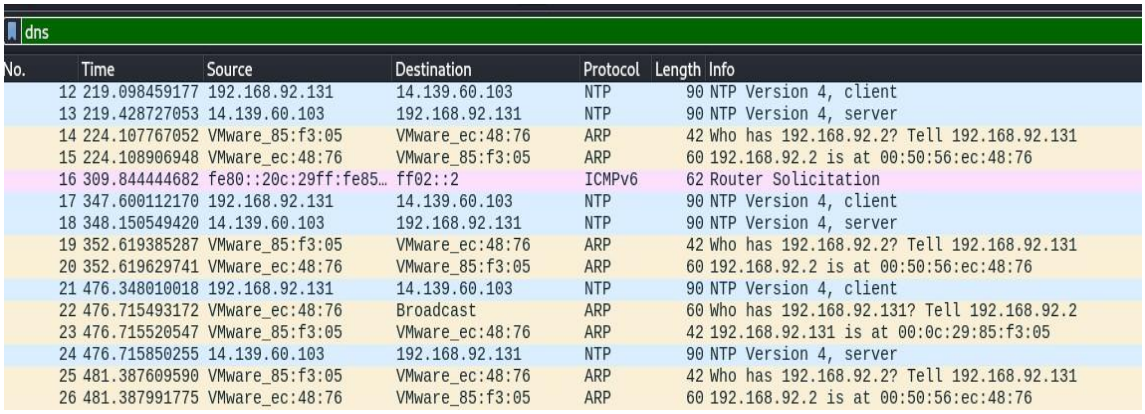
- *Enabling the firewall*: finding out the firewall configuration through the pc, so had to take help from YouTube to enable it. It was found in the control panel, and after following the steps I was able to enable the Windows Defender Firewall.
- *Setting up Wireshark:* had to setup Wireshark with the help of YouTube and setting the connection to eth0 and configuring the protocols.

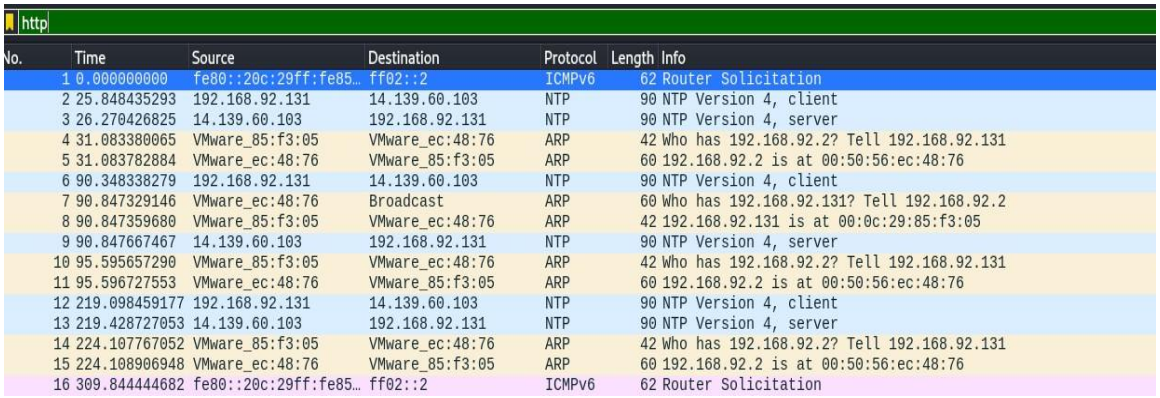
- **Results and outcomes:**

1. *Enabling Windows Defender Firewall*:
   By going to control panel, clicking system and security option we can find windows defender firewall.



2. *Using Wireshark*:
   Start Wireshark and set it into eth0 or your private network and monitor the network traffic.





http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::20c:29ff:fe85…	ff02::2	ICMPv6	62	Router Solicitation
2	25.848435293	192.168.92.131	14.139.60.103	NTP	90	NTP Version 4, client
3	26.270426825	14.139.60.103	192.168.92.131	NTP	90	NTP Version 4, server
4	31.083380065	VMware_85:f3:05	VMware_ec:48:76	ARP	42	Who has 192.168.92.2? Tell 192.168.92.131
5	31.083782884	VMware_ec:48:76	VMware_85:f3:05	ARP	60	192.168.92.2 is at 00:50:56:ec:48:76
6	90.348338279	192.168.92.131	14.139.60.103	NTP	90	NTP Version 4, client
7	90.847329146	VMware_ec:48:76	Broadcast	ARP	60	Who has 192.168.92.131? Tell 192.168.92.2
8	90.847359680	VMware_85:f3:05	VMware_ec:48:76	ARP	42	192.168.92.131 is at 00:0c:29:85:f3:05
9	90.847667467	14.139.60.103	192.168.92.131	NTP	90	NTP Version 4, server
10	95.595657290	VMware_85:f3:05	VMware_ec:48:76	ARP	42	Who has 192.168.92.2? Tell 192.168.92.131
11	95.596727553	VMware_ec:48:76	VMware_85:f3:05	ARP	60	192.168.92.2 is at 00:50:56:ec:48:76
12	219.098459177	192.168.92.131	14.139.60.103	NTP	90	NTP Version 4, client
13	219.428727053	14.139.60.103	192.168.92.131	NTP	90	NTP Version 4, server
14	224.107767052	VMware_85:f3:05	VMware_ec:48:76	ARP	42	Who has 192.168.92.2? Tell 192.168.92.131
15	224.108906948	VMware_ec:48:76	VMware_85:f3:05	ARP	60	192.168.92.2 is at 00:50:56:ec:48:76
16	309.844444682	fe80::20c:29ff:fe85…	ff02::2	ICMPv6	62	Router Solicitation