VPN Hands-On Lab Report

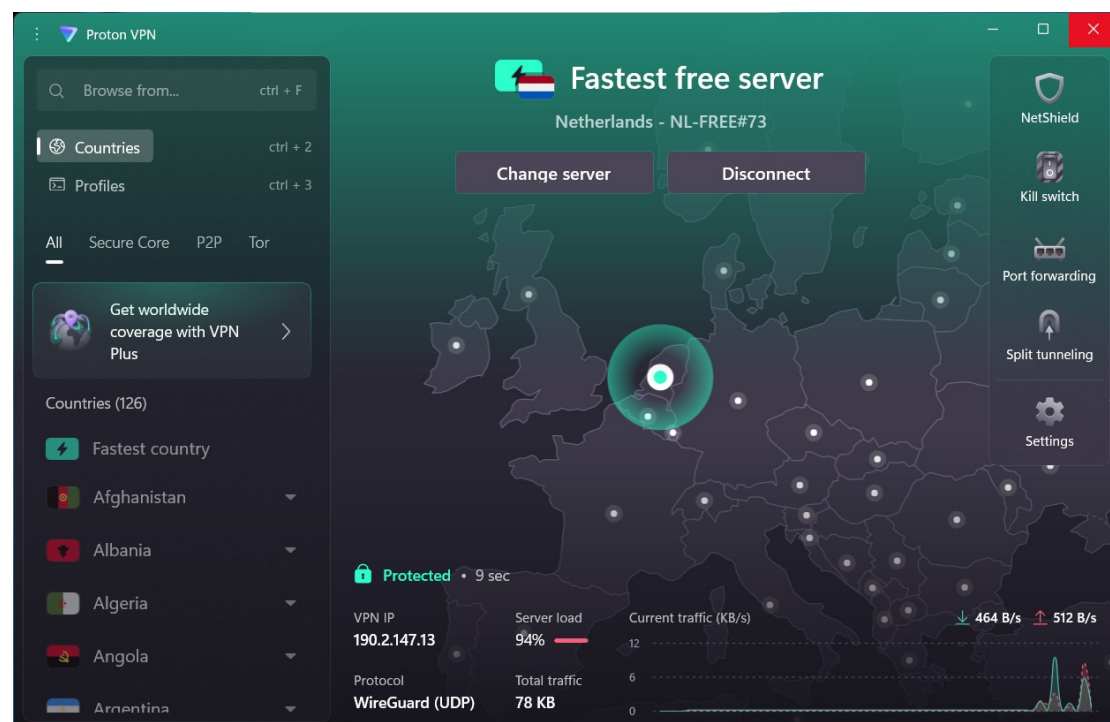Course: Cyber Security

Date: 10/03/2025

Objective

To understand the role of Virtual Private Networks (VPNs) in protecting privacy and ensuring secure communication.

Tools Used VPN Client: ProtonVPN Free

Verification Tool: https://whatismyipaddress.com

- Web Browser: Chrome/Firefox/Edge
- Steps Performed Choose a reputable free VPN service and sign up
- Selected ProtonVPN Free.
- Created a free account using email.
- Download and install the VPN client
- Downloaded the official VPN client.
- Installed and logged into the application.
- Connect to a VPN server (closest or any location)
- Chose nearest server location for better speed.
- Status showed "Connected."

Verify your IP address has changed (use whatismyipaddress.com)

Checked IP before VPN:

Checked IP after VPN:

- Browse a website to confirm traffic is encrypted
- Visited Google/YouTube.
- Verified HTTPS padlock symbol confirming encryption.

Disconnect VPN and compare browsing speed and IP

Disconnected VPN → IP reverted to ISP's original IP.

Browsing speed without VPN was slightly faster.
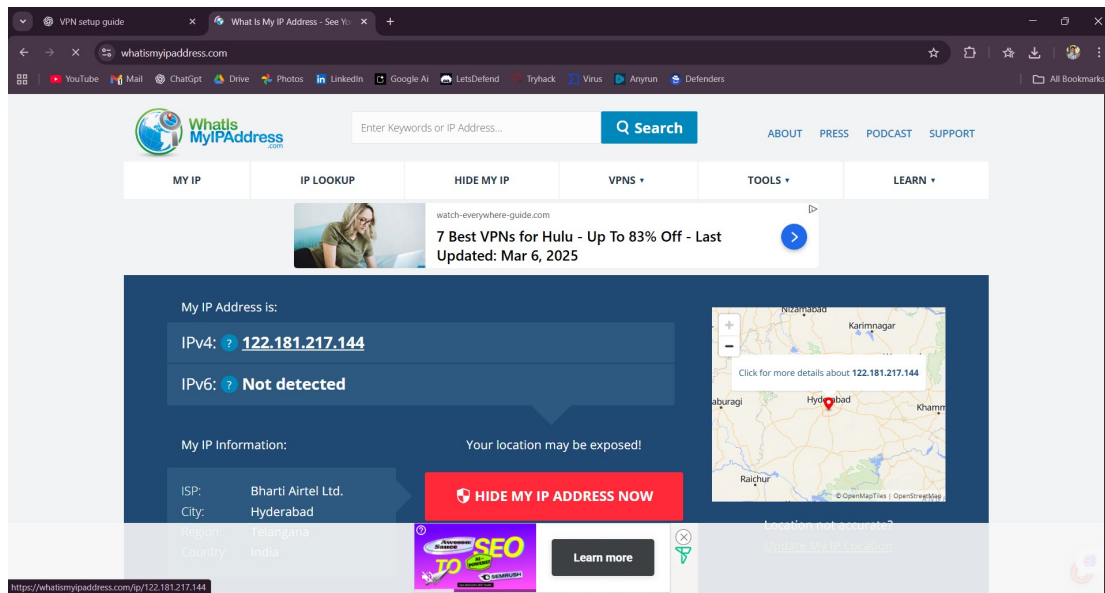
Research VPN encryption and privacy features

- VPN uses protocols like OpenVPN, WireGuard, IKEv2/IPSec.
- Traffic is encrypted end-to-end, preventing monitoring by ISPs and attackers.
- Masks real IP address for privacy.
- Write a summary on VPN benefits and limitations

Benefits:

1. Protects privacy by masking IP
2. Encrypts traffic (safe on public Wi-Fi)
3. Helps bypass geo-restrictions
4. Provides secure communication

Limitations:

- May reduce internet speed
- Free VPNs have limited servers/bandwidth
- Cannot guarantee complete anonymity
- Does not protect against malware/phishing
- Speed: Slightly reduced while using VPN
- Encryption: Confirmed through HTTPS websites

Conclusion The VPN successfully changed the IP address, encrypted internet traffic, and demonstrated privacy protection. This lab showed the importance of VPNs in cybersecurity while also highlighting limitations such as reduced speed and incomplete anonymity.