HELP DOCUMENT:

Step 1: Download and Install ” Win64OpenSSL\_Light-3\_4\_0.exe” from [https://slproweb.com/products/Win32OpenSSL.html](https://slproweb.com/products/Win32OpenSSL.html).

Step 2:Install OpenSSL on your laptop:

- Follow the installation prompts.

- Ensure to set the installation path and update the system environment variables.

Step 3: Configure the VPN:

1. Generate certificates and keys using OpenSSL commands.

2. Set up the server and client configurations on the same laptop.

3. Ensure the proper OpenVPN configuration files are in place.

Step 4: Test the VPN connection:

- Use Wireshark to capture packets and verify encryption.

- Test file sharing between the client and server setup.

Step 5: Analyze Network Traffic:

- Open Wireshark and start capturing packets.

- Verify that the data packets are encrypted.

Step 6: Perform Vulnerability Assessment:

- Use \*\*Nmap\*\* to scan the network setup.

- Identify potential vulnerabilities or open ports.

Step 7: Document Results:

- Record observations from Wireshark and Nmap.

- Include screenshots of the processes and outcomes.

Step 8: Conclude and Provide Recommendations:

- Summarize the strengths and any identified issues in the VPN.

- Suggest improvements for better security.