Task 8 :Identify and Remove Suspicious Browser Extensions

Prepared By: Arti Kumari

1. Introduction and Setup

- **Objective:** To install and test a Virtual Private Network (VPN) client to understand its role in **encrypting traffic** and **masking identity** on the internet.

- **Tool Used: Windscribe Free Tier**

- **Protocol Used: OpenVPN**

- **Verification Tool:** whatismyipaddress.com

2. Verification and Observations

1. **Identity Masking:** Upon connecting to the Windscribe server (e.g., in London), the publicly displayed IP address immediately changed from my local IP to the server's IP. This confirmed that all my outbound network requests were being proxied and my true location was successfully **masked**.

2. **Traffic Security:** Browsing a website confirmed that the VPN established a working **encrypted tunnel**. This prevents local threats (like

attackers on public Wi-Fi) or intermediate networks (like the ISP) from reading the content of the data.

3. **Performance Limitation:** A noticeable **reduction in browsing speed** was observed while connected to the VPN. This is a typical trade-off due to the overhead of encrypting/decrypting traffic and routing data over a longer path.

3. Summary of VPN Security and Privacy

Category	Security Principle	Description
Data Security	**Encryption Tunnel**	The VPN wraps all data in an encrypted layer (using a strong algorithm like **AES-256**) before it leaves the device. This makes the data unreadable to anyone intercepting the traffic.
Privacy Protection	**IP Masking**	By substituting the user's local IP address with the VPN server's IP, the VPN protects the user's geographic location and identity from websites, advertising trackers, and government surveillance.