CSCD 330 Lab 5

Cooper Bissell

1. IP addresses/Port numbers
    1. IP addresses [1]

        127.0.0.1

        127.8.0.1

        127.2.0.1

        127.0.0.5
    2. Ports [2]

        43060

        5432
2. Who is the Client, who is the Server?
    1. All IP addresses are in this capture are in the 127.0.0.0/8 range, so all packets are in the loopback range and are on one host, therefore the host is both the server and the client, but I don't believe that's the answer you're looking for.
    2. tcp://127.0.0.1:43060 appears to be the client due to it reaching out and sending the first (syn) packet to the presumed server, tcp://127.0.0.1:5432, which sends back a packet (syn ack, no 2) to start communications, and a final packet (ack, no 6). We can also see that the presumed client starts trying to upload data to the server with PSH flags, which going back to the Wireshark TCP V9 lab is quite similar to what is described there.
3. What interface were these packets taken over?
    1. These packets were taken over the loopback interface. All packets are in the loopback range therefore this is all over the loopback interface
4. What is the MSS?
    1. The MSS is 65495 [3]
5. Are there any packets larger than the MSS?
    1. No, none were observed in the packet [4]
6. What causes Retransmissions in general?
    1. the Packet becoming corrupted, loss of packet, packet timing out, out of order packets [5] [6]
7. What may have caused the retransmission in this pcap?
    1. Packets 3, 4, 5, 23, 24, 25, 32, 33 and 36 were marked as retransmissions. these were most likely due to manipulation by `tc`. [7]
8. What was the retransmission rate?
    1. 23.1% [8]

9. Can `tc` be used to cause retransmissions? what rules could have done this?
    1. Yes, `tc` can force delays or packet loss, which would trigger retransmissions.
    2. it looks like `loss 25%` was was applied to this pcap through `tc`, e.g. `tc qdisc add dev eth0 root netem loss 25%` [9]
10. What Wireshark filter shows only the retransmitted packets?
    1. The display filter `tcp.analysis.retransmission` only shows retransmitted packets.
11. Does the packet loss appear to affect the transmission rate?
    1. Yes, loss does slow down the transmission rate. After each retransmission (packets 23–25, 32–33, and 36), there's a noticeable pause in traffic before the connection resumes. These gaps line up with the sender waiting for its retransmission timeout to expire before trying again.
12. Can you tell what file type was sent? If so, what was it?
    1. The file is a PDF, and that PDF is a very corrupted looking lab 1 from this class from 2023
13. How can you reconstruct the sent data from the pcap? What was sent?
    1. You can export the file by following the TCP stream, viewing the data as raw, and then saving it as a PDF[10]. again, a corrupted 2023 lab 1 file
14. Do you see a DNS call, if so what port? If not, why not?
15. There is no traffic flagged as DNS or any traffic that has to do with upd.port == 53, therefore there is no dns traffic.
16. dns in this context would be unusual

---

[1] `tshark -r mystery.pcap -Y "ip" -T fields -e ip.src -e ip.dst | tr '\t' '\n' | sort | uniq` ↩

[2] `tshark -r mystery.pcap -Y "tcp" -T fields -e tcp.srcport -e tcp.dstport | tr '\t' '\n' | sort | uniq` ↩

[3] `printf "%d\n" $(( 16#$(tshark -r mystery.pcap -Y "tcp" -T fields -e tcp.options.mss | tr '\t' '\n' | sort -u | sed 's/^.\{4\}//' | tr -d '[:space:]')))` ↩

[4] `tshark -r mystery.pcap -Y "tcp" -T fields -e tcp.len | tr '\t' '\n' | sort | uniq` ↩

[5] https://www.chappell-university.com/post/spurious-retransmissions-a-concern ↩

[6] https://orhanergun.net/resolving-tcp-retransmission-troubleshooting ↩

[7] `tshark -r mystery.pcap -Y "tcp.analysis.retransmission" -T fields -e frame.number` ↩

[8] `echo "$(tshark -r mystery.pcap -Y 'tcp.analysis.retransmission' | wc -l) / $(tshark -r mystery.pcap -Y 'tcp' | wc -l) * 100" | bc -l` ↩

[9] `man tc | grep loss` ↩

[10] https://ask.wireshark.org/question/22490/how-to-retrieve-an-PDF-file-from-a-ftp-connection-if-its-in-binary-instead-of-ascii-format/ ↩