**Practical 8**

**Objectives: To try OpenVPN.**

For this exercise, you will need two Win10 virtual machines and use OpenVPN to set up a secured connection between them.

**Exercise Setting up the two Win10 virtual machines.**

1. Login to the lab desktops.
2. Create a folder D:\EHD-*yourname* (eg D:\EHD-johntan) if you have not done so in the previous semester. You can keep your EHD files in this folder.
3. Go to C:\BaseImages and copy the Win10 folder to your D:\EHD folder.

(you can also download the Win10 virtual machine from the following Dropbox link: <https://www.dropbox.com/sh/4x22syj7ia8ppq2/AAB6fEPo2vrOxArtmHr6xU1ha>)

1. Create another copy of the Win10 folder in your D:\EHD folder and rename the folder as “Win10-2”.

You now have two Win10 virtual machines. Choose one Win10 to be the Server, and the other Win10 will be the Client.

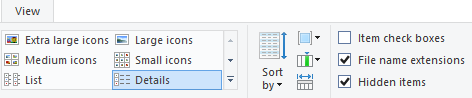


1. Using VMware Workstation, power on and login to the Win10 VM that will be the Server.

Username : admin

Default password : 1qwer$#@!

1. To change the size of the VM screen, right-click on the background and choose "Display settings". Click "Advanced display settings".
2. Choose your desired Screen Resolution. Click Apply.
3. In Windows Explorer, click on View menu.
4. Check the boxes for “File name extensions” and “Hidden items”.



1. Browse to www.wireshark.org and download and install Wireshark (64-bit version) with default options. You can also download the Wireshark installation file from the previous Dropbox link, under "Files-for-Topic1".
2. Using VMware Workstation, power on and login to the Win10 VM that will be the Client.

Username : admin

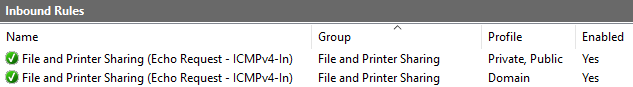
Default password : 1qwer$#@!

**Exercise Accessing a shared folder without VPN.**

Description : First you will access shared files without any VPN setup.

In Win10 VM (Server):

1. In the Search textbox, type “Firewall” and run Windows Firewall with Advanced Security.
2. In the left hand pane, click Inbound Rules.
3. Look for the two rules “File and Printer Sharing (Echo Request – ICMPv4-In)”. Right-click on both rules and choose “Enable Rule”. This will allow other systems in the Private, Public and Domain profiles to ping to the Win10 VM.



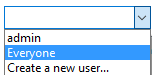
1. Create a folder called “shared” in C drive.
2. Create a text document called “flower.txt” in the “shared” folder.
3. Edit flower.txt to have the following contents (you can enter other text if you wish) :

rose

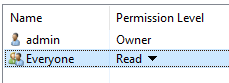
violet

lily

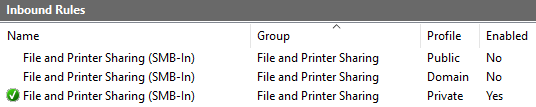
1. Right-click on the shared folder and select “Share with”, “Specific people”.
2. In the textbox for entering a name, click on the arrow and select Everyone.



1. Click Add to give the Everyone group Read access to the shared folder.



1. Click Share.
2. If asked about turning on network discovery and file sharing for all public networks, you can click No.
3. Click Done.
4. In Windows Firewall with Advanced Security, click Inbound Rules.
5. Check that the rule File and Printer Sharing (SMB-In) for Private profile is enabled.



Check that File and Printer Sharing (SMB-In) is enabled for Private profile

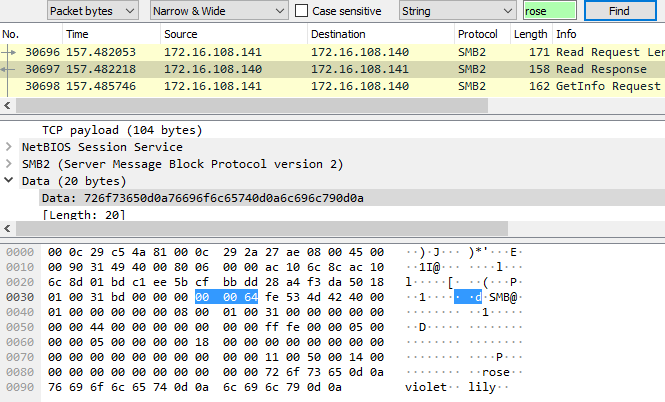
1. In the bottom left corner, click on the Windows icon and choose All apps. Look for Wireshark and run it.
2. In Wireshark, go to the Capture menu and select Options to select the network interface to capture packets on.
3. Click on the Ethernet interface and click Start.

In Win10 VM (Client):

1. In the bottom left corner, right-click on the Windows icon and choose Run.
2. Type “\\*Win10-ServerIP*\shared” where *Win10-ServerIP* is the IP of the Win10 that is the Server. A window will be opened, with flower.txt displayed.
3. Double-click on the flower.txt to view it. Close the file.
4. Close the shared folder window.

In Win10 VM (Server):

1. Stop the Wireshark capture.
2. In your Wireshark capture, can you find the packet containing the contents of flower.txt? (Tip : go to Edit menu, Find Packet. Set the Display filter to “String” and change “Packet list” to “Packet bytes” and do a search for “rose”. Or you can type “frame contains rose” in the Filter textbox to search for the string “rose”)



Questions :

Is there any encryption when accessing a shared folder over the network? no

What protocol is used when reading shared files over the network? Smb2

**Exercise Installing OpenVPN Community version**

Description :

OpenVPN is an open source VPN solution that uses the SSL/TLS protocol.

Normally OpenVPN clients and servers authenticate one another using certificates and keys in a public key infrastructure, but in this practical exercise, we will just use a simple static key solution for a single server and a single client.

In both Win10 VMs (Server and Client):

1. Browse to <https://openvpn.net/community-downloads> and download the latest stable OpenVPN installation file for Windows 10. You can also download the OpenVPN installation file from the previous Dropbox link under “Files-for-Topic8”.
2. Install the OpenVPN with default options.
3. Accept all the default values and click Next.

**Exercise Setting up the VPN Server and VPN Client with a Static Key**

Description:

OpenVPN runs on UDP port 1194 by default. The following IP addresses will be used for the VPN tunnel.

Windows 10

VPN Server

(on UDP Port 1194)

Windows 10

VPN Client

VPN tunnel

IP : 10.8.0.2

IP : 10.8.0.1

In Win10 VM (Server):

1. In the bottom left corner, click on the Windows icon and select All apps. Look for OpenVPN. Right-click on “Generate a static OpenVPN key” and choose “Run as administrator”.

A static key has been generated and saved in C:\Program Files\OpenVPN\config\key.txt”. You can open this file to see the key value.

1. Copy the generated key.txt to the shared folder.
2. Start Notepad as Administrator.
3. Enter the following contents:

dev tun

ifconfig 10.8.0.1 10.8.0.2

secret key.txt

1. Save the file as “server.ovpn” in the C:\Program Files\OpenVPN\config folder.

In Win10 VM (Client):

1. Access the shared folder from the Win10 (Server) and copy key.txt to C:\Program Files\OpenVPN\config.
2. Close the shared folder window.
3. Start Notepad as Administrator.
4. Enter the following contents, replacing *Win10-ServerIP* with the IP address of the Win10 that will be the VPN Server:

dev tun

remote *Win10-ServerIP*

ifconfig 10.8.0.2 10.8.0.1

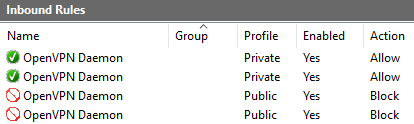
secret key.txt

1. Save the file as “client.ovpn” in the C:\Program Files\OpenVPN\config folder.

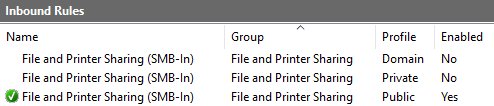
**Exercise Connecting to OpenVPN**

In Win10 VM (Server):

1. In the bottom left corner, click on the Windows icon and choose All apps. Look for OpenVPN and run OpenVPN GUI. An OpenVPN GUI icon will appear in the System tray of the Taskbar.
2. Right-click on the OpenVPN GUI icon and choose Connect.
3. If a Windows Firewall popup appears asking if you want to allow OpenVPN to communicate on private networks, click “Allow access” so that Windows Firewall will allow connections to the OpenVPN. (you can always make changes to the Windows Firewall later)
4. Run Windows Firewall with Advanced Security and click on Inbound Rules. The following rules were added to allow connections to the OpenVPN for Private profiles, and to block connections to the OpenVPN for Public profiles.



1. In Windows Firewall with Advanced Security, Inbound Rules, look for the rules “File and Printer Sharing (SMB-In)”. Disable the rule for Private profile and Enable the rule for Public profile.



When the Win10 (Client) tries to access the shared folder, it will not be able to do so over the default private connection, but it has to go through the OpenVPN connection.

In Win10 VM (Client):

1. In the bottom left corner, click on the Windows icon and choose All apps. Look for OpenVPN and run OpenVPN GUI. An OpenVPN GUI icon will appear in the System tray of the Taskbar.
2. Right-click on the OpenVPN GUI icon and choose Connect.
3. If a Windows Firewall popup appears asking if you want to allow OpenVPN to communicate on private networks, click “Allow access” so that Windows Firewall will allow connections to the OpenVPN. (you can always make changes to the Windows Firewall later)

On both Win10 VMs (Server and Client) :

1. When the connection is successful, the OpenVPN GUI icon in the System Tray will turn green. Use ipconfig to see your VPN IP address (either 10.8.0.1 or 10.8.0.2).

**Exercise Capturing network packets through VPN**

In Win10 VM (Server):

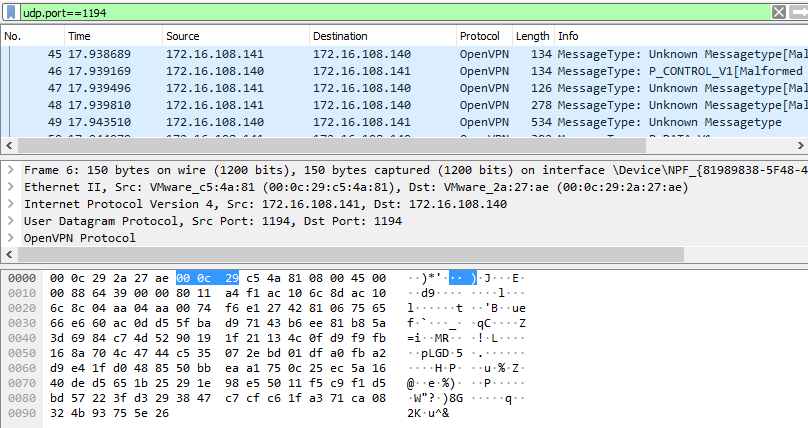
1. Run Wireshark and start capturing packets on the Ethernet interface.

In Win10 VM (Client):

1. Access the shared folder on the VPN Server using \\10.8.0.1\shared. Double-click on the VPN Server’s flower.txt to view it.

In Win10 VM (Server):

1. Stop the Wireshark capture.
2. In your Wireshark capture, can you find the packet containing the contents of flower.txt? You should not be able to see the contents in cleartext.
3. Look for packets going to and from the VPN Server’s UDP port 1194. The contents of these packets are encrypted.



1. Close the shared folder window.
2. Disconnect from the VPN connection.

In Win10 VM (Client):

1. Disconnect from the VPN connection.

*End of Practical*