

Task 8: Working and Understanding VPN

Objective

To understand how Virtual Private Networks (VPNs) function, their role in online privacy and security, and to gain hands-on experience by installing and testing a free VPN client.

Tools Used

- VPN Clients: ProtonVPN (Free), Windscribe (Free)
- Web Tools: whatismyipaddress.com
- Browsers: Google Chrome, Mozilla Firefox
- OS: Kali Linux

Steps Performed

1. Sign Up for a Free VPN

- Choose ProtonVPN as the VPN provider.
- Visited protonvpn.com and created a free account.

2. Download and Install VPN Client

- Downloaded the ProtonVPN client for Windows.
- Installed the software and logged in using the credentials created during signup.

3. Connect to a VPN Server

- Opened the VPN client and selected a server located in the Netherlands (Free Tier).
- Clicked "Connect" to initiate the VPN session.

4. Verify IP Address Change

- Before connecting: IP was 192.168.xxx.xxx (original location).
- After connecting: IP changed to 10.2.0.2.
- Used whatismyipaddress.com to confirm the change.

5. Confirm Encrypted Traffic

- Browsed a few websites like Google, YouTube, and Wikipedia.
- Confirmed all connections were HTTPS and encrypted.
- Verified certificate details to check for end-to-end encryption.

6. Disconnect and Compare

- Disconnected from the VPN.
- Rechecked IP address and browsing speed.
- Observed that the original IP was restored and the speed was slightly increased.

Key Learnings

- VPNs help protect user privacy by masking IP addresses and encrypting traffic.
- VPNs are useful when using public Wi-Fi, preventing eavesdropping.
- Not all VPNs guarantee anonymity; logs and DNS leaks can still expose data.
- Free VPNs often come with limitations like speed caps, fewer servers, or restricted bandwidth.