CYBER SECURITY INTERNSHIP REPORT

Title: Introduction to Network Security Basics

Intern Name: **Satvik Bhagat**
Internship Duration: *25 May 2025 – 25 June 2025*
Internship Organization: *The Red Users – Cyber Security Internship*

Objective

The objective of this report is to explore and demonstrate fundamental network security practices. This includes understanding common cyber threats, configuring secure network environments, monitoring traffic, and analyzing suspicious activity through practical tools and real-time observation.

Proficiencies Obtained

- Basic Network Security
- Threat Identification
- Firewall Configuration
- Packet Analysis using Wireshark

Tools & Platforms Used

- Windows Defender Firewall
- Wireshark (for traffic analysis)
- Kali Linux (optional - Wireshark pre-installed)

Core Concepts in Network Security

Common Network Threats

Virus: Infects files or programs and requires user action to spread.

Worm: Spreads independently across networks, consuming resources.

Trojan: Disguises as legitimate software, provides backdoor access.

Phishing: Tricks users into revealing sensitive data via fake communication.

CYBER SECURITY INTERNSHIP REPORT

Fundamental Security Concepts

Firewalls: Monitor & block/allow network traffic to prevent intrusions.

Encryption: Encodes data to prevent unauthorized access.

Secure Configurations: Disabling unused services, applying patches, strong credentials.

Network Security Implementation

Network Setup

Home Setup: Windows PC, Wi-Fi router, and 1-2 additional connected devices.

Virtual Lab: Use VirtualBox/VMware with a router and VMs to simulate networks.

Security Measures Implemented

Windows Firewall Configuration

Access: Windows + I > Update & Security > Windows Security > Firewall

Enabled Firewall for Domain, Private, and Public networks.

Controlled App Access: Reviewed and modified firewall app permissions.

Advanced Settings: Defined custom rules for specific ports and programs.

Network Traffic Analysis - Wireshark

Captured live network traffic during web browsing:

- HTTP/HTTPS Traffic
- DNS Resolution
- TCP Handshakes
- ICMP (Ping)

Suspicious Events:

- Failed TCP handshakes
- DNS queries to unknown domains

CYBER SECURITY INTERNSHIP REPORT

Secure Configuration Practices

Change Default Passwords:

- Router Access: Changed admin password
- User Accounts: Set strong passwords

Wi-Fi Encryption Settings:

- WPA2/WPA3-Personal with strong passphrase

How Security Measures Help

Firewall: Protects system from unauthorized access

Password Security: Prevents default credential attacks

Encryption: Secures data transmission

Traffic Analysis: Detects threats early

Secure Configuration: Minimizes attack vector

Reflection & Best Practices

For Large/Enterprise Networks

- IDS/IPS systems
- VLAN segmentation
- Centralized Authentication
- Endpoint Detection & Response
- Patch Management
- Network Access Control

CYBER SECURITY INTERNSHIP REPORT

Spreading Awareness

Conduct sessions on:

- Using strong passwords
- Avoiding suspicious links
- Enabling 2FA
- Keeping software updated

Use demos to promote better understanding