CSCD 330 – Computer Networks

Lab 5, TCP and Wireshark

Overview:

We've gone over lots of TCP specifics and learned how to associate them with what is going on in `wireshark` analyzing `pcap` files.

Today you will put together all the TCP and `wireshark` knowledge we have to analyze the file `mystery.pcap`.

Write up:

Analyze the `pcap` file and write up your report being sure to answer **all** the following questions in no more than 2 pages.

Questions:

1. What port numbers and IPs are used for the client and server.
2. Since the IP addresses are the same how can you make assumptions on who's the client and who's the server?
3. What network interface was likely used to take this `pcap`? Include your reasoning as to why you came to this conclusion?
4. What is the `MSS` for the client and server?
5. Are any packets larger than the `MSS`, if so which ones?
6. What causes retransmissions in general?
7. What do you think was the cause of retransmissions seen in the `pcap` file? Be sure to give evidence.
8. What was the retransmission rate?
9. Can I emulate this retransmission rate with a TC rule? If so, give me an example of a rule that works to cause retransmissions.
10. Can you include a `wireshark` filter so only the retransmitted packets are displayed once applied, if so what is the filter?
11. Does the packet loss appear to affect the transmission rate?
12. Can you tell what file type was sent? If so, what was it?
13. Can you reconstruct the sent data from the `pcap`? If so, what is the data?
14. Do you see a DNS call, if so what port? If not, why not?

Note: `tc` is a program on your virtual machines that you can read about using the `man` pages or any online resources.

Turn in:

You must submit a PDF file with proper grammar. As discussed in class this is a technical document, be succinct and precise. You may include **relevant** figures or screenshots if necessary, but if we find them to be irrelevant you will be deducted points. Be sure to give evidence for any statements made and explain how the conclusion was determined. Do not go over the 2 page limit, we won't read it.

The 2 page limit is only for written text, the bibliography may extend to a third page.

Citations:

If you use **any** websites as references please cite them. You may also cite the book or slides when making statements. If you, for example, find a `tc` rule online that does what I ask, be sure to cite it.

Reminder:

This is an **individual assignment**. I want to see what you know, not your neighbor.