Experiment No. 4

Title: Setting up VPN on windows and Linux machine

Roll No.: 16010420075 **Experiment No.: 4**

Aim: To setup VPN on Windows and Linux machine

\

Resources: virtual box

Theory

A virtual private network, or VPN, is an encrypted link between a device and a network via the Internet. The encrypted connection aids in the secure transmission of sensitive data. It protects against illegal eavesdropping on traffic and allows the user to work remotely. In corporate settings, VPN technology is commonly used.

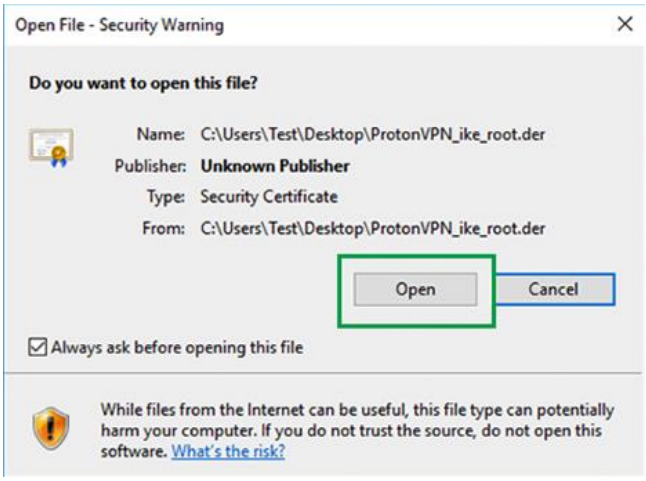
A virtual private network (VPN) connects a corporate network to the Internet via encrypted connections. Traffic remains private as it travels because it is encrypted between the device and the network. An employee can work from home and still connect to the company network safely. A VPN can be used to connect even smartphones and tablets.

The virtual network's traffic is sent securely via a tunnel, which is an encrypted link established via the Internet. As it travels through this tunnel, VPN traffic from a computer, tablet, or smartphone is encrypted. Offsite employees can then connect to the corporate network via the virtual network.

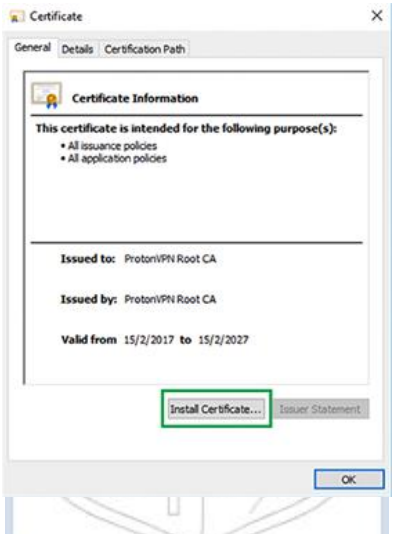
IMPLEMENTATION AND RESULTS:

Setting up VPN on windows:

1. Download the **ProtonVPN IKEv2 Certificate**.
2. **Open** the Certificate.

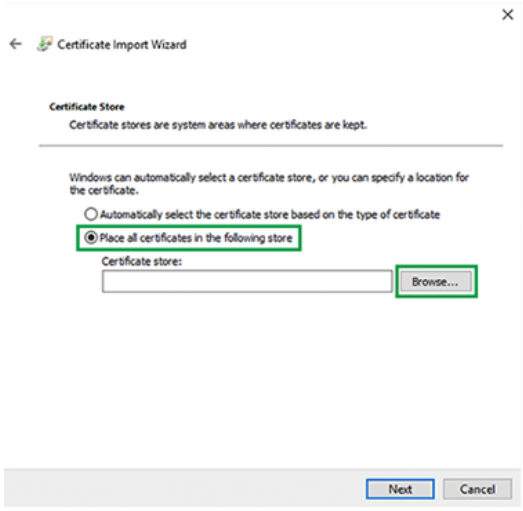


3. Click **Install Certificate.**

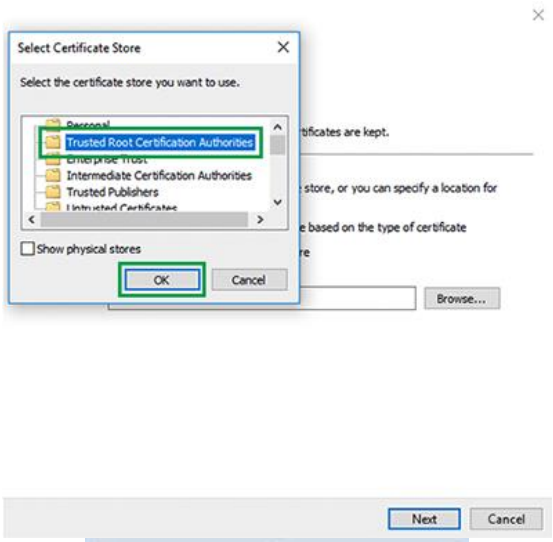


4. Select **Local Machine** and click **Next**.

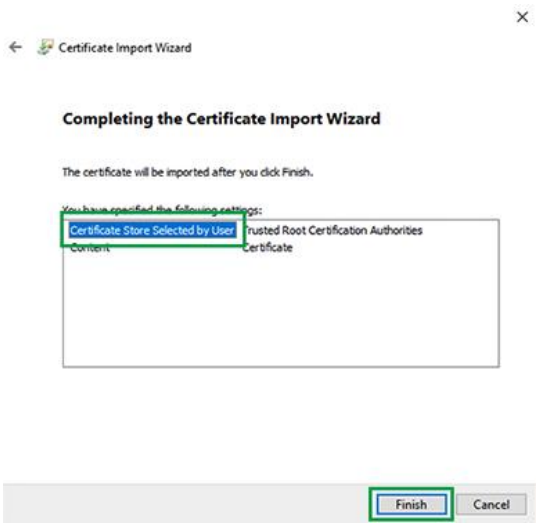
5. Select **Place all certificates in the following store** and click **Browse**…



6. Select **Trusted Root Certification Authorities** and click **OK**, then **Next**.



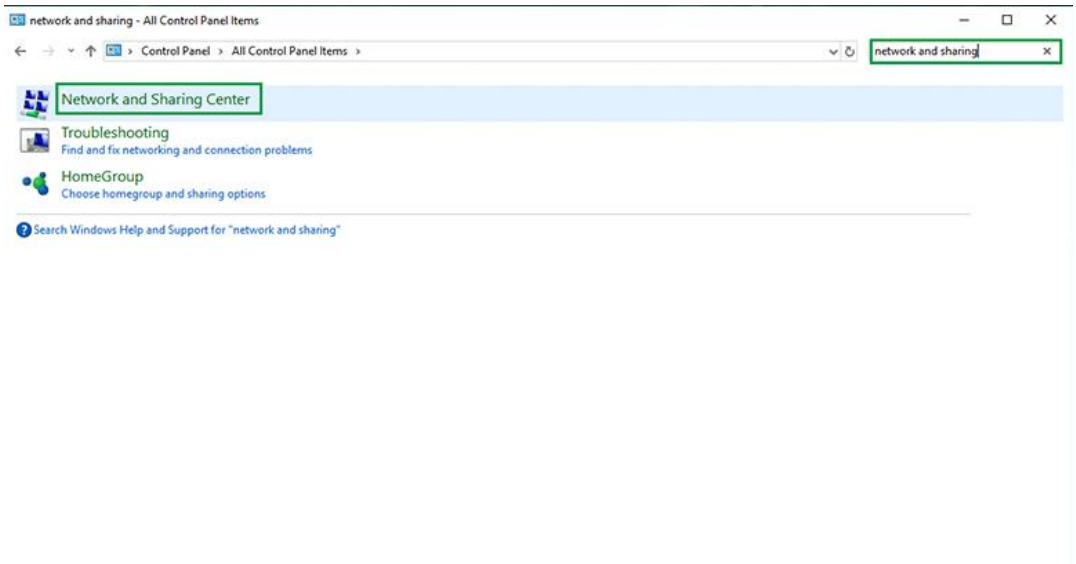
7. Click **Finish** and then **OK** on the Certificate Import Wizard window.



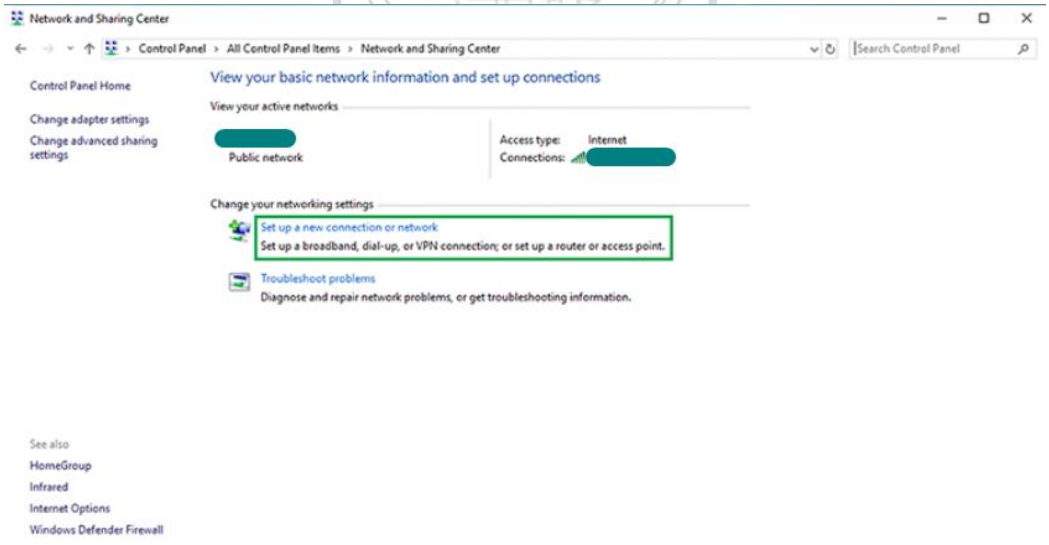
Connecting to the VPN:

1. Open the Windows Control Panel.

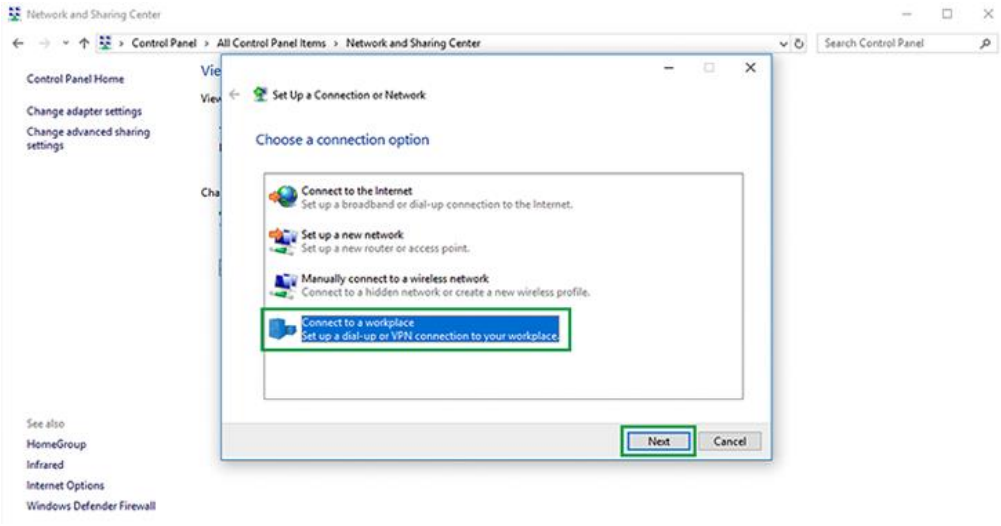
2. Search for “Network and Sharing Center” and open it.



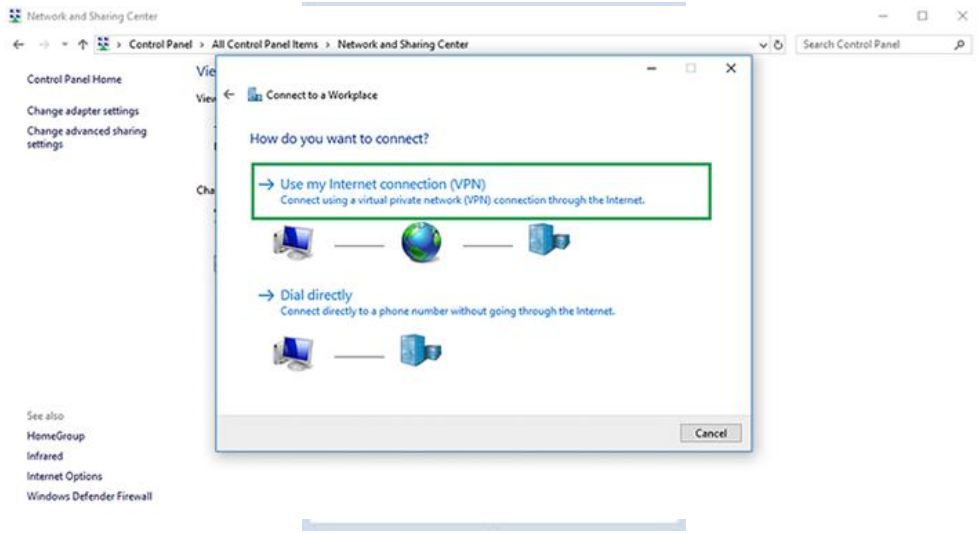
3. Click on **Set up a new connection or network**.



4. Select **Connect to a workplace** and click **Next**.

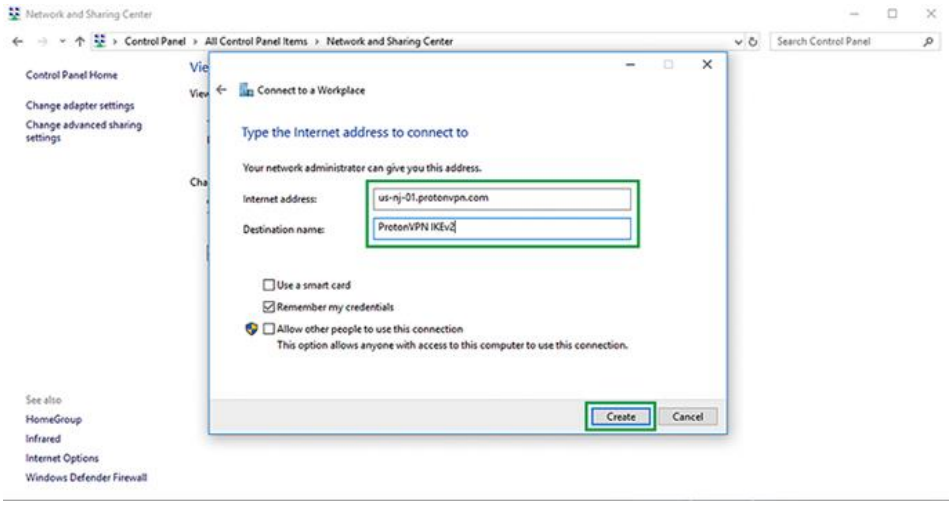


5. Click on **Use my Internet connection (VPN)**.

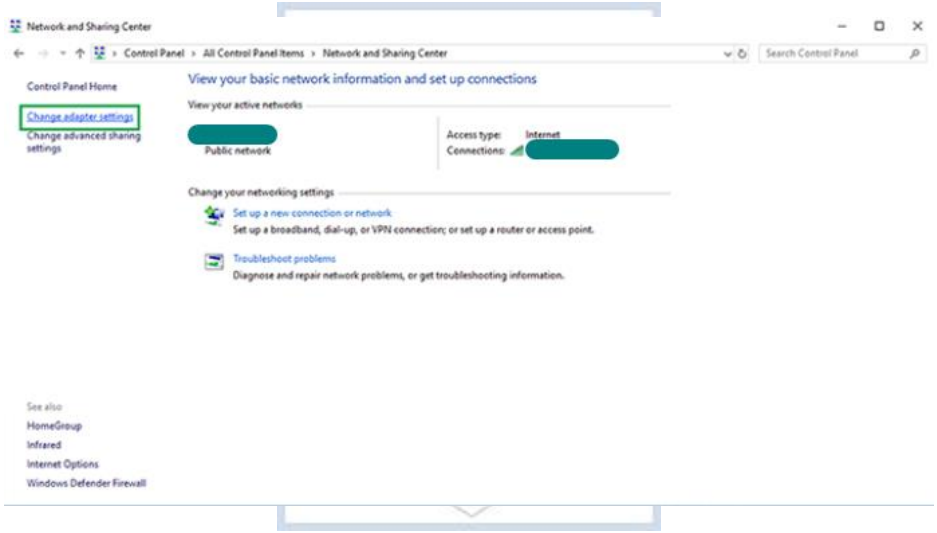


6. In the server field, enter the **hostname** of the server you wish to connect to except for a Free server (for example we used US server **us-nj-01.protonvpn.com**). Free servers do not work with the IKEv2 connection protocol due to the load balancers used on the hostnames. Server hostnames can be found in the Downloads category in your account, under the Server Configs section. Each server is named according to its server number and a two-letter country code: https://account.protonvpn.com/downloads

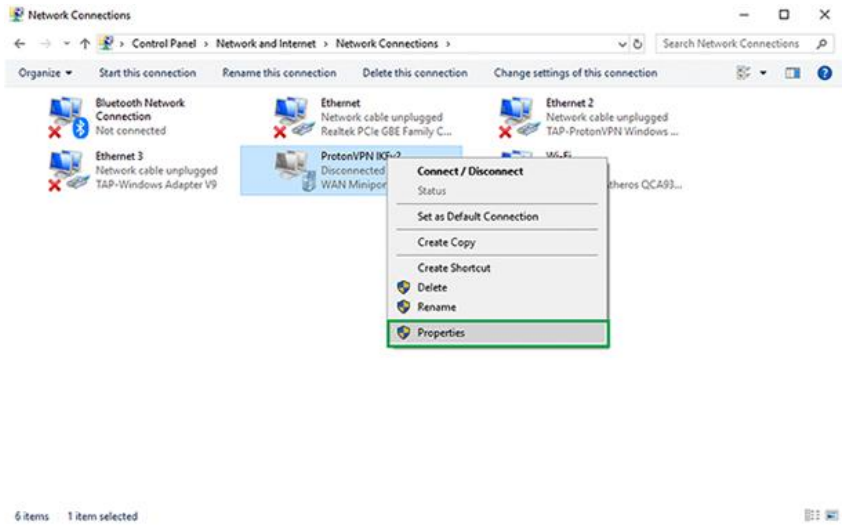
Type any name you choose in the "Destination name" field, then click **Create**.



7. You will return to Network and Sharing Center window – click on **Change adapter settings**.



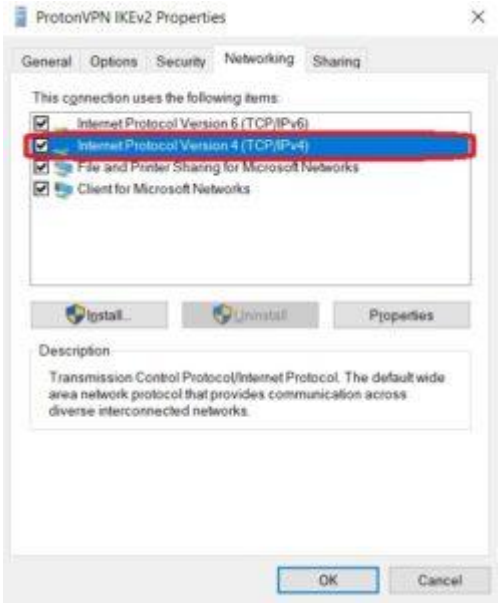
8. Right-click on the Network adapter you have created and select **Properties**.



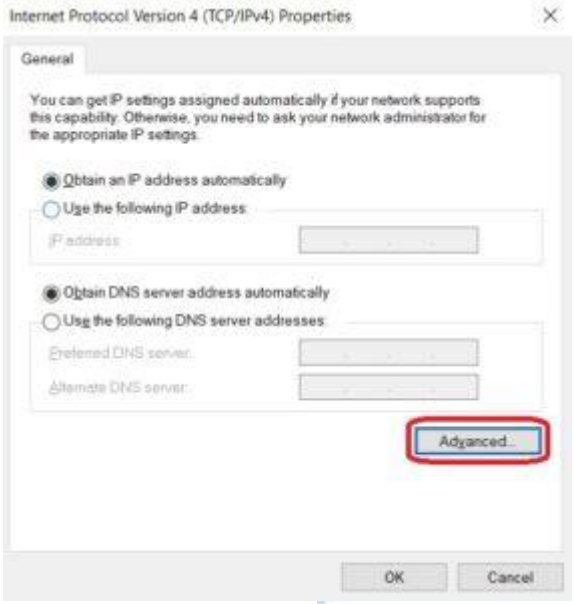
9. Microsoft changed the Windows 10 Desktop and mobile VPN routing behavior for new VPN connections. The option **Use default gateway on remote network** in the Advanced TCP/IP settings of the VPN connection is now disabled by default. To access this option:

- Select the **Networking** tab in the ProtonVPN IKEv2 Properties Window

- Double-click on **Internet Protocol Version 4**



- Select **Advanced…**

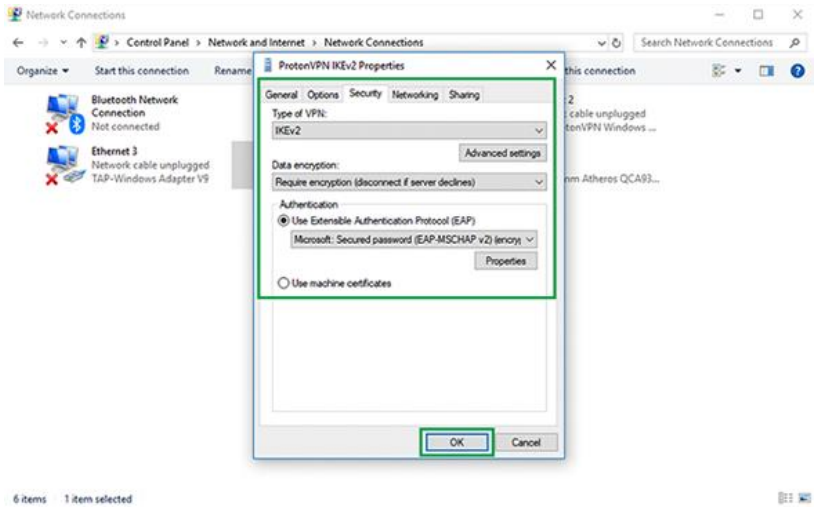


- Here you will see the **Use default gateway on remote network** option

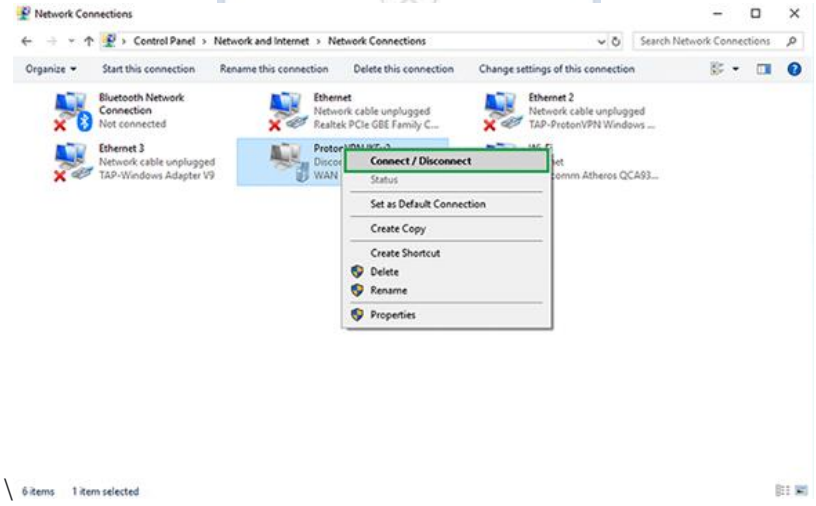
10. Select the **Security** tab in the ProtonVPN IKEv2 Properties window and enter these settings:

Type of VPN: **IKEv2**
Data encryption: **Require encryption (disconnect if server declines)**
Authentication: **Use Extensible Authentication Protocol(EAP) and EAP-MSCHAP v2**

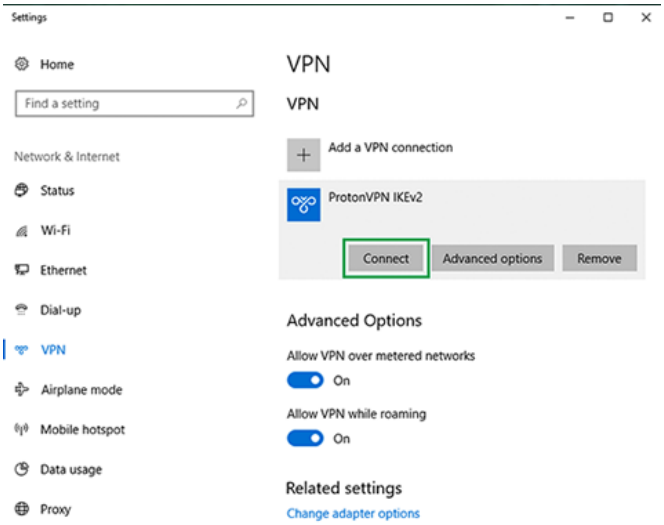
Click **OK** to save the settings.



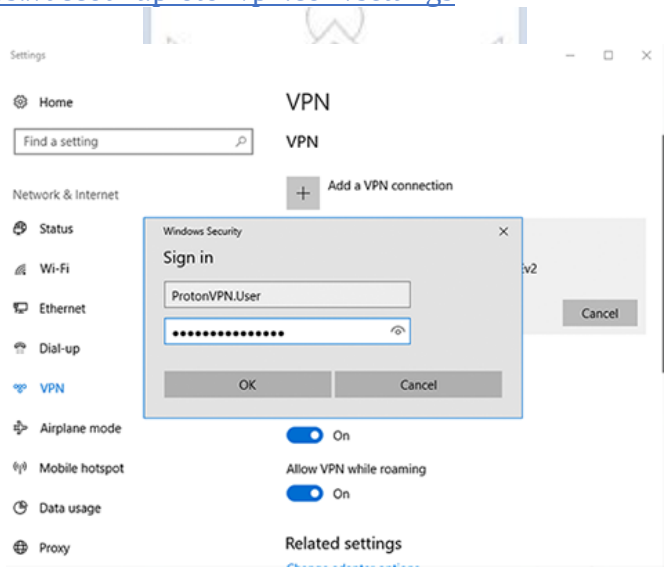
11. Right-click on the Network adapter that you created and click **Connect / Disconnect**.



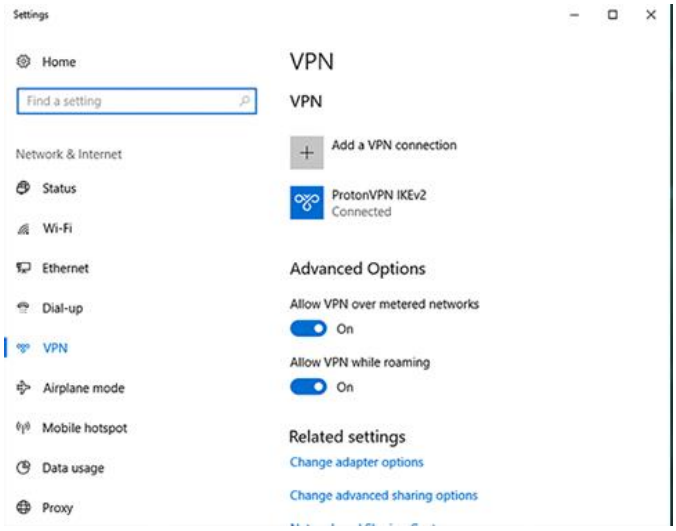
12. The Windows 10 built-in VPN client will open up. Select your profile and click **Connect**.



13. You will be prompted to enter your VPN credentials – **you will have to enter your OpenVPN/IKEv2 credentials**, which can be found in the Account category: https://account.protonvpn.com/settings

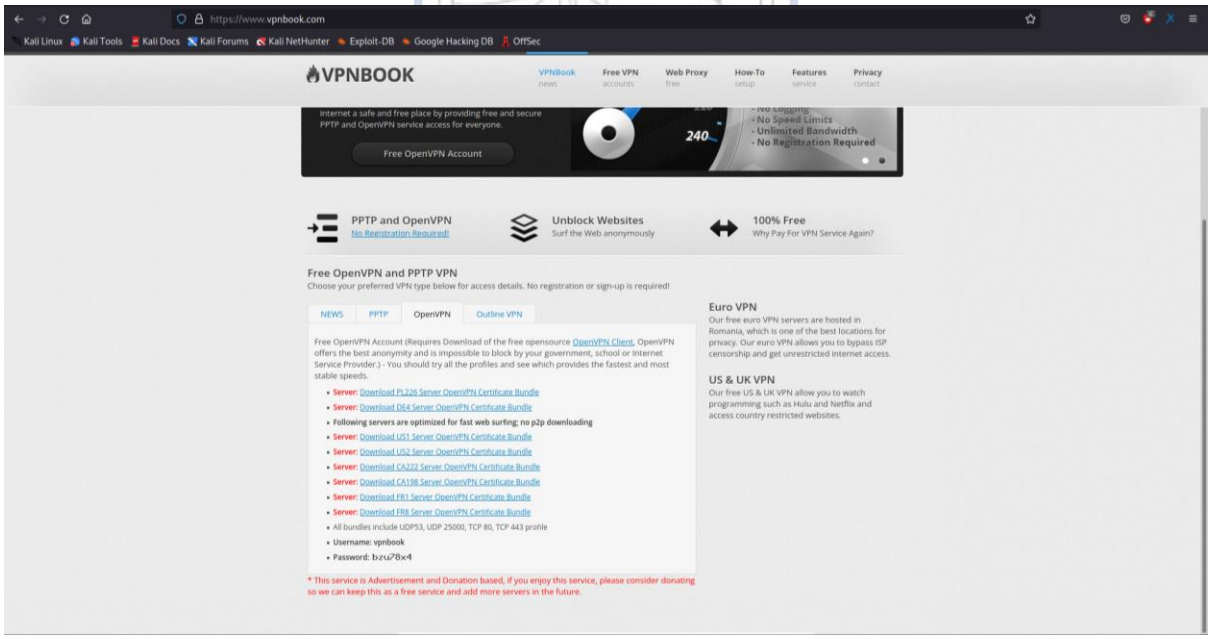


14. That's it! You have successfully connected to a ProtonVPN server via the IKEv2/IPsec protocol. In order to disconnect, just simply select the profile again and click **Disconnect**.

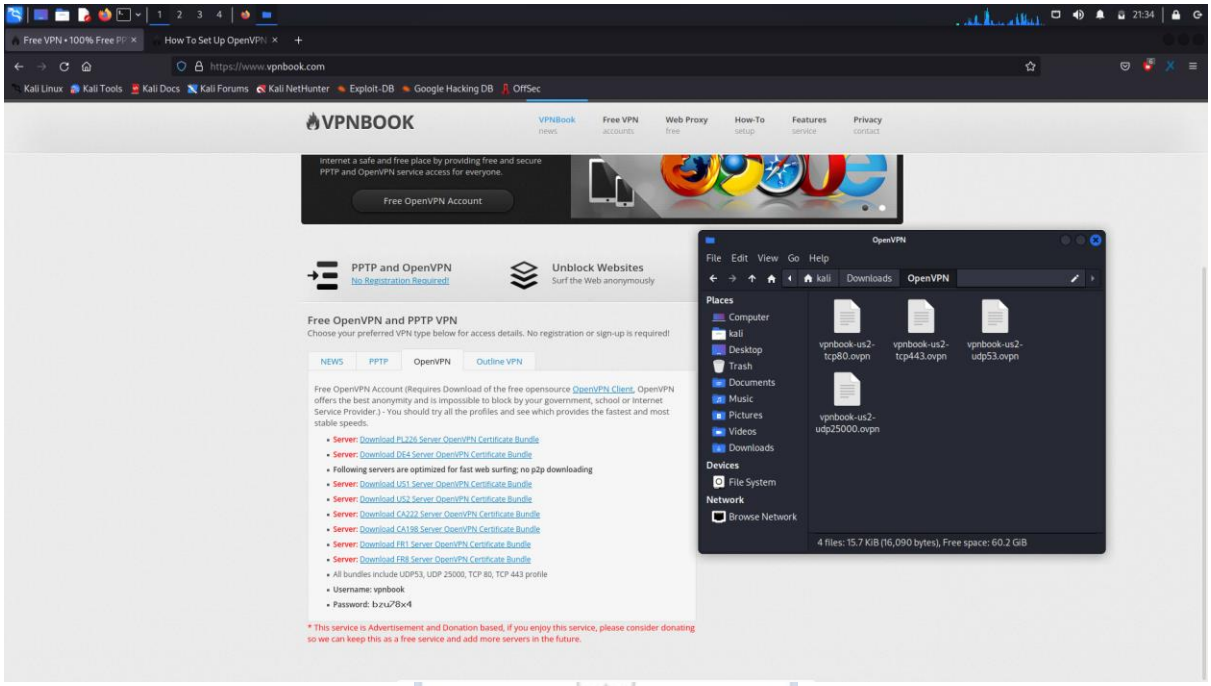


Setting up VPN on Linux (Kali):

1. Open www.vpnbook.com in your browser and select “OpenVPN” as option.

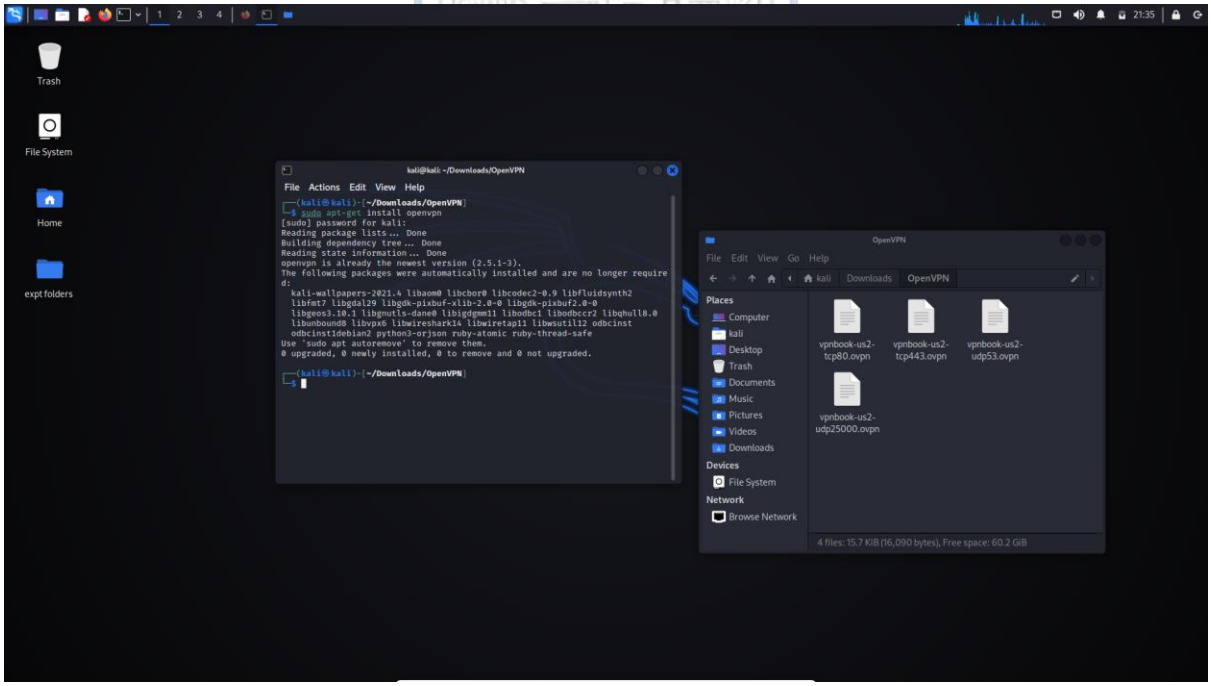


2. Download any of the server mentioned in the website. Save it in any desired folder. Open terminal in that folder.

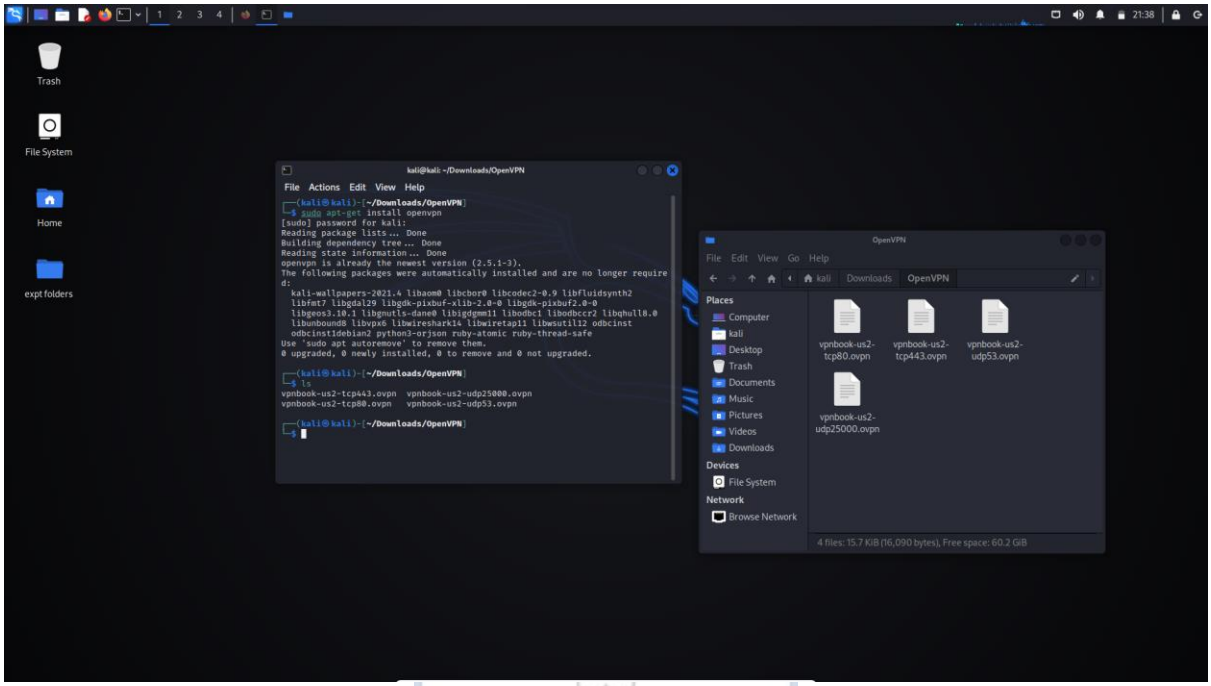


3. Type the following command to install OpenVPN

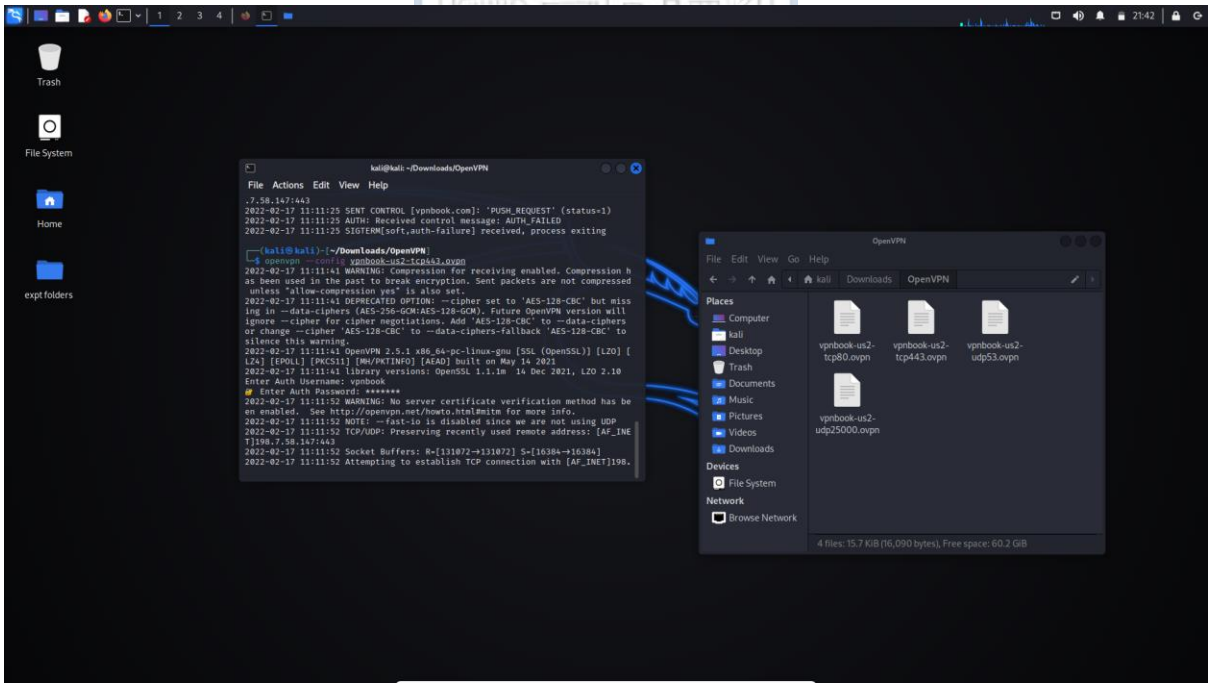
```
$ sudo apt-get openvpn
```



4. List the files using ls command in the terminal.



5. Launch OpenVPN client with one of the VPNBook OpenVPN profile.
   Command: "`openvpn --config vpnbook-us2-tcp443.ovpn`"
   Continue to enter username and password given in the website.



After completing the steps, you will notice that the VPN is connected!

Outcomes:

CO-1: Realize that premise of vulnerability analysis and penetration testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Installation of VPN in Windows and Linux machines were successfully shown.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.protonvpn.com
- www.vpnbook.com