Cyber Security Internship – Task 8

Task Title: VPN Setup and Privacy Testing

Submitted By: Gourav Swaroop

Date: 15/08/2025

Objective

To understand the role of Virtual Private Networks (VPNs) in protecting online privacy and securing communications. The task involved selecting a reputable VPN service, connecting to a server, verifying encryption, and evaluating the benefits and limitations of VPN usage.

Tools Used

- **ProtonVPN (Free Tier)** – Chosen for strong security features and good reputation
- **WireGuard** – Lightweight, modern VPN protocol
- **Kali Linux Terminal** – For VPN connection commands
- **ipinfo.io** & **whatismyipaddress.com** – For IP address verification
- **speedtest.net** – For internet speed comparison
- **Web Browser** – To verify encrypted traffic

Step-by-Step Process

1. Choose a reputable free VPN service and sign up

- Selected **ProtonVPN Free Tier** for its strong encryption, no-logs policy, and trustworthy reputation.
- Registered a free ProtonVPN account on the official ProtonVPN website.

2. Download the VPN client/configuration

- Logged into the ProtonVPN dashboard and downloaded the **WireGuard configuration file** for a free server location.
- Saved the .conf file to the **Downloads** directory.

3. Connect to a VPN server

- Moved the downloaded .conf file to /etc/wireguard/ and renamed it proton.conf:
- sudo mv ~/Downloads/wg-JP-FREE-14.conf /etc/wireguard/proton.conf
- Set correct file permissions:
- sudo chmod 600 /etc/wireguard/proton.conf
- Connected to the VPN using:
- sudo wg-quick up proton

4. Verify IP address change

- Before VPN: IP showed my real ISP location.
- After VPN: IP changed to a **Tokyo, Japan** IP address.
- Verified using:
- curl https://ipinfo.io

  and **whatismyipaddress.com** in a browser.

5. Browse a website to confirm encrypted traffic

- Accessed multiple websites and confirmed they loaded through the VPN server.
- Checked browser's security lock icon (HTTPS) to verify encrypted connection.

6. Disconnect VPN and compare browsing speed and IP

- Disconnected using:
- sudo wg-quick down proton
- Compared speeds with and without VPN using **speedtest.net** – observed a slight drop in speed while connected.

7. Research VPN encryption and privacy features

- ProtonVPN uses **AES-256 encryption** and modern protocols like **WireGuard** and **OpenVPN**.
- Has DNS leak protection and a kill switch to prevent accidental IP exposure.

8. Summary – VPN Benefits and Limitations

Benefits:

- Hides real IP for privacy.
- Encrypts traffic to prevent interception.
- Useful for bypassing geo-blocks.
- Safer browsing on public Wi-Fi.

Limitations:

- Speed reduction due to encryption.
- Free servers may be slower or crowded.
- Does not protect from malicious websites directly.