Elevate Labs – Cyber Security Internship

Name:Srinivas Atta

Task 8: Setup and Test a VPN for Privacy Protection

By: Ministry of MSME, Govt. of India

Objective

Learn how to set up and use a VPN to protect privacy and secure online communication, then observe its real-world impact.

Tools Required

- Free VPN client (e.g., ProtonVPN free tier, Windscribe free)
- IP address checker (`whatismyipaddress.com`)

Execution Steps / Guide

1. Choose a Trusted VPN Provider
    - Selected ProtonVPN free tier for reliability and transparency.
2. Sign Up and Install the Client
    - Registered with ProtonVPN and downloaded the official app.
3. Connect to a VPN Server
    - Opened the app and connected to the nearest free server.
4. Verify IP Change
    - Checked `whatismyipaddress.com` before and after connecting to VPN.
    - Confirmed public IP address successfully changed to VPN server location.
5. Test Encrypted Traffic
    - Browsed several websites.
    - Noted that traffic now flows through an encrypted tunnel—preventing local Wi-Fi/network snooping.
6. Disconnect VPN for Comparison

    - Observed that browsing speed can be affected (slightly slower with VPN).
    - Rechecked IP to confirm returned to ISP's address.
7. Research VPN Features
    - Studied how VPNs use encryption protocols (OpenVPN, WireGuard, IKEv2).
    - Learned no-log policies, DNS leak protection, and kill switch features.
8. Summarize Benefits and Limitations
    - Documented how VPN helps ensure privacy but isn't a total anonymity solution.

Findings / Results

- VPN successfully installed and connected (see attached screenshot of ProtonVPN connected).
- Public IP changed — confirmed on IP checker sites.
- Web traffic encrypted — browsing activity not visible to ISP or network admin.
- Performance impact — web pages loaded slightly slower; streaming speeds varied.
- VPN privacy features — highlighted kill switch, encryption strength, DNS/IP leak protection.

Security Analysis

VPN encrypts and tunnels all outgoing network traffic, protecting it from local eavesdroppers and letting the user mask their true location and IP. However:

- VPN providers themselves can see unencrypted data unless using a trusted no-log service.
- VPN does not protect against phishing, malware, or websites tracking via cookies.
- Free VPNs may have usage, location, or privacy limitations.

Recommendations

- Use trusted VPN services with strong encryption and a transparent no-logs policy.
- Always check for DNS and IP leak protection in client settings.
- Consider paid VPNs for access to more locations and increased speed/privacy.

- Use VPN along with other security best practices (browser hygiene, anti-phishing measures).
- Avoid accessing sensitive accounts (bank/email) over untrusted VPN services.

Outcome

- Gained practical experience with VPN setup and testing.
- Learned how VPNs enhance privacy and the limits of their protection.
- Recognized the difference between encrypted and unencrypted web traffic.

Key Concepts

- VPN privacy and encryption
- Tunneling protocols (WireGuard, OpenVPN, IKEv2)
- IP masking
- DNS leak protection
- Network security