# Cybersecurity Internship Report - Task 8

**Intern Name:** Sai Aditya
**Organization:** Elevate Labs
**Task Title:** Working with VPNs
**Date:** August 15, 2025

## Objective

The objective of this task is to gain hands-on experience with a Virtual Private Network (VPN) by setting up a free client, connecting to a server, and verifying its functionality. The task also involves understanding the fundamental role of VPNs in protecting online privacy and securing communication.

## Tools Used

- Operating System: Kali Linux
- VPN Client: [Specify the free VPN service used, e.g., ProtonVPN
- IP Verification Tool: whatismyipaddress.com
- Browser: Google Chrome

## Scenario

The scenario for this task involved a practical exercise to set up and use a VPN to understand its core functions. The process began with selecting and installing a reputable free VPN client. After installation, a connection was established to a server in a different geographical location. The IP address was then verified to confirm that the connection was active and the user's online identity was masked. Finally, the browsing experience with the VPN was compared to a non-VPN connection to understand its impact on network speed and privacy. The entire process was documented, along with key research on VPN benefits and limitations.

## Procedure

1. Selected and Installed VPN Client: Chose a reputable free VPN service and completed the signup process. Downloaded and installed the official client on the system.
2. Connected to a VPN Server: Launched the VPN client and connected to a server located in [Specify a country, e.g., "the Netherlands"].
3. Verified IP Address: Visited an IP verification website to confirm that the public IP address and geographical location had changed from the local network's information to the VPN server's.
4. Verified Encrypted Traffic: Conducted a brief browsing session to confirm that web traffic was being routed securely through the VPN tunnel.
5. Compared Performance: Disconnected from the VPN and compared the browsing speed and IP address to the encrypted session to observe the effects of the VPN on network performance.
6. Researched VPN Features: Researched the technical aspects of VPNs, including encryption protocols and privacy features.

## Theories & Learnings

- What is a VPN?

A VPN creates a secure, encrypted "tunnel" over a public network, such as the internet. All data sent and received through this tunnel is protected from eavesdropping.

- How a VPN Protects Privacy:

A VPN hides a user's real IP address by assigning them a new one from the VPN server. This makes it difficult for websites, advertisers, and third parties to track the user's online activity and real-world location.

- Encryption:

The primary security feature of a VPN is encryption. It scrambles data, making it unreadable to anyone who intercepts it. Common encryption standards include AES (Advanced Encryption Standard).

- Benefits:

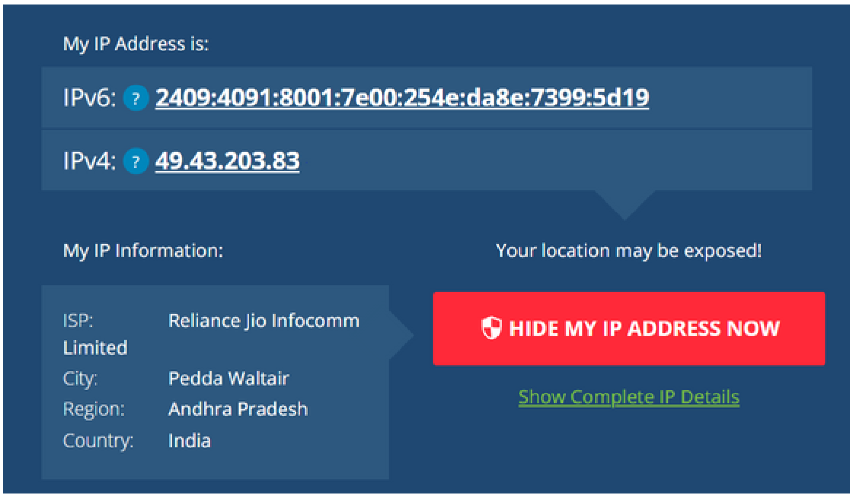
VPNs are essential tools for protecting privacy on public Wi-Fi networks, bypassing geographical content restrictions, and preventing Internet Service Providers (ISPs) from monitoring online activity.

- Limitations:

While effective, VPNs do not offer complete anonymity. Free VPNs may have data caps or slower speeds. All VPNs can slightly reduce network speed due to the encryption and routing process.

# Screenshots

## 1) IP Address before VPN



My IP Address is:

IPv6: 2409:4091:8001:7e00:254e:da8e:7399:5d19

IPv4: 49.43.203.83

My IP Information:

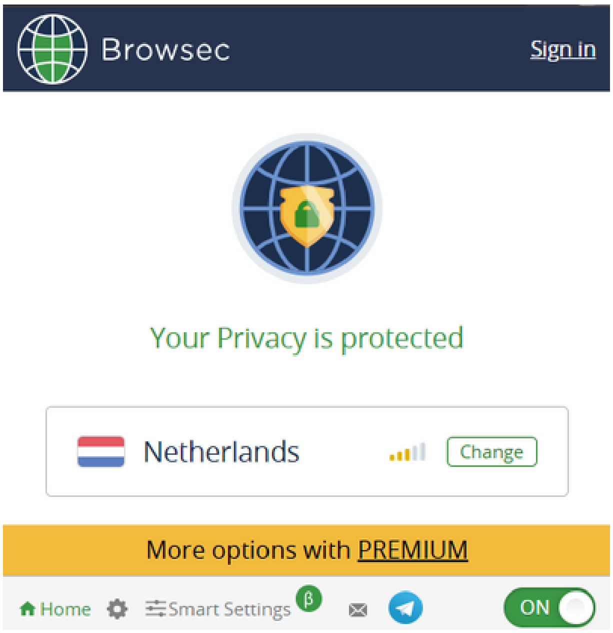
ISP: Reliance Jio Infocomm Limited
City: Pedda Waltair
Region: Andhra Pradesh
Country: India

Your location may be exposed!

**Fig1: Screenshot of IP address before VPN**

This screenshot shows the IP address and location of the network before connecting to the VPN. The IP information, including the ISP (Reliance Jio Infocomm Limited) and location (Pedda Waltair, Andhra Pradesh, India), confirms the original, unmasked identity and geographical location of the connection.

## 2) VPN Activation



Your Privacy is protected

Netherlands

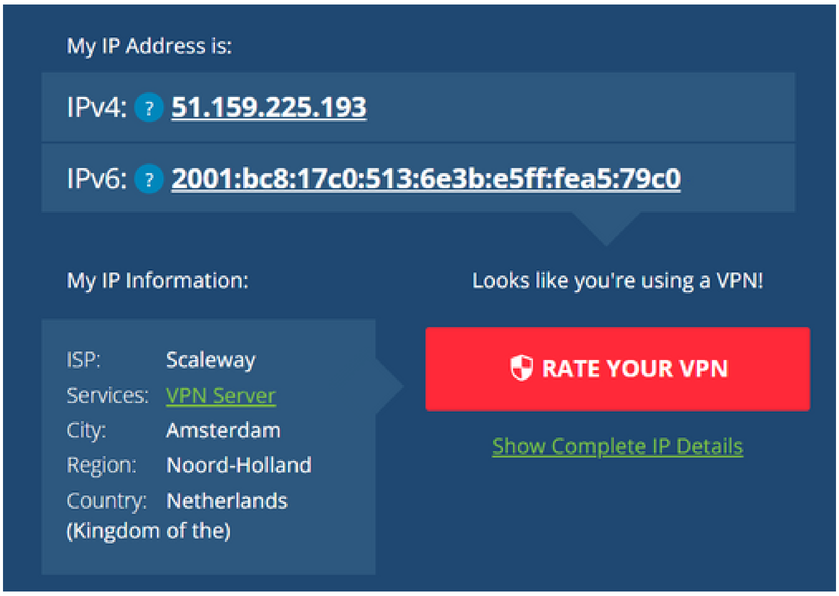
ON

**Fig2: VPN Activation (Browsec VPN)**

This image provides visual confirmation that the VPN client (Browsec) has been successfully installed and is active. The interface clearly shows that a connection has been established to a server located in the Netherlands, indicating that all subsequent web traffic is being routed through an encrypted tunnel.

I have used Browsec for this task and I have been using it since 2023.

### 3) IP Address after VPN



My IP Address is:

IPv4: 51.159.225.193

IPv6: 2001:bc8:17c0:513:6e3b:e5ff:fea5:79c0

My IP Information:

| | |
|---|---|
| ISP: | Scaleway |
| Services: | VPN Server |
| City: | Amsterdam |
| Region: | Noord-Holland |
| Country: | Netherlands (Kingdom of the) |

Looks like you're using a VPN!

Fig3: Screenshot of IP Address after VPN

This final screenshot of the IP verification website demonstrates the core functionality of the VPN. The IP address has been changed (51.159.225.193), and the geographical information now reflects the VPN server's location (Amsterdam, Noord-Holland, Netherlands). This proves that the VPN is working correctly to mask the original IP address and protect the user's online

## Conclusion

This task provided a practical, hands-on understanding of VPNs as a fundamental cybersecurity tool. The process of setting up a client and verifying the IP address change demonstrated how a VPN successfully masks a user's identity and location. The exercise highlighted the significant benefits of using a VPN to protect privacy and secure data, while also acknowledging its limitations and the importance of choosing a reputable service.

## DISCLAIMER

This activity was conducted in a controlled environment solely for educational purposes. No unauthorized traffic interception or monitoring of third-party networks was performed.