Name Chris Bero

This project introduces the student to wireshark. It will illustrate a couple of techniques for viewing the results of captured network traffic. The sample file has a telnet session, an ssh session and a web page access. **The name of the input file is Project_input.pcapng**

Information regarding the IP addresses for machines (some of these addresses may show up and others may not) used with the capture of the data are listed below. The important address is my office ip address.

Office PC: ip = 146.229.163.81 with physical address: 00-19-B9-29-57-90

Default Gateway: 146.229.175.254
DHCP Server : 146.229.250.143
DNS Servers: 146.229.163.139 and 146.229.224.33
Primary WINS Server : 146.229.128.15
Secondary WINS Server: 146.229.128.15
eagle: 146.229.162.146
blackhawk: 146.229.162.184

To run Wireshark in the labs, type Wireshark as a command in a terminal window and run it as unprivileged. Then load the provided input file into Wireshark (Wireshark opens with a graphical menu – under files, select open and open the file provided), and then proceed with the analysis outlined below.

Telnet Analysis

1) Use "telnet" as the filter in the filter box – do not use the quote marks, and after typing in telnet, click on apply. Only telnet packets should be shown

2) What is the packet number for the first telnet packet 434

3) When the first telnet packet is sent, the TCP handshake has already been performed. So, change the filter to TCP and click on apply. Find the three packets showing the TCP handshake for the telnet connection (note they should be just before the packet number of step 2 and in the info line you should see a syn, syn-ack and ack sequence). What are the packet numbers for the handshake? 425, 430, 431

4) Look at the first packet of the handshake – click on it in the list and then look at the information at the bottom. Click on the transmission control protocol section and provide values for the following questions:

   a. What is the source port number: 3704

   b. What is the Destination port number: 23

   c. Expand the options section and give the maximum segment size: 1460 bytes

   d. Under the options section are Selective ACKs (SACK) allowed? Yes

5) Change the filter back to telnet and look at the first telnet packet and expand the IP section.

   a. What is the source IP address 146.229.162.240

   b. What is the destination IP address 146.229.163.81

   c. What is the Time to Live for the packet 64

   d. What is the total length of the **IP packet** 52

6) Looking at the various telnet packets, you should be able to find the login prompt (hint look at the provided lengths for each of the telnet packets. Most are 55 or 60, but longer ones contain more data and are a good place to look for text). To view the telnet data that is in the packet, expand the telnet section and see what data is present. If you click on the telnet section, the data is highlighted in the packet at the bottom as well. See the note below. The server in this connection is 146.229.162.240

   a. What packet number contains the login prompt sent from the server to the client? 457

   b. What is the login name used tango

   c. What is the password gnathumu

   d. List all commands that were performed while the telnet section was active

   dir exit
   ls
   cd

Note: for the login name, telnet echoes the data back to the client. So each letter of the login name is repeated. Make sure that you look only at the data sent from the client. The password is not repeated back to the client. The character string \r\n indicates a return has been entered

7) What is the last telnet packet number 895

8) On the pull down menu select Statistics →Conversations, click on the TCP: 34 tab and under the port B column look for the telnet connection (#23). Select that conversation and then click on follow stream. Use this information to correct any mistakes you may have above. Note information sent by the client is in red. Information sent by the server is sent in blue.

HTTP Analysis

1) Use "http" as the filter for the data file. You will see some packets that have the protocol **ssdp – Simple service discovery protocol – ignore these packets when working with the http filter.**

2) What is the packet number for the first http packet 996

3) When the first http packet is sent, the TCP handshake has already been performed. So, change the filter to TCP and click on apply. Find the three packets showing the TCP handshake for the http connection (note they should be just before the packet number of step 2 and in the info line you should see a syn, syn-ack and ack sequence). What are the packet numbers for the handshake? 993, 994, 995

4) Look at the first packet of the handshake – click on it in the list and then look at the information at the bottom. Click on the transmission control protocol section and provide values for the following questions:

   a. What is the source port number: 3709

   b. What is the Destination port number: 80

   c. What is the window size given 65535

   d. Expand the options section and give the maximum segment size: 1460 B

   e. Under the options section are Selective ACKs (SACK) allowed? Yes

5) Change the filter back to http and look at the first http packet and expand the IP section.

   a. What is the source IP address 146.229.163.81

   b. What is the destination IP address 157.166.255.19

   c. What is the Time to Live for the packet 128

   d. What is the total length of the IP packet 322

6) Expand the Transmission Control Protocol Section of the first http packet

   a. What is the source port number 3708
   b. What is the window size given 65535

   c. What is the difference between the Next Sequence number and the sequence number 282

   d. Expand the SEQ/ACK analysis section. How many bytes of TCP data are being sent 282

7) Expand the Hypertext Transfer protocol section of the first http packet.
   a. What version of HTTP is being used 1.1

   b. What browser is being used Firefox 20.0

   c. What encoding is being accepted. gzip, deflate

ssh Analysis

1) Use "ssh" as the filter – do not use the quote marks, and after typing in ssh, click on apply. Only ssh packets should be shown

2) What is the packet number for the first ssh packet 102

3) For the first ssh packet, expand the Transmission Control Protocol section

   a. What is the source port number 3378

   b. What is the destination port number 22

   c. What is the window size given 64623

   d. How many bytes of data are contained in the TCP packet 80

4) This ssh session contains a remote login. Can you determine the login name and password? Why or Why not? Follow the conversation for the ssh transmission (port b value is 22)

I cannot. because I dont have access to the keypairs being used.