**Network Security VPN’s**

**Assignment 1:**

**OpenVPN-Client-Connection-and-IP-Verification**

This assignment demonstrates setting up an OpenVPN server on a Linux machine, establishing a VPN connection from a client (same machine), and verifying the change in public IP address before and after connecting to the VPN. The goal is to create a self-hosted VPN environment for secure remote access and privacy. Since I already have an .ovpn configuration file, I can directly use it to connect to the VPN and verified my IP address before and after the connection,

**1. Introduction**

For this, I used an existing OpenVPN configuration file (.ovpn) to connect my Linux machine to a VPN. I verified the public IP address before and after the VPN connection to demonstrate secure tunneling.

**2. Tools Used**

* OpenVPN client on Linux
* curl for IP address verification

**3. Procedure**

**Step 1: Check public IP before VPN connection**

I ran the command:

curl ifconfig.me

This showed my real public IP address before the VPN connection.

**Step 2: Connect to the VPN using .ovpn file**

Using the OpenVPN client, I connected to the VPN:

sudo openvpn --config /vpn/client.ovpn

I provided the required credentials when prompted, and the connection was successfully established.

**Step 3: Verify public IP after VPN connection**

In a new terminal session, I ran:

curl ifconfig.me

This showed the VPN server’s public IP address, confirming that my traffic was routed through the VPN.

**4. Results**

* Original IP (before connection): [36.255.18.105]
* New IP (after connection): [202.21.42.138]

**5. Conclusion**

Using the provided OpenVPN configuration, I successfully connected to a VPN on my Linux system and verified that my IP address changed, indicating encrypted and private network communication.

**6. Attachments**

* configuration file
* Terminal outputs for IP before and after connection (Screenshots)



