CIT210/L OP. SYS. MANAGE (Lab Assignment 3) (80 Points)

Lab 3 : Installing and Configuring Network Applications (Web Server, FTP, TFTP)

Tools and Software

The following software and/or utilities are required to complete this lab.

Server 2016/2019/2022 Installation

- FileZilla Server (You can Install Linux Server as FTP server)
- Tftpd64

Client Windows 10/11 Installation

- PuTTY
- FileZilla Client
- Wireshark

Wireshark Captures

Wireshark is a network packet analyzer (also known as a packet sniffer). Wireshark is a computer program that can intercept, log and display the traffic passing over a digital network (or part of a network). It can be used to log data traveling over a variety of network types (cable, wireless) and, provided that the content of the data packets is unencrypted, display that data in real time.

Packet sniffers like Wireshark can be used for a variety of purposes both good...

1. Analyze network problems and test network communication.
2. Debug client/server communications and other network protocol communications
3. Monitor network usage and bandwidth (including internal and external users and systems)
4. Detect network misuse by internal and external users
5. Detect network intrusion attempts (like port scanning).
6. Filter suspect content from network traffic

and bad...

- Gain information for effecting a network intrusion
- Spy on other network users and collect sensitive information such as passwords (depending on any content encryption methods which may be in use)

Getting Wireshark:

Wireshark is free and supported on all Windows, Mac and Linux/Unix machines. It can be obtained by going to:

http://www.wireshark.org/download.html

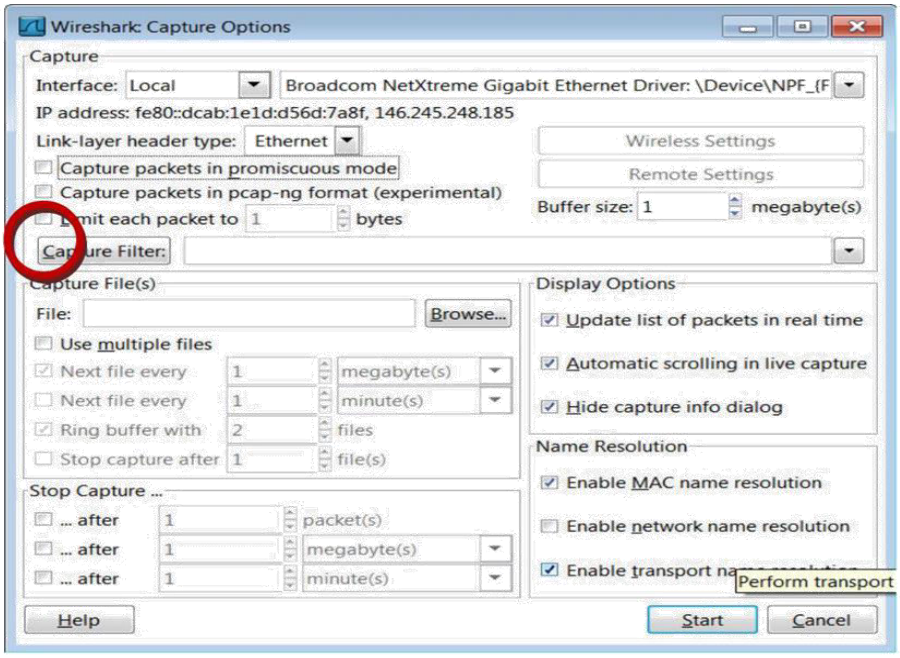
Select a Network Device

When you first start Wireshark you will be brought to the default startup screen. In order to begin a network capture you will need to choose a network device to use. There are several ways to do this: for now you can simply select the "List the Available Capture Devices" button, circled in red below.

In the pop-up box that appears you will need to select one of the devices available on your machine.

Most machines will only have one network interface available.

In the "Capture Options" window that appears uncheck the "Capture packets in promiscuous mode" checkbox (we only want to capture messages sent directly to your own machine). The click "Start" in both the "Capture Options" window and then in the "Capture Interfaces" window.



Running Wireshark

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will de displayed. Initially, no data will be displayed in the various windows.

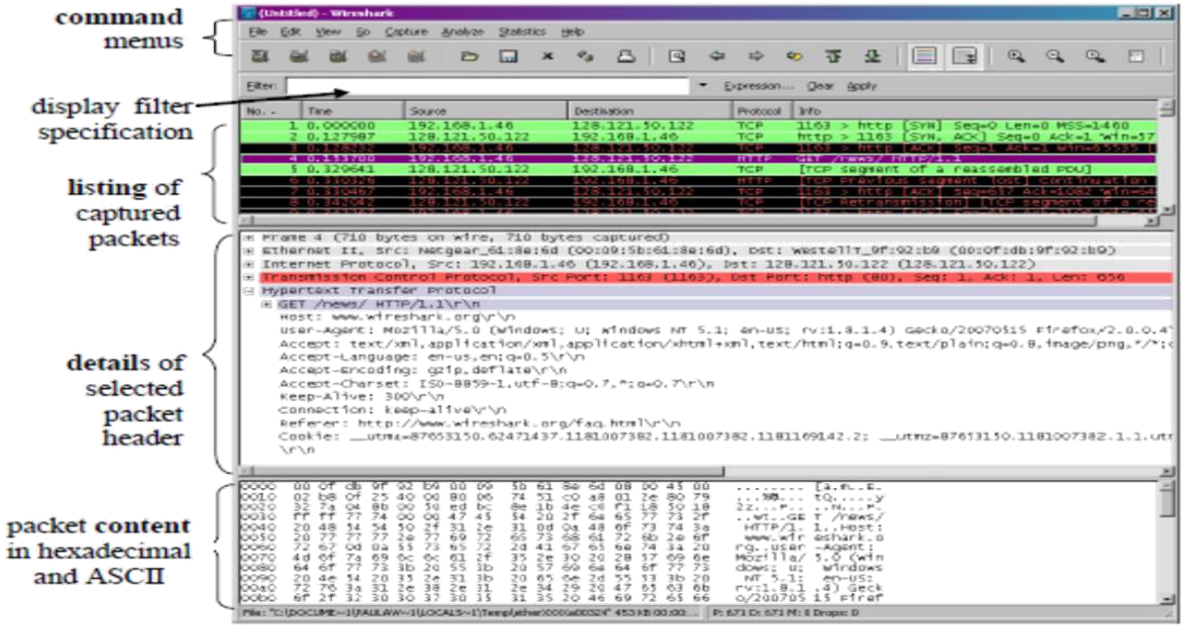
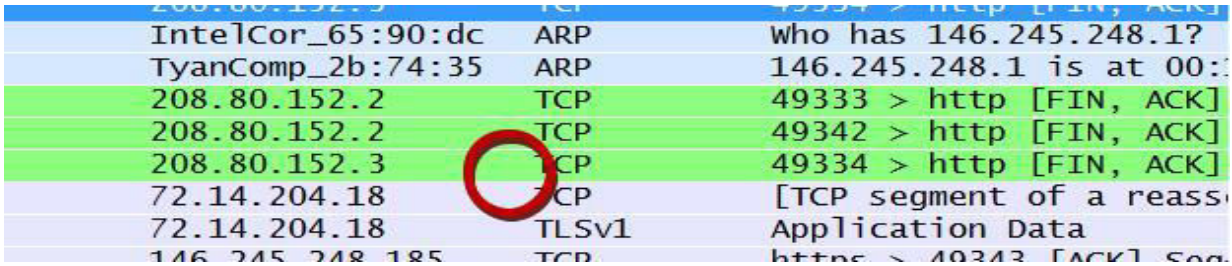
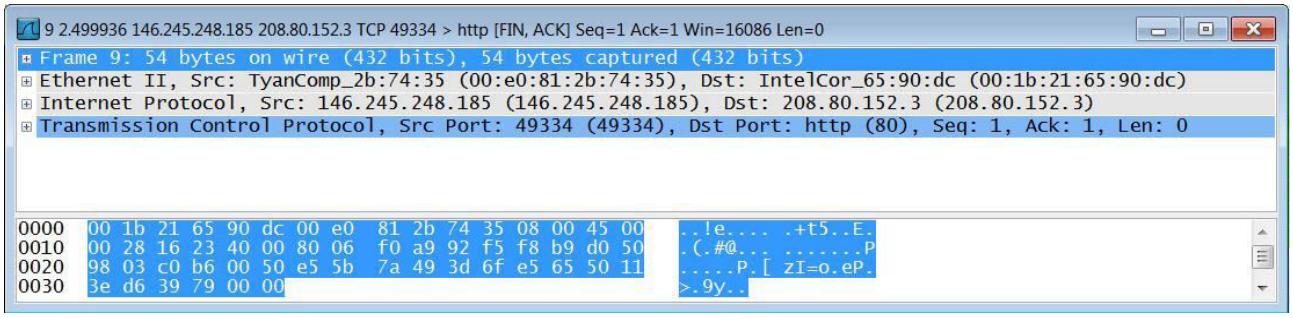


Figure 2: Wireshark Graphical User Interface

Mac Addresses, IPv4 Addresses, Port Addresses
Look in your packet capture window for a packet that is using the TCP protocol.



Double click on the packet line to obtain more details about that specific packet:



Task 1: Install Configure and run Wireshark software and capture traffic: (10 Points)

Task 2: Open couple of websites, capture http communication and answer the following questions: (10 Points)

a. Which version of the HTTP protocol is used in these transactions?
b. What is the domain name of the Web server?
c. What browser and version does the client use in this capture?
d. What software and version is running on the Web server?
e. What other documents/files did the client request during this transaction?

Task 3: Basic Apache Configuration (30 Points)

Exercise 1: Installation and Basic Configuration of the Apache Web Server (8 points)

1. Open a terminal window and check whether the Apache Web Server is installed by using the command
(Deliverables: Screenshot Command)_____

2. If it is not, use yum(Cent OS) or apt-get (Ubuntu)at the command line to install the httpd and httpd-manual packages. They are small and should not take too long to download and install.

(Deliverables: Screenshot Command)_____

Exercise 2: Locating key Apache files and folders (12 Points)
1. Locate each of the following files on your hard disk drive and record their locations:

• Apache Reference Manual
_____
• Apache configuration file
_____
• Document root
_____
• Error documents directory
_____
• Log files
_____
• The Apache daemon (executable)
_____

Exercise 3: Configure and Run Apache Web Server (10 Points)

1. Find and Edit the Apache configuration file if needed.

2. Start the Apache Web server

3. A window stating **httpd start successful** should appear. Click **OK**.

4. Check that the server is running on port 80 by using the command

netstat -npl | grep httpd

Answer the following Question
1. What special user and group name does Linux use for running apache?
2. How can you test your Apache installation?
3. What are the log files generated by Apache?
4. What is Virtual Hosting?
5. How to secure Website hosted on Apache Web Server?

Task 4: Install, Configure Connect FTP Server (Filezilla server or (any other FTP Server), Filezilla client can be used if you are using Windows System) . Do file transfers, Capture and record communication with Wireshark. (20 Points)

Screenshot: Capture the communication and find ftp ports used for communication.

FileZilla is an open source FTP client, it is available on multiple platforms like Linux and Windows. This client also supports FTP over secured connections that is SFTP and FTPS. You can use this software to upload and manage your files in your webserver. When you wish to upload your website and number of files are more or size of files are very large. Then you can use FTP upload, because uploading a file of very large size through cPanel File Manager can cause an error in uploading.

Most of the cPanel accounts comes with a system FTP account, through which you can access and manage all the files in your home directory. Passwords of system account for cPanel and FTP are same in most cases.

To use FileZilla FTP client, to manage and upload the website, please follow these steps −

Step 1 − Download and install FileZilla FTP client from FileZilla website. The installation process of this software is the same as other software's.

https://filezilla–project.org/download.php

Step 2 − After installing open your FileZilla FTP client. In the quick connect bar, you will find text box to provide hostname. Enter your ftp hostname, which can be IP address of your server or **ftp.<your_domain.com>**.

Step 3 − Enter the username and password for your ftp account.

Step 4 − Enter Port on which you want to connect to your FTP server. In most of the cases, it is 21, but if you leave this field empty then FileZilla will automatically find the appropriate port to connect.

Step 5 − Click Quickconnect to connect to the FTP server.

Step 6 − After a successful connection, you can move or copy files from the left hand side pane (which are your local computer directories) to the Right hand pane (which are your remote server directories and files). You can drag and drop files from the left to right pane or vice versa.

Step 7 − You can view the status of your moving or copying in the pane, which is on the lower side of the interface.

1. What are the defaults ports used in linux ftp server ?
2. What Is Active and Passive Mode?
3. How would you manage number of FTP clients that connect to your FTP server?
4. How to limit the FTP login attempts to fight against botnet/illegal login attempts?
5. Is it Possible to maintain log of FTP requests and responses?

Task 5: Install Configure and Transfer files from tftp server to tftp client using tftp64 application (10 Points)

Screenshot: Capture the communication and find tftp port used for communication

1. What is the Difference between TFTP and FTP Server?