CONESTOGA College

Course	**INFO8965: Computer and Network Security**
Activity	**Internet Traffic Analysis**
Student Name	
Date performed	

Note:

- For IP addressing in this lab, **XY** represents the last two digits of your student ID.
- This lab activity must be attempted individually.
- Use the given lab report template to provide required output/information.
- Submission instructions are also provided at this lab handout.

Objectives

- Analyse network traffic using traffic capture utility like Wireshark.
- Setup an FTP server in a Virtual Machine

Resources

- PC / Laptop
- Virtual Box: https://www.virtualbox.org/wiki/Downloads
- Windows 10 VM / Windows 11 VM
- Wireshark: https://www.wireshark.org/download.html
- FileZilla: https://filezilla-project.org/

Reference(s)

- Learn more about VirtualBox networking modes:
  https://www.virtualbox.org/manual/ch06.html
  https://www.nakivo.com/blog/virtualbox-network-setting-guide/

(A) Capturing and Analyzing FTP Traffic

Task 1: Install and Run FTP Server

(a) Use Host-only Adapter configuration for your Windows 10 VM.

- VirtualBox > File > Host Network Manager
- Select the VirtualBox Host-Only Ethernet Adapter
  - Click create if it does not exist yet.
- Click Properties and assign the following values.
  - IPv4 Address: 192.168.**XY**.1 (**Note**: XY in this IP address represents the last two digits of your student ID).
  - IPv4 Network Mask: 255.255.255.0
  - Click DHCP server tab.
  - Select Enable Server and change the fields as given below.
    - Server address: 192.168.XY.100
    - Server mask: 255.255.255.0
    - Lower address bound: 192.168.XY.101
    - Upper address bound: 192.168.XY.254
- Click Apply. Make sure that DHCP server is enabled. Close Host Network Manager.
- VirtualBox > Right click Windows 10 VM > Settings.
  - Select Network from the left-hand pane and confirm the settings as shown below in figure 1.

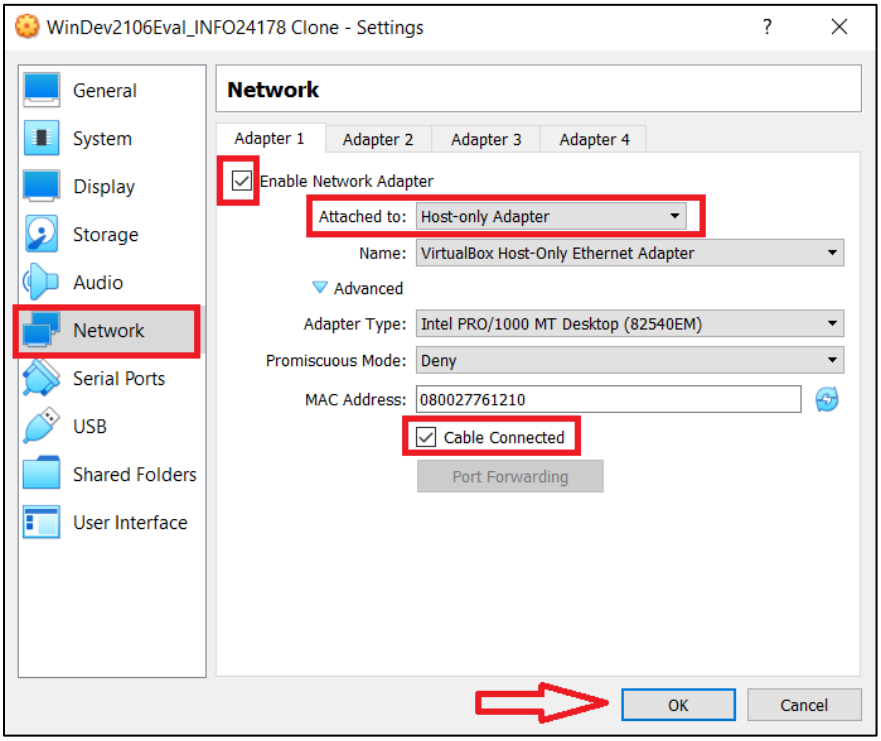

Figure 1: Using Host-Only Adapter for the VM

(b) VirtualBox has a powerful feature known as snapshots that allows users to save the current state of their VM. At any point in the future, you can restore the VM to this state no matter

how much changes have been made to the VM since last snapshot. Take a snapshot of your Windows 10 VM as shown in figure 2.

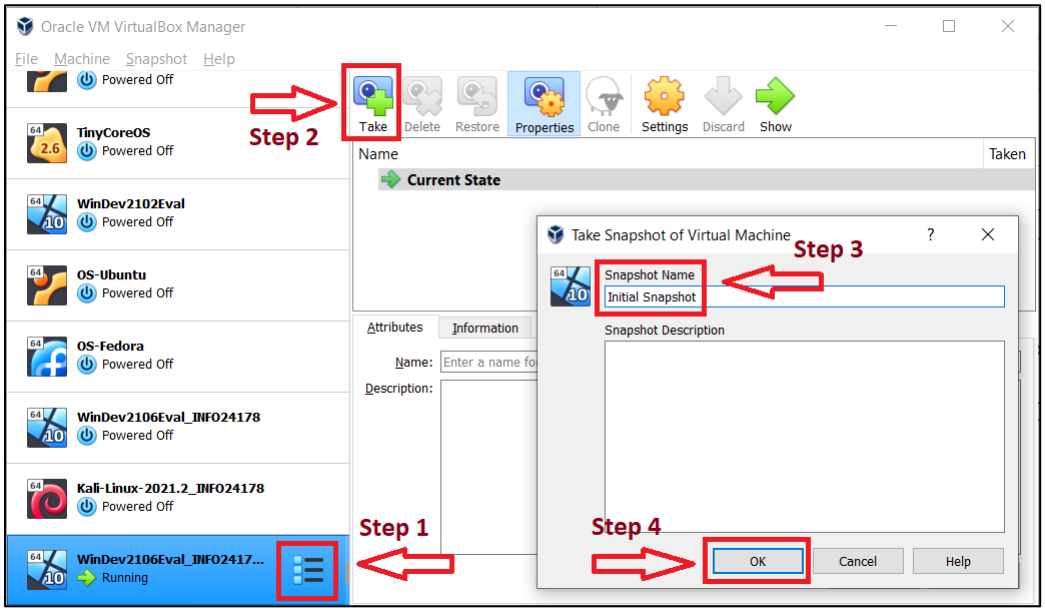

Figure 2: Creating a Snapshot of the VM in Virtual Box

(c) Install Cerberus software on your **Windows 10 VM**. For convenience, a zipped file is also shared under Contents>Week 5. During installation and initial configurations, make sure to change the settings as explained in the following figures.

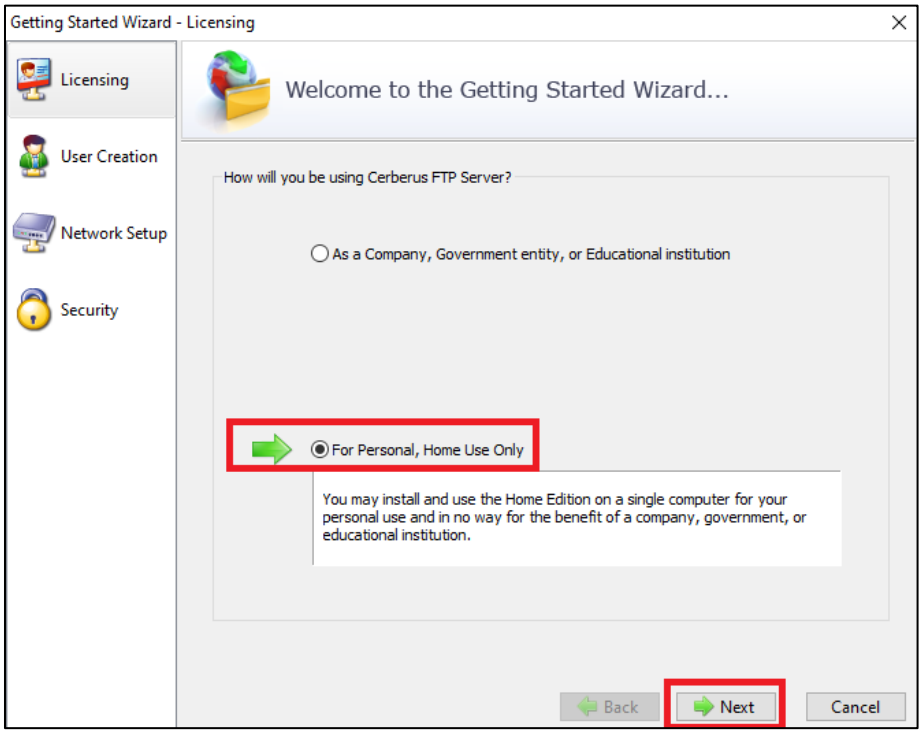

Figure 3: Installing Cerberus for personal use only.

Keep the 'Anonymous' username as you do not need to create any new user. (Of course, you can create one for testing).

Notice that the server will create a folder called '**ftproot'** in your C drive. Go to the C drive of your Windows 10 VM and create a text file in this folder. Write something interesting in it and save it with your name.

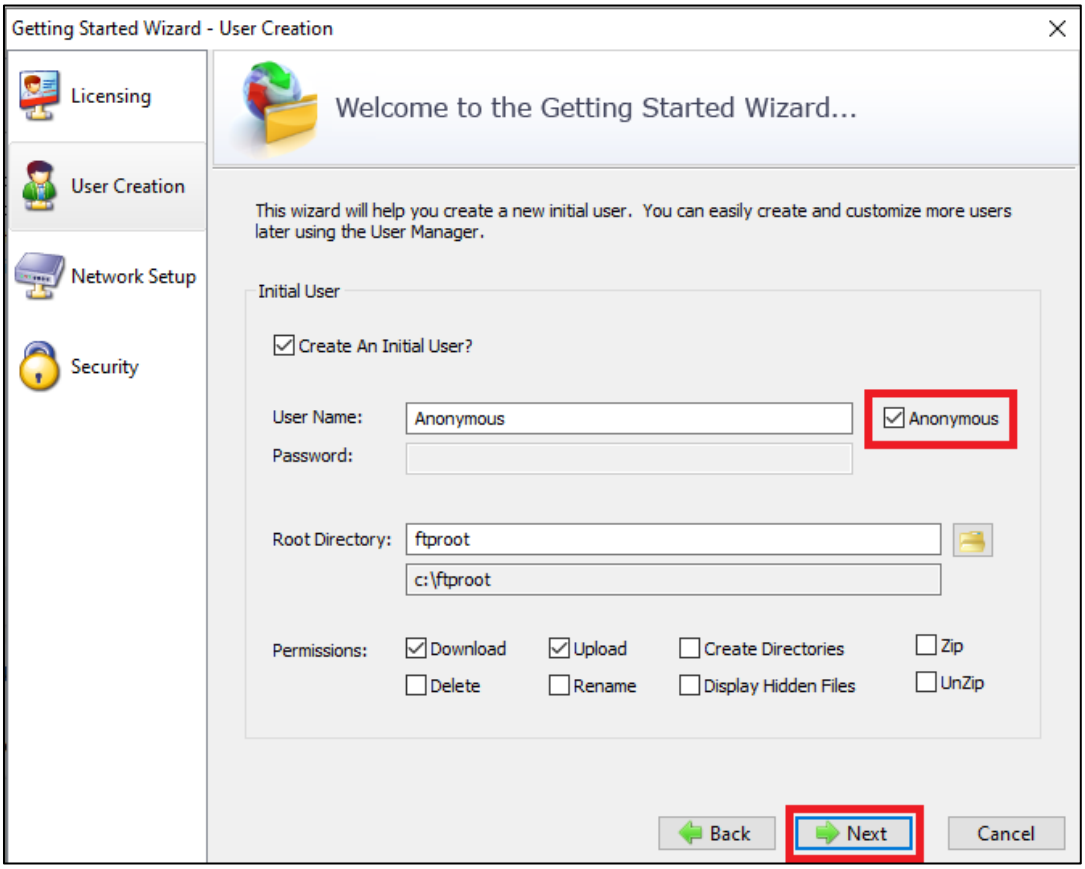

Figure 4: Initial configuration – Anonymous username

Oracle VM VirtualBox provides several networking adapters that can be separately configured to operate in one of the following modes. You can read more about them using the references provided at the start of this lab handout.

- Not attached
- Network Address Translation (NAT)
- NAT Network
- Bridged networking
- Host-only networking

For this lab activity, we will use Host-only networking that is used to create a network containing the host and a set of VMs without the need for the host's physical network interface. A virtual network interface like a loopback interface is created on the host for communicating between a host and guest VM. In case of host-only adapter networking, the

setup will remain unable to detect public address. Simply click ‘Next’ in this case as shown in figure 5.

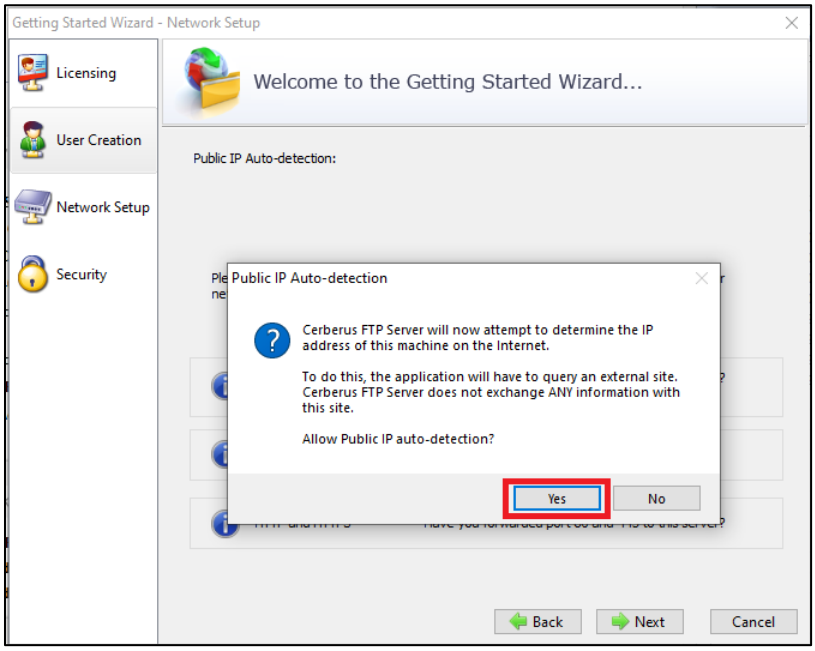

Figure 5: Detecting public IP addresses

Uncheck ‘Do not Allow Unencrypted FTP’ option as shown in figure 6.

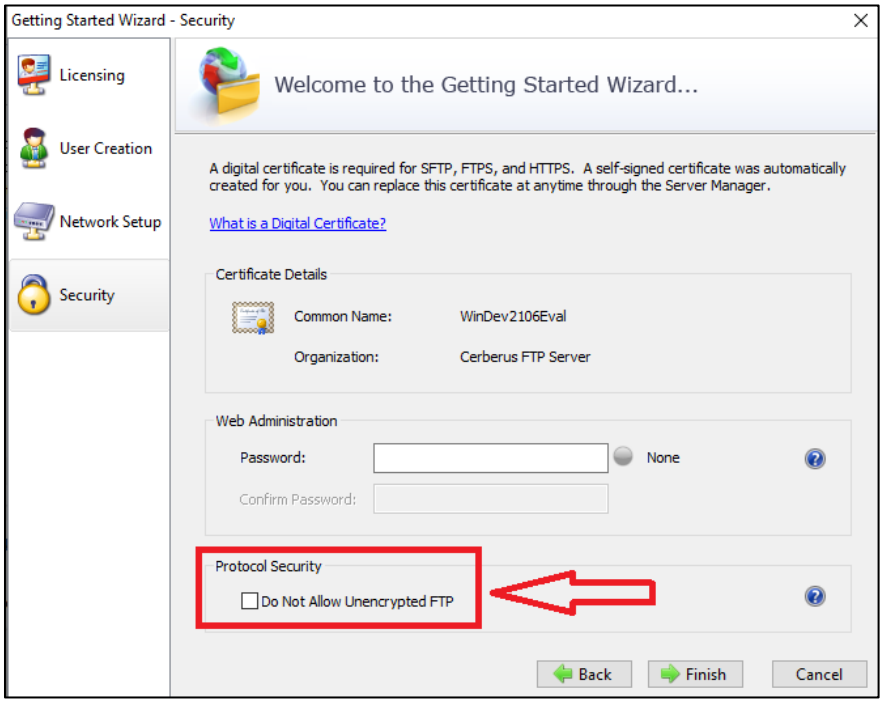

Figure 6: Permitting unencrypted FTP traffic.

To capture and analyse the FTP traffic in plain, disable secure control and data as shown in figure 7 (Cerberus>Configure>Interfaces) and figure 8 (Cerberus>Configure>Security).

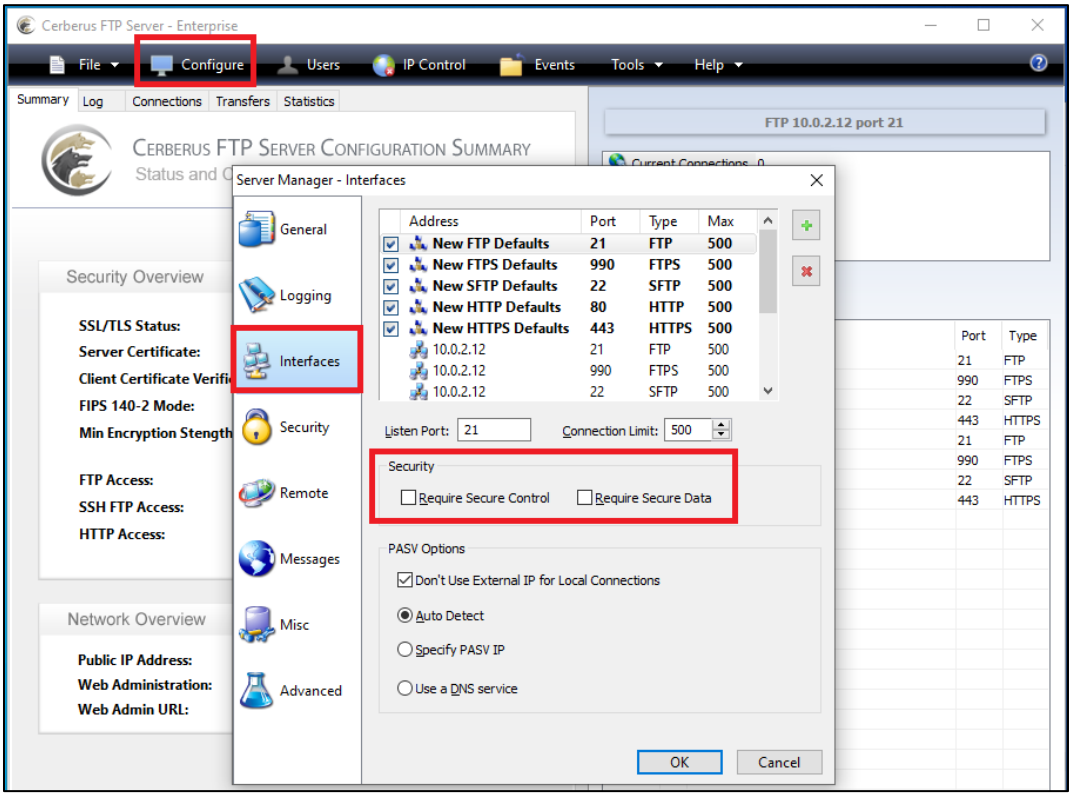

Figure 7: Disabling secure control and data

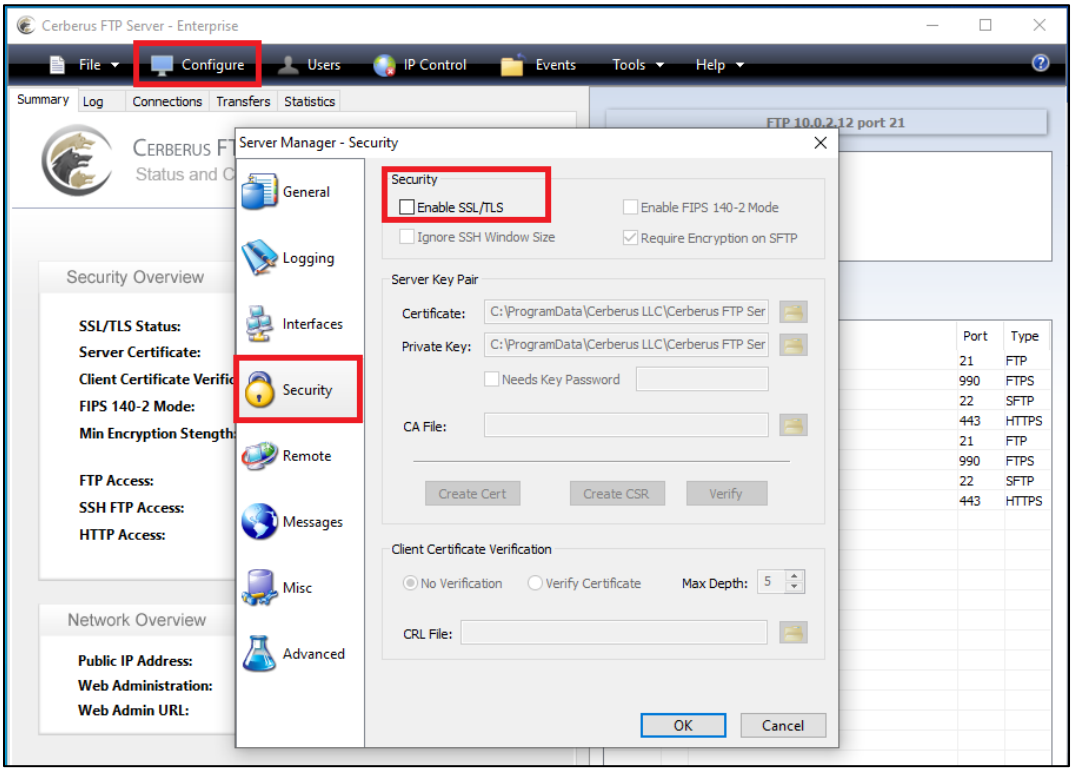

Figure 8: Disable SSL/TLS

Set a password for anonymous user as shown in figure 9. Cerberus > Users > Click Anonymous.

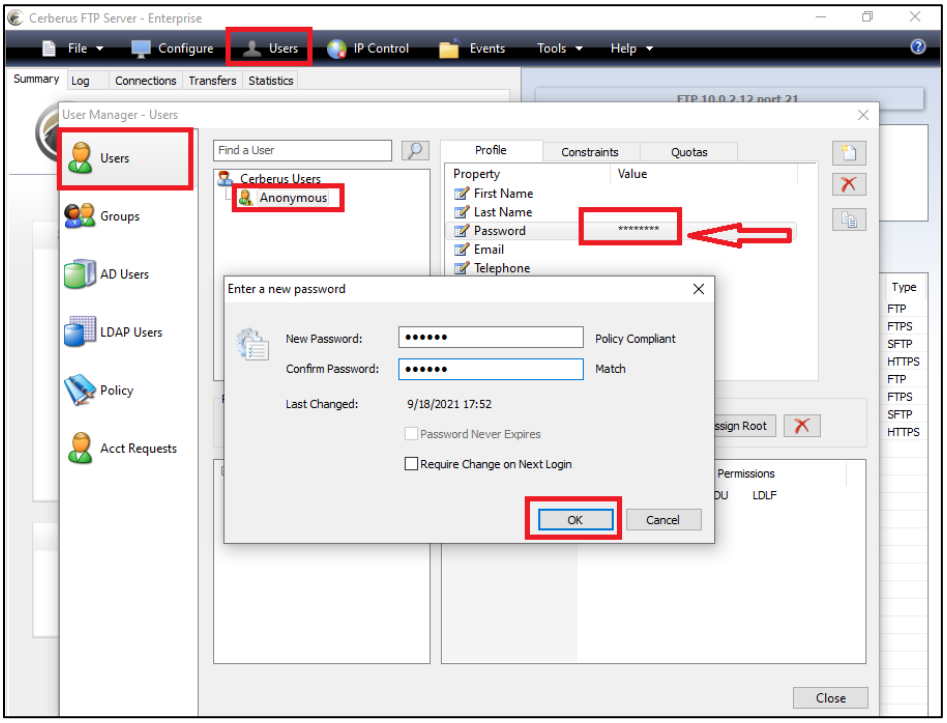

Figure 9: Set a password for the Anonymous user.

Note down the IP address for the FTP server as shown in figure 10. **Note:** In your case this IP address might be different.

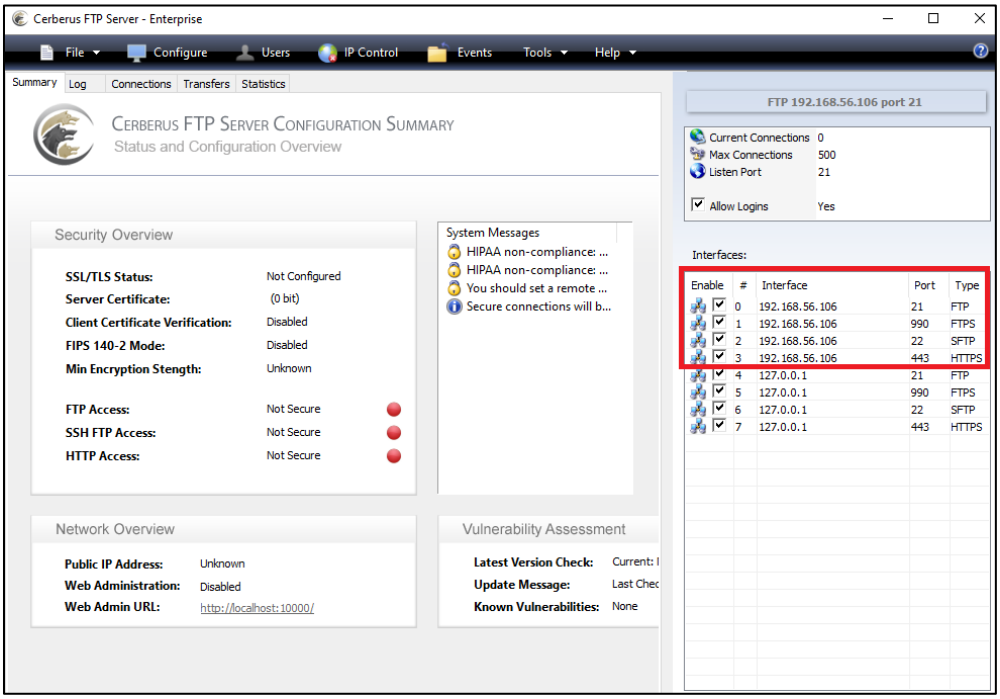

Figure 10: IP address for Cerberus FTP Server

Task 2: Download File and Capture FTP Transactions

a) Download and install an open-source FTP client FileZilla from https://filezilla-project.org/. Note: Install the **FileZilla Client** and NOT FileZilla Server. During installation, you do not need to change any default setting(s).

b) Start Wireshark on your host machine. Double click 'VirtualBox Host-Only Network' interface to begin traffic capture as shown in figure 11.

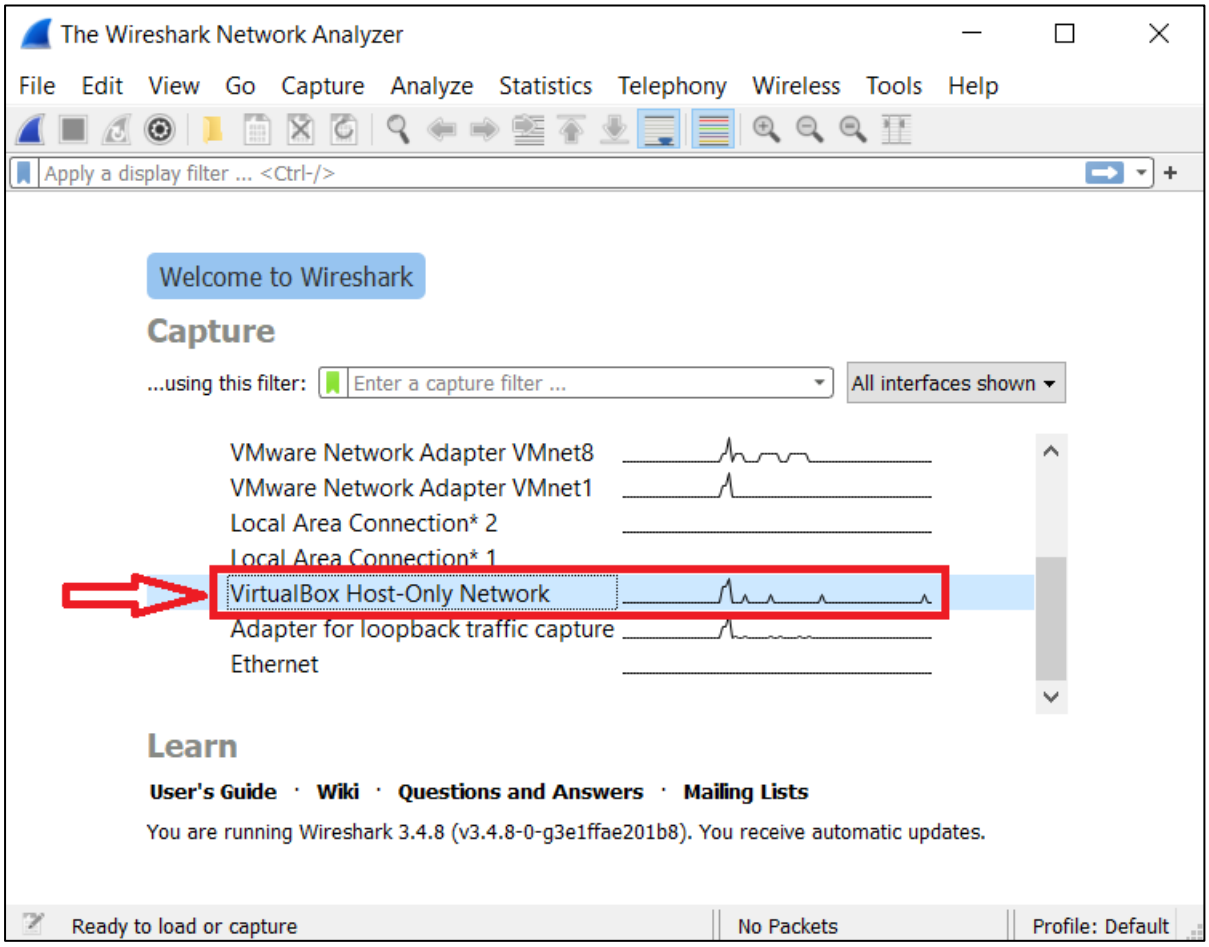

Figure 11: Select the network interface and start capturing traffic

c) Open FileZilla client on your host machine and provide appropriate values for Host, Username and Password fields. Then click Quickconnect as shown in figure 12, to open the FTP connection and retrieve directory listing.

Go to Cerberus FTP Server in VM and observe the log messages for these transactions. (Cerberus> Log).

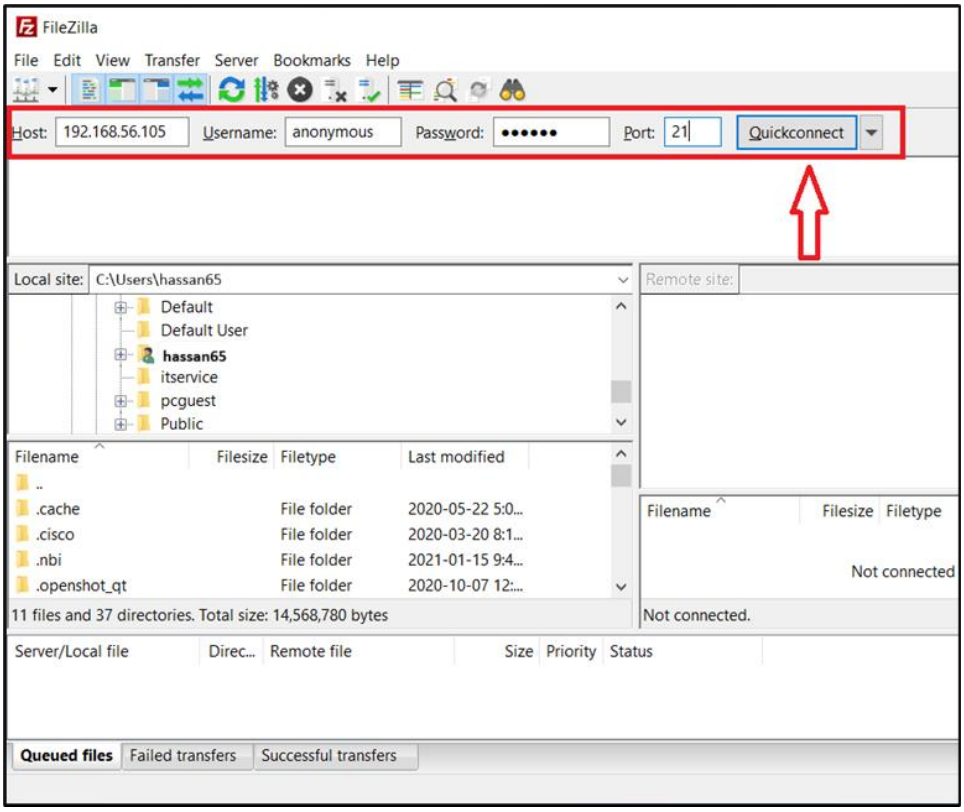

Figure 12: FileZilla Client – Connect to FTP server running on VM

In FileZilla Client, select the file hosted on FTP server, right click and download it as shown in the figure 13.

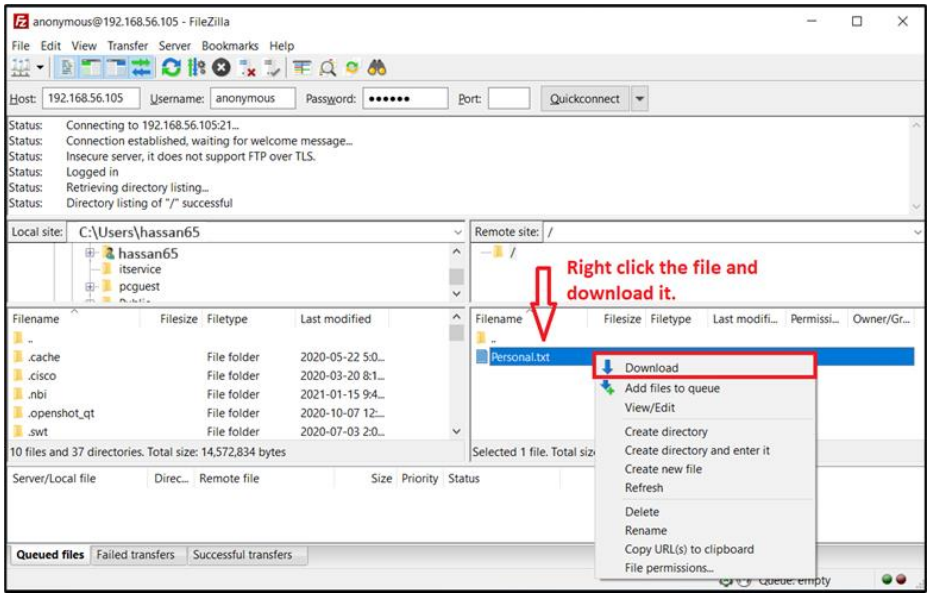

Figure 13: Download your file that is hosted on FTP server.

d) Stop the Wireshark capture and use the filter '**tcp.port == 21 or tcp.port == 20**' to see only FTP related traffic captures as shown in figure 14.

FTP is a protocol used by computers to share information over the network and is optimized for large file transfers between computers. The FTP client first establishes a control connection request to the server port 21. Control connection requires a username password to establish a connection. Later, a separate data connection is established to transfer files and folder.

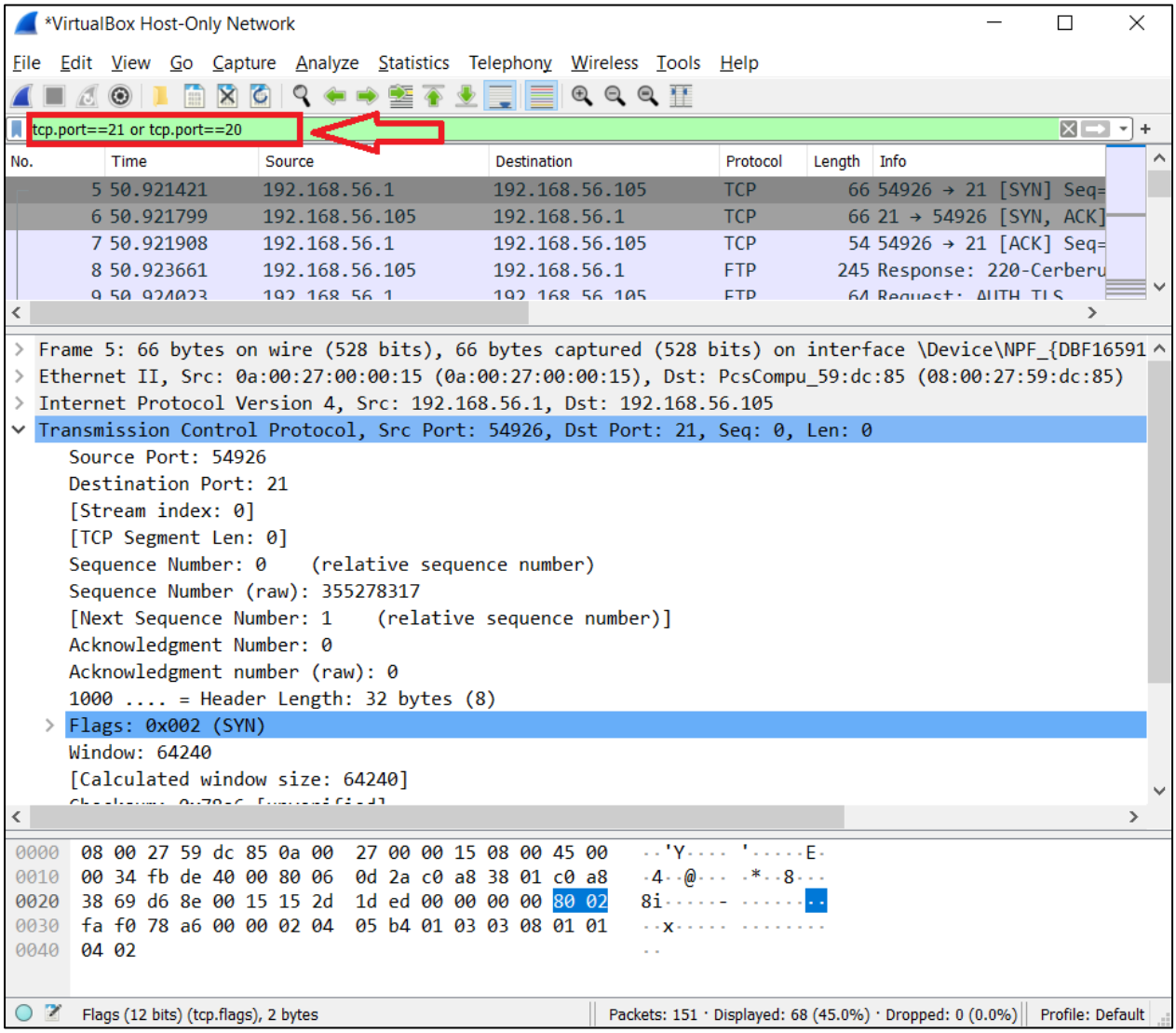

Figure 14: Apply filter to view only FTP related traffic

e) In the listed packets, identify the packets related to initial FTP login transactions. Find the frames that correspond to the username and password transaction. Notice that both username and password are supplied in clear text. Take a screen capture and paste it in **Output # 1** (Use Lab Report Template to complete this lab activity). Make sure that required packets are clearly highlighted. You can use any drawing tool for this purpose.

f) In Wireshark, from the menu, select Statistics → FlowGraph. Change the flow type to TCP flows and enable 'Limit to display filter'. A flow graph similar to that shown in figure 15 will appear. This graph clearly shows the TCP handshakes.

Find out how many 3-way handshakes occurred. Take their screen capture, highlight these handshakes, and paste them in **Output # 2**.

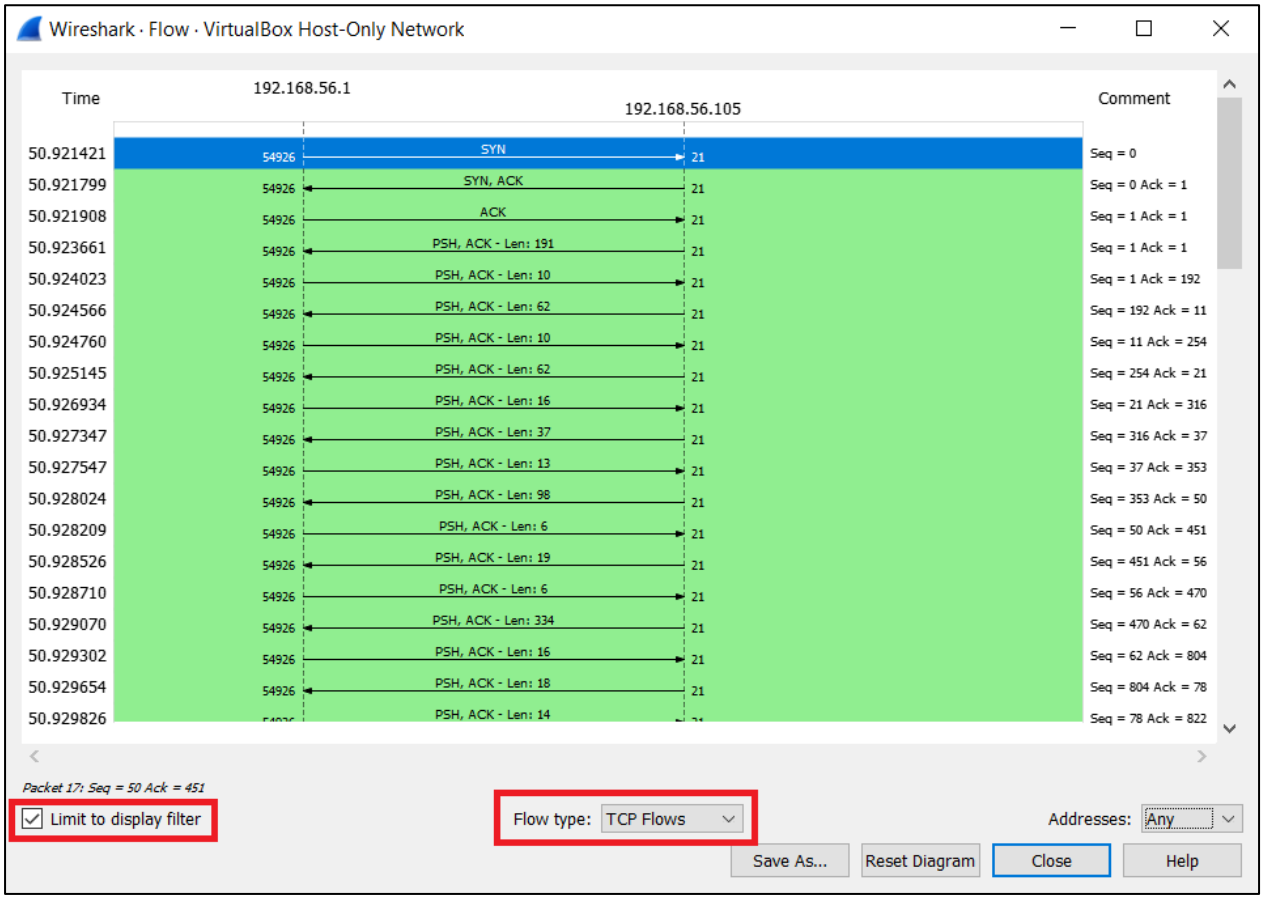

Figure 15: Flow graph in Wireshark

g) In the main Wireshark capture window, find the frames that correspond to the transfer of the actual file. Notice that the file is transferred in clear text. Take a screenshot, clearly highlight these packets, and add them to **Output # 3**.

(C) Submission Check List		
	To Do	**Done**
1	Please use the provided **Lab report template** to complete attempt. Make sure the form in the cover page is filled up.	
2	Provide all the required outputs.	
3	Give appropriate title or captions (small description) to all the output boxes. (10% marks per output will be deducted, if they are not properly captioned)	
4	Submit your report as instructed.	