National University of Computer and Emerging Sciences

Laboratory Manuals

for

Computer Networks

(CL -3001)

Course Instructor	Dr. Arshad Ali
Lab Instructor(s)	Ms. Zoha Waheed
Section	BCS-5A
Semester	Fall 2024

Department of Computer Science
FAST-NU, Lahore, Pakistan

Lab Manual 04

Objective:

- Analyzing the **FTP** packets using Wireshark
- Analyzing the **ICMP** packets using Wireshark

Lab Statement 1: Capturing FTP packets using Wireshark (10)

Step 1: **Start a Wireshark capture.**

a. Close all unnecessary network traffic, such as the web browser, to limit the amount traffic during the Wireshark capture.

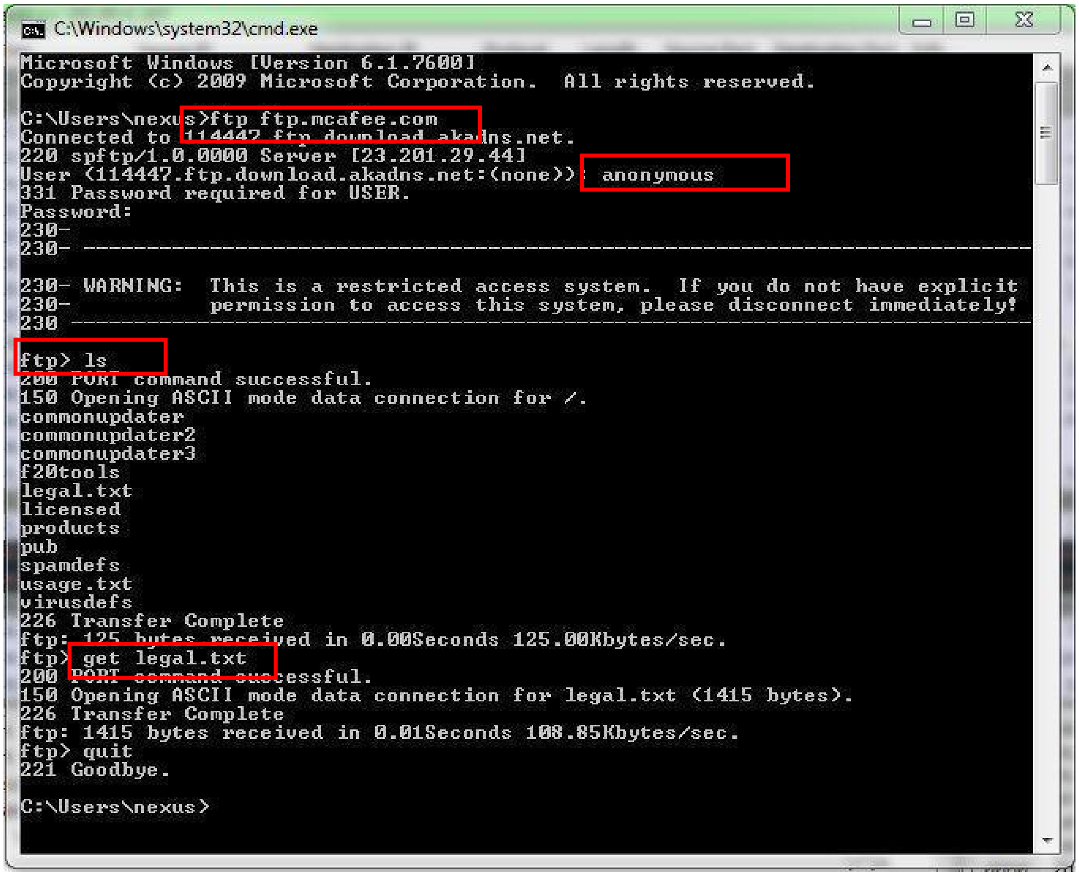
b. Start the Wireshark capture.

Step 2: **Download the .txt file.**

a. From the command prompt, enter ftp ftp.mcafee.com

b. Log into the FTP site for mcafee.com with user **anonymous** and no password.

c. Locate and download any .txt file.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\nexus>ftp ftp.mcafee.com
Connected to 114447.ftp.download.akadns.net.
220 spftp/1.0.0000 Server [23.201.29.44]
User (114447.ftp.download.akadns.net:(none)): anonymous
331 Password required for USER.
Password:
230-
230- ---------------------------------------------------------------------------

230- WARNING:  This is a restricted access system.  If you do not have explicit
230-           permission to access this system, please disconnect immediately!
230 ----------------------------------------------------------------------------

ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /.
commonupdater
commonupdater2
commonupdater3
f20tools
legal.txt
licensed
products
pub
spamdefs
usage.txt
virusdefs
226 Transfer Complete
ftp: 125 bytes received in 0.00Seconds 125.00Kbytes/sec.
ftp> get legal.txt
200 PORT command successful.
150 Opening ASCII mode data connection for legal.txt (1415 bytes).
226 Transfer Complete
ftp: 1415 bytes received in 0.01Seconds 108.85Kbytes/sec.
ftp> quit
221 Goodbye.

C:\Users\nexus>
```

Step 3: **Stop the Wireshark capture.**

Step 4: **View the Wireshark Main Window**

Wireshark captured many packets during the FTP session to ftp.mcafee.com. To limit the amount of data for analysis, type **tcp and ip.addr == 195.89.6.167** in the Filter. The IP address, **195.89.6.167**, is the address for ftp.mcafee.com.

Step 5: **Analyze the packets**

Carefully analyze the packets in Wireshark windows and answer the following question:

Use the FTP_Session.pcapng (Wireshark Capture File) to answer the questions below

1. FTP uses two port numbers: 20 and 21. Apply **tcp.port==20** and **tcp.port==21**. Analyze the result and write down the purposes of these two ports for FTP.

2. Filter out each packet using either FTP or FTP-DATA Protocol (using **ftp || ftp-data** filter). Mention each packet number and its purpose with reference to request made and response received in the above mentioned FTP Session in command line to get file legal.txt

(screenshot show above). Also look for **Response Code** and **Response Arg** in the FTP Header for each packet

(There are **19 such packets** and you have to write one/two lines explanation for each packet, what the packet is doing w.r.t FTP Session (Screenshot shown above) **e.g., Packet 104: Client asks server to send the data on IP:192.168.1.2 and Port:16341** [63(0x3F),213(0xD5) and **(0x3FD5=16341)])**

Lab Statement 2: Analyzing ICMP Packets using Wireshark (10)

- **Step 1:** Run Wireshark
- **Step 2:** Load the Session file **ICMP_Session**

- **Step 3:** Now filter out all non-ICMP packets by typing "icmp" (without quotes) in the filter field towards the top of the Wireshark window

- **Step 4:** Analyze the ICMP Packets and answer the following questions

1- Are ICMP messages sent over UDP or TCP?	
2- What is the link-layer (e.g., Ethernet) address of the host?	
3- Which kind of request is sent through these ICMP packets?	
4- How many requests are sent through the host?	
5- What is the IP address of your host? What is the IP address of the destination host?	
6- Why is it that an ICMP packet does not have source and destination port numbers?	

7- What values in the ICMP request message differentiate this message from the ICMP reply message?	
8- Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	
9- Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	
10-Examine the packet no 56. What are the ICMP type and code numbers? Why is the IP and TCP Header included in the ICMP Header? What does these headers depict?	