COMP416 – Project 2

PART 1.A

1. **How many TCP packets are transmitted in total while your KUSIS ID number is exchanged one by one with non-persistent connections?**

138 TCP packets are transmitted in total with non-persistent connections.

Graphical user interface, application

Description automatically generated

1. **How many cipher suites does your client support? Which frame is this information part of?**

My client supports 49 cipher suites. It can be seen by selecting any of the ‘Client Hello’ packets. The information is under the Transport Layer Security -> TLSv1.3 Record Layer: Handshake Protocol: Client Hello -> Handshake Protocol: Client Hello

**Graphical user interface, text, application

Description automatically generated**

1. **In which frame does the server provide its choice of cipher suite? Which cipher does your server choose? What is the complete name of Server-Hello packet and the possible reason for it?**

The cipher suite choice of the server is under the Transport Layer Security -> TLSv1.3 Record Layer: Handshake Protocol: Server Hello -> Handshake Protocol: Server Hello. My server chooses cipher suite: TLS\_AES\_256\_GCM\_SHA384 (0x1302).

**Table

Description automatically generated**

1. **What is the message type for (a) Client Hello (b) Server Hello? What are other message types supported through the employment of this field?**

The message type is Client Hello, and its code is (1). Message type is Server Hello, and its code is (2). These are two of the SSL handshake message types. There are other types such as Hello Request (0), Certificate (11), ServerKeyExchange (12), Certificate Request (13), ServerHelloDone (14), Certificate Verify (15), ClientKeyExchange (16), Finished (20).

PART 1.B

1. **Report both delays for 5 different executions and present the measurements as a single graph. Briefly describe the reasons for the results you have obtained.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Execution | TCP – Message 1 | SSL – Message 1 | TCP – Message 2 | SSL – Message 2 |
| 1 | 10757950 ns | 13066209 ns | 37919171 ns | 1275222927 ns |
| 2 | 7248948 ns | 15103905 ns | 51874764 ns | 946148923 ns |
| 3 | 3427127 ns | 20469126 ns | 46421968 ns | 1252470144 ns |
| 4 | 7098524 ns | 8163134 ns | 41583112 ns | 822007628 ns |
| 5 | 4599148 ns | 10925767 ns | 38992920 ns | 701874278 ns |

Table

Description automatically generatedTable

Description automatically generatedThe delay rates of SSL connections are a lot larger than the delay rates of TCP connections. I analyzed the exchanged packet numbers of both connections. While TCP connection sends 258 packets, SSL connection sends 686 packets which is more than twice of the TCP. The reason is that SSL encrypts and decrypts the data, and this slows down the connection.

PART 2

1. **Explain the following fields in the TCP stream and the significance of relative numbering: (a) Sequence number (b) Next Sequence Number (c) Acknowledgement Number**

The *sequence number* used is for keeping the track of the bytes that are sent out by a host. It is a counter, and it is at offset 32. For example, if a TCP packet contains 800 bytes of data, then the sequence number will increase by 800 after the packet is transmitted.

The *acknowledgement number* is used for keeping the track of the bytes that is received by a host. It is a counter, and it is at offset 64. For example, if 800 bytes of data received by a host, then the acknowledgment number will increase by 800 after the host sends out a packet in response.

The *next sequence number* is calculated by Wireshark. It Is calculated as; Sequence Number + TCP Segment Len.

1. **What is the sequence number of the TCP segment containing the HTTP POST command? Note that 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.**

Sequence number of the TCP segment is 152802.

Application

Description automatically generated with low confidence

1. **What is the TTL value for the TCP packets originating at your end? What is the TTL value for the packets received from the server? Can you confirm the number of nodes in between using another method?**

TTL value for the TCP packets originated at my end is 47.

TTL value for the TCP packets received at my end is 64.

Number of nodes can be find by using the traceroute command in the terminal.

Table

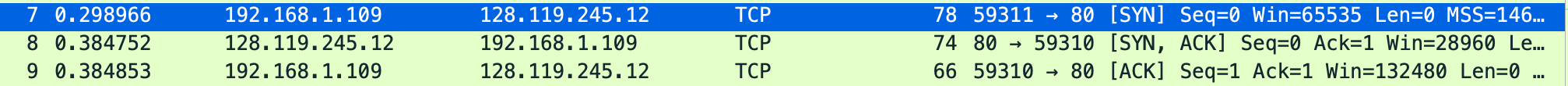
Description automatically generatedGraphical user interface, table

Description automatically generated with medium confidence

Graphical user interface, text, application, chat or text message

Description automatically generated

1. **Capture the three-way handshake between your machine and the http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html server. Provide a table with the following entries for the relevant packets involved in the three-way handshake: (a) Sequence Number (b) Flag value and significance (c) Window size (d) RTT (e) Frame for being ACK-ed (only for Ack packets)**

Three-way handshake is shown below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Packets | Seq Number | Flag Value | Window Size | RTT | Frame for being ACK-ed |
| [SYN] | 0 | Syn: Set | 65535 | 0.00000 sec | - |
| [SYN, ACK] | 0 | Acknowledgment: Set, Syn: Set | 28960 | 0.153291000 sec | 6 |
| [ACK] | 1 | Acknowledgement: Set | 132480 | 0.000101000 sec | 8 |

1. **What does the stream index in the TCP header signify? Are the packets being transmitted during the experiment all belonging to the same stream index? What does the same or different stream index mean in the context of this experiment?**

Stream index shows a unique number for each stream. All the packets in the experiment have the same stream index, and it is 1. They should be the same because they all belong to the same connection. If there would be a different stream index it would belong to some other stream. I also added a column for the stream index.

Graphical user interface, application, table, Excel

Description automatically generated

1. **Print the RTT graph for the entire communication. What is the average RTT value for the entire communication sequence?**

The RTT values are shown below.

Chart, line chart

Description automatically generated

PART 3

1. **What is the source and destination socket address for the query packet? Under which header can this information be found?**

This information can be found under the User Datagram Protocol.

Source IP: 192.168.1.109, Source Port: 53914

Destination IP: 192.168.1, Destination Port: 53

A picture containing text

Description automatically generated

1. **Examine the DNS query message? What is the ‘type’ of DNS query being sent? Is there any ‘answers’ field in the query message?**

The type of the DNS query being sent is A (Host Address), which stands for IPv4 type. There is an ‘answers’ field in the response query as shown below.

**Graphical user interface, application

Description automatically generated**

1. **Find the UDP Flags and briefly state the purpose of the first five fields?**

UDP Flags are shown below.

Table

Description automatically generated with medium confidence

1. **On applying the ‘UDP’ filter, do you find packets belonging to other protocols? If yes, which other protocols do you observe and briefly state their utilities.**

On applying ‘UDP’ filter, I found other packets belonging to other protocols. I observed SSDP and MDNS. SSDP is used for small networks, including home networks. It does not provide encryption, and the location of the sender is not checked. MDNS is a naming protocol for the computers in a local link. It maps the hostnames to IP addresses.

1. **What are the types of DNS Records (name them in the report, but you may be asked about their significance during the demo)? How can you specify the type of DNS Record when using the ‘nslookup’ command? Share the results for using the nslookup with any ‘3’ DNS Record Types.**

There are a lot of DNS record types. But the most common ones are A, CNAME, NS and MX. We can specify the type of DNS record when using the ‘nslookup’ command by:

nslookup -type=<type> tufts.edu

Graphical user interface, text

Description automatically generatedGraphical user interface, text, application

Description automatically generated

1. **What is recursive querying? How can you perform a recursive/non-recursive nslookup? What is the Flag value for a recursive and a non-recursive nslookup query?**

Recursive querying means that the query requests information from the DNS server, and if the server does not have the information, it requests other DNS servers for IP addresses. We can perform recursive and non-recursive (iterative) nslookup. Its default is recursive, and to query non-recursively -norecurse flag can be used.

Text

Description automatically generated