Daniel I Montes

Tony Espinoza

CSCD 330

5/10/24

Lab 5

1. What port numbers and IPs are used for the client and server.

   The IPs are 127.2.0.1, 127.0.0.5, 127.0.0.1 and the ports are 5432 and 43060.

2. Since the IP addresses are the same how can you make assumptions on who's the client and who's the server?

   One way to tell apart who the client and server is, is by seeing which one makes requests. The client will make a request and the server will fulfill the request hopefully. It is like a search bar on a browser, it acts like a client and if you call www.snkrs.com it will fulfill the request.

3. What network interface was likely used to take this pcap? Include your reasoning as to why you came to this conclusion?

   I believe Ethernet might be the interface likely used because of the IPs.

4. What is the MSS for the client and server?

   The MSS is 65495 bytes.

5. Are any packets larger than the MSS, if so which ones?

   A TCP packet is larger than MSS because it holds a MAC header, IP header, TCP header/options/payload.

6. What causes retransmissions in general?

   In general, the main cause for retransmissions is packet loss which can be cause by different things one is network congestion. Packet loss is caused but a lot of different things like network errors, bugs in the software, etc.

7. What do you think was the cause of retransmissions seen in the pcap file? Be sure to give evidence.

   I think retransmission was caused in this pcap file because packets were missing sequence numbers.

8. What was the retransmission rate?

   I think the retransmission rate is around 23%. I got that percent by doing 9/39 * 100. 23.07 or 23.1

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.

   You can use a command to add back in the packet loss. Use “sudo tc qdisc add dev ens4 root netem delay” + the percent.

10. Can you include a wireshark filter so only the retransmitted packets are displayed once applied, if so what is the filter?

    Tcp.analysis.retransmission

11. Does the packet loss appear to affect the transmission rate?

    Yes, the packet loss can affect retransmission rate because if they do not get to their destination it is lost. There are other factors that could also affect the rate like I stated in question 6.

12. Can you tell what file type was sent? If so, what was it?

    It was sent to a PDF.

13. Can you reconstruct the sent data from the pcap? If so, what is the data?

    Yes, it is the lab 1 scavenger hunt.

14. Do you see a DNS call, if so what port? If not, why not?

    I do not see a DNS call because there is not any HTTP or HTTPS in the pcap file, so that means it did not access an outside network. The ports used are not DNS ports, DNS uses port 53.

Work Cited

https://www.jagchanna.ca/emulating-network-latency-and-packet-loss-in-linux/#google_vignette