**CPS3498 Computers Security**

**Lab 3: Network Transport and Applications**

**Description:**

Networks work by transporting data from point A to point Z, and vice versa. Protocols standards are established to control data communication. Internet Control Message Protocol (ICMP) is a transport protocol used between different devices on an IP network to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. User Datagram Protocol (UDP) is a connectionless (without requiring prior communications to set up special transmission channels or data paths) transport protocol used to send small amount of data, where the timeliness of the traffic is more important than the completeness of the traffic. Transmission Control Protocol (TCP) is a connection-oriented protocol to provide reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer.

There are various applications using TCP/IP for data communication. Understanding the nature of the data communication with these protocols is a necessary step toward establishing secure connection. File Transfer Protocol (FTP) is a protocol for file sharing that is often utilized for upload and download files from a server. Simple Mail Transfer Protocol (SMTP) is used for sending Email message between servers and operates on TCP port 25. Messages sent are retrieved by using either Post Office Protocol version 3 (POP3) or Internet Message Access Protocol version 4 (IMAPv4). POP3 operates on TCP port 110 and IMAP operates on TCP port 143.

This lab use tools such as netstat and Wireshark in Windows system to understand how IP packets interact with one another to establish connection and find information where it is supposed to go. And the same tools will be used to see the use of cleartext packet transfer of data between applications described in previous paragraph. Note that you may encounter difficulty in observing some data if you are not performing the lab procedures on campus.

**Procedure:**

**Lab 3.1 Network Transport**

**Lab A Network Communication Analysis in Windows**

1. Long on to a PC with the administrator account, or an account that has administrator privilege.
2. Open the command prompt. For Windows 7/8, click on Start, enter **cmd** in “Search program and file.” For Windows 10, type **cmd** on Cortana. Right click “cmd.exe” from search result and choose “Run as Administrator.” For Mac, start a **Terminal**.
3. At the command prompt, type **arp -a** and press Enter. There should be no entries. If there are, clear them with the **arp –d** or **netsh interface ip delete arpcache** and press Enter. You will need administrator privilege to delete any entry in the list. For Mac, type **sudo arp – d –a**.
4. Start Wireshark. The startup screen of the Wireshark displays the commands to use Wireshark.
5. Start capturing data by clicking on “Interface List” on the startup screen. In the Capture Interface dialog box, click on Start to start capturing data.
6. At the command prompt, type **ping** xxx.xxx.xxx.xxx and press Enter. Note that the xxx.xxx.xxx.xxx is the IP address of Default Gateway (Ref. Lab1 for details). Observe the response on command prompt, you should receive four replies
7. Stop capturing data in Wireshark by clicking on Capture 🡪 Stop. Observe the captured session as example below. What types of packets are being sent during the ping request?

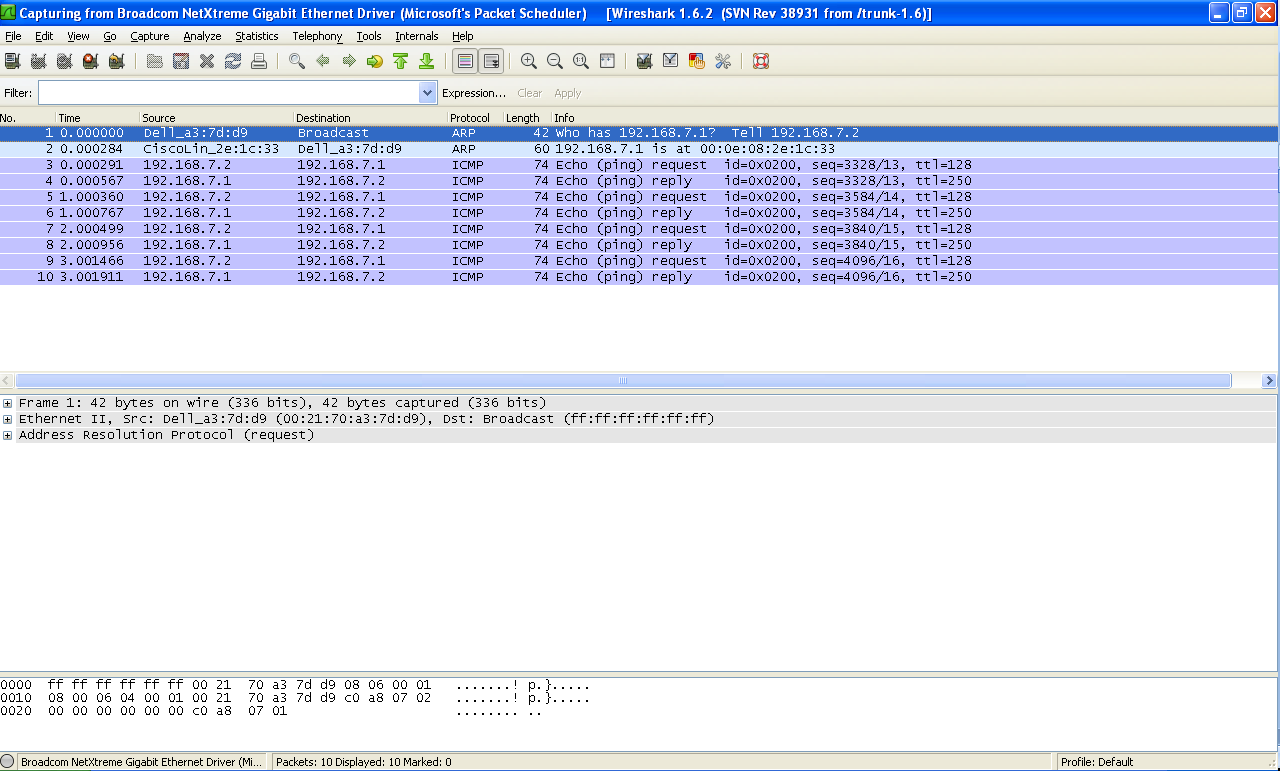


Figure 2-1

1. As shown in Figure2-1, there are 3 sections on the Wireshark’s main screen
   1. Packet list section: Located at the top, this section displays a summary of packets captured. Clicking on any of these packets displays more detailed information in the other two sections (Double clicking on any of these packets reveals the information on a new window).
   2. Tree view section: Located in the middle, this section displays a tree format detailed information on the packet selected in the top section.
   3. Data view section: Located at the bottom, this section shows the raw data of a captured packet in hexadecimal and textual formats.
2. Select the first packet that has a protocol of ARP and a destination of Broadcast. Then select in the tree view section. The part labeled Ethernet II (Click on the + sign).
3. Select the line shows Destination.
   1. What is the broadcast address in hexadecimal?
   2. Observe that the broadcast address is also highlighted in the data view section.
   3. Which is first, the source or the destination? What else is in the Ethernet part of the header?
4. In the tree view section, click on Address Resolution Protocol and expand it.
   1. What are the fields?
   2. Do they all have data?
5. In the packet list section, select the ARP reply packet, which should be the ARP packet listed right below the broadcast packet. The information in the tree view and data view sections will change accordingly. Now select the Broadcast packet. What are some differences between the two packets?
6. In the packet list section, click on the first ping request. Notice there are four of them as well as four replies. What protocol does Wireshark list as being used by ping to send and reply?
7. Click inside the Filter text box on the Filter bar and type **arp** and press Enter. Notice that only ARP packets are displayed. If you have incorrect syntax, the background is highlighted in red. It is in green if the syntax is correct. Click on Clear to see all packets.
8. Start a new capture session in Wireshark by choosing Capture 🡪 Interface 🡪 stop 🡪Start and clicking Continue without Saving, or Capture 🡪 Interfaces 🡪 Restart.
9. At the command prompt, type **nslookup kean.edu** and press Enter. Stop the capture in Wireshark (Capture🡪 Stop) once you get the response.
10. In the packet list section, select the first packet that has DNS listed in the protocol. In the tree view section, expand the User Datagram Protocol item and observe the information that is displayed. What are the source/destination ports? What is the checksum value?
11. Repeat step 15 and type **arp –a**. If you see any entries, type **arp -d**.
12. At the command prompt, type **telnet** **eve.kean.edu** and press Enter. If you can connect to eve, logon to your eve account and type **cat /etc/passwd**. You can now logout from eve.
13. Stop capturing in Wireshark. In the packet list section, select the first packet that has TCP listed in the protocol.
14. In the tree view section, expand the Transmission Control Protocol item and observe the information displayed.
    1. What are the source/destination ports?
    2. What is the checksum value?
    3. What differences do you notice between the TCP and UDP headers?

**Lab 3.2 Network Applications**

**Lab A FTP Communication**

1. Long on to a PC with the administrator account, or an account that has administrator privilege.
2. Go to [www.kean.edu/~acm](http://www.kean.edu/~acm) and select Download Software from the top menu to download Putty, FTP Client and SSH Secure Shell and install it on your computer. For Mac, ssh has been implemented on Terminal.
3. If you have already an index.html file written, use the html file and skip to step 5. Otherwise open notepad. In notepad, type the following text:

<html>

<head><title> A Simple Web Page </title>

<body><h1> This page is under construction. </h1>

<p> More computer security information will be posted here. </p>

</body>

</html>

1. Save the file on desktop with filename as index.html
2. Double click index.html or the html file you created before to make sure there are no errors on the page.
3. If this is your first time to log on to “eve,” the Computer Science department server, open the Putty click on “Run” on Security Warning. On Putty Login window, enter eve.kean.edu as the Host name and select SSH in connection type. For Mac, type **ssh user\_name@eve.kean.edu**, and enter password at the Password prompt.
4. Once Putty is on, type your User name and Password.
5. After logon, enter “passwd” to change the default password to your desire one.
6. Enter “ls –al” to see your file structure.
7. Type **cat /etc/passwd.** Explain the information returned from the command.
8. Use “cd ..” and “chmod 0755 login\_ID” to change the attribute of your root directory to be accessible by others.
9. Enter “cd” to return to your root and “mkdir public\_html” to create the sub-directory under your root. Now change its attribute with “chmod 0755 public\_html.”
10. Upload the index.html to EVE using SSH Secure File Transfer. Open SSH Secure File Transfer and click on Quick Connect, type **eve.kean.edu** and User Name then press Enter. Enter password at the Password prompt. For Mac, type **sftp user\_name@eve.kean.edu:file**. Observing the packet list section in the Wireshark.
    1. Do you see any packets listed as ftp protocol? What other protocols can you find other than ARP and TCP?
    2. Select first SSH protocol and expand the Transmission Control Protocol item. What are the source/destination ports?
11. Now you can open a web browser and enter eve.kean.edu/~your\_login\_id to see your web page. Note that the file names are case sensitive. And the index file must be .html, not .htm. Also, every referenced file must has 0755 permission.
12. Open any Internet browser, such as IE or Firefox. Enter eve.kean.edu in the URL box and press Enter. Observing the packet list section in the Wireshark, do you see any packets listed as http protocol?
13. In the tree view section, expand the Transmission Control Protocol item and observe the information displayed.
14. What are the source/destination ports?
15. What is the checksum value?

**Lab B Email Prorocols: SMTP and POP3**

1. Logon to the eve using Putty (see step 6 in Lab A)
2. At the command prompt, type **mail you@xxx.xxx** (e.g., [john@kean.edu](mailto:john@kean.edu)). Enter subject in

**Subject: Test message from (your name)**

1. Press Enter to create a blank line. The blank line is used to separate the heading of the email from the body of the message.
2. Type a message for at least three lines long. When you are done with the message, type a period on a line by itself to end the message and press Enter.

Hello,

This message is sent from eve.kean.edu

This is to practice sending email using SMTP commands.

1. Type <**Ctrl> D** to end and send the email or <Ctrl>C twice to abort sending email.
   * What message did you get from the mail server?
   * Can you think of a way that this process can be exploited?
2. Repeat Step 2-5, but type **mail –r** [**spoofing@eve.kean.edu**](mailto:spoofing@eve.kean.edu)[**you@xxx.xxx**](mailto:you@xxx.xxx)**.** 
   * What is the difference in the email header between this email and last email?
   * Is there a way to find out the true identity of the sender?

**Notes and Suggestions:**

* Different computers may have different operating systems and hardware configurations. If you use your own computer for this lab, the above procedure may not be completely applicable. For example, you cannot follow the same procedure for MAC computer.
* Make sure that the computer is back to its original condition. Do not leave a computer in a non-functioning condition.

**Lab report:**

* Your report should include all information required to be noted in the procedure, any problems/issues you encountered during the lab and how did you resolve them.