Wireshark Project

The project comprises four distinct tasks, with each task corresponding to a specific protocol. The overall project is worth 40 points, with each individual task accounting for 10 points. The project is scheduled for completion within a one-week timeframe, and it is expected that students will collaborate in pairs, forming groups of two.

It is necessary to retrieve the protocol-specific reports from Wireshark and extract the responses to each question from these reports. Subsequently, you are required to produce hard copies of these reports, which will be collected by each respective group.

Evaluation:

The assessment will be divided into two stages. The first stage is based on the report that will be submitted as a hard copy, and the second stage involves a practical discussion with each team. The majority of the grade will be determined by the discussion and your understanding of the answers.

1-HTTP Protocol

Using this link http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Answer these questions:

1-What languages (if any) does your browser indicate that it can accept to the server?

2-What is the IP address of your computer? Of the gaia.cs.umass.edu server?

3-When was the HTML file that you are retrieving last modified at the server?

4-How many bytes of content are being returned to your browser?

Using this link http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Answer these questions:

1- Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

2- Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Using this link http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

Answer these questions:

1- How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

2- Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Using this link http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

Answer these questions:

User Name: wireshark-students

Password: network

1- What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

2- When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

2-DNS Protocol

Using this link http://www.ietf.org answer these questions

1- Locate the DNS query and response messages. Are then sent over UDP or TCP?

2- What is the destination port for the DNS query message? What is the source port of DNS response message?

3- To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

4- Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

5- Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

3-TCP Protocol

Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-labs/alice.txt and retrieve an ASCII copy of Alice in Wonderland. Store this file somewhere on your computer.

Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html

1- What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
2- What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
3- What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
4- What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
5- What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.
6- What is the length of each of the first six TCP segments?
7- What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

4-UDP Protocol

Start capturing packets in Wireshark some UDP packets sent by others will appear in your trace choose any one of them and answer the questions:

1- Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header?
2- determine the length (in bytes) of each of the UDP header fields
3- The value in the Length field is the length of what?
4- What is the maximum number of bytes that can be included in a UDP payload?
5- What is the largest possible source port number?
6- What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.
7- Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. Describe the relationship between the port numbers in the two packets.

If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created

http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip