COMP 416 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?**

Graphical user interface, table

Description automatically generated with medium confidence138 TCP packets are transmitted in total.

1. **How many cipher suites does your client support? Where can these details be found within the traffic you just monitored?**

Graphical user interface, text

Description automatically generatedThe client support 45 cipher suites, one can see the details by clicking any client hello packets and then as in the image below

1. **Does the client support any other version of the TLS/SSL? If yes, how many? If not, what may be the reason/s for this?**

Graphical user interface, text

Description automatically generatedThe client support 4 versions of TLS: 1.0, 1.1, 1.2, 1.3 as can be seen in the image.

**4. Locate the message with the TLS Protocol ‘Server Hello’. Can you identify the Cipher which the server will be using during this connection? Find the hex dump of the key and report it in your answer.**

The cipher that server is using is:

04710c4d0ab508413bf0b20ed2ae077d4c289a24319c40815bdb17631c45c96660c71d0c…

Hex dump:

A picture containing text

Description automatically generated04 71 0c 4d 0a b5 08 41 3b 00a0 f0 b2 0e d2 ae 07 7d 4c 28 9a 24 31 9c 40 81 5b 00b0 db 17 63 1c 45 c9 66 60 c7 1d 0c 55 bb 03 b7 0b 00c0 da e1 6c 04 ae 14 24 1c a4 48 28 f8 01 2f f5 75 00d0 dc 52 75 76 f3 80 48 2d

PART 1.B

**5. 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.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EXEC NO | TCP-MSG1 | TCP-MSG2 | SSL-MSG1 | SSL-MSG2 |
| 1 | 1290132ns | 13213504ns | 2608614ns | 287362584ns |
| 2 | 1285392ns | 13107760ns | 2800751ns | 306692898ns |
| 3 | 1246840ns | 14334623ns | 2460027ns | 307926068ns |
| 4 | 1273813ns | 12936784ns | 2452739ns | 284262711ns |
| 5 | 1273213ns | 12437228ns | 2217265ns | 282188154ns |

Graphical user interface, table

Description automatically generatedGraphical user interface

Description automatically generatedSince delay time of SSL connection is lot bigger than TCP connection, I analyzed both connections.

As can be seen in the images, in order to provide a secure connection, SSL connection exchange more than double packets that are in the normal TCP connection. Thus, delay time is longer in SSL connection. Security comes with drawbacks.

PART 2

**6. What is the Acknowledgement Number and the ‘relative ack number’ in the TCP header? What does it signify?**

A picture containing graphical user interface

Description automatically generatedThe acknowledgement number is the 32-bit sequence number of the next byte the receiver expects to receive. Relative ack number is the acknowledgement number relative to the first seen segment for a particular connection since the ack number may be too big. In the image relative ack number is 1, and raw acknowledgement number is 2805783393.

**7. 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.**

Graphical user interface

Description automatically generatedThe sequence number of the TCP segment containing HTTP post is 1.

**8. 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 packets originating in my end is 64.

TTL value for the packets received from the server is 43.

In order to see TTL value and number of nodes between one can also use traceroute command in the terminalText

Description automatically generatedGraphical user interface

Description automatically generatedGraphical user interface

Description automatically generated.

1. **Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the *EstimatedRTT* value (see Section 3.5.3 in the textbook) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation (Section 3.5.3 in the textbook) for all subsequent segments.**

Alpha is taken as 0.125, values are rounded to 9 significant bits.

Seg1: Measured = 0.145547000 seconds, Estimated = 0.145547000 sec

Seg2: Measured = 0.144749000 seconds, Estimated = 0.145447250 sec

Seg3: Measured = 0.146717000 seconds, Estimated = 0.145605969 sec

Seg4: Measured = 0.148962000 seconds, Estimated = 0.146025473 sec

Seg5: Measured = 0.150205000 seconds, Estimated = 0.146547914 sec

Seg6: Measured = 0.153252000 seconds, Estimated = 0.147385924 sec

Chart, line chart

Description automatically generated

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 a same or different stream index mean in the context of this experiment?**

Stream index is a variable unique to Wireshark it and the value of it is the same for all packets which have the same ip1, ip2, port1, port2 values. Also, it does not matter whether ip1 and port1 are for source or destination. Thus, all packets in the experiment have the same stream index value and it is 0. The packets which have different stream indexes belongs to different connections.

A picture containing table

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?**

Source Ip = 192.168.1.107, Source port = 63637

Destination Ip = 192.168.1.1, Destination port = 53

Graphical user interface, text

Description automatically generatedOne can see the information inside the UDP header and Internet Protocol Version header.

1. **Locate the header under which the name of the website you have requested the IP address for is mentioned?**

Graphical user interface, text, application

Description automatically generatedDomain name System (query) -> Queries

**13. Can you derive the local DNS server you connected work in iterative or recursive manner? Please provide a detailed explanation. Besides, explain the advantages and disadvantages of an iterative and recursive approach over each other.**

**Text

Description automatically generated**When I checked Domain name System (query) ->Flags header I saw “recursion desired: Do query recursively” statement which indicates that my local DNS server works iteratively. The advantage of the recursive DNS is that thanks to caching recursive DNS tends to be fast than iterative approach, however it is vulnerable to attacks, such as amplification attacks and cache poisoning. Thus, iterative approach seems to be better in terms of security.

**14. How many replies were received in response to the DNS query? What was the type of the IP you have received and what does it mean? Identify another type and describe what that corresponds to.**

**Text

Description automatically generated**1 reply were received in response to the DNS query. There are 5 types of IP addresses: A, B, C, D, E. The type of the IP I have received was A. Types are differentiated based on their high-end bits. 52 is the high-end bit for Caltech.edu. Type A IP addresses are used in very extensive networks. Type E IP addresses are kept for future use or research and development purposes. [Source: https://superuser.com/questions/1028699/what-do-different-types-of-lan-ip-addresses-mean]

**15. What are 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.**

Althought there exists plenty of dns record the most common types and the ones we see in the class are: A, CNAME, MX and NS. In order to specify the type of DNS Record we can use:

* Text

  Description automatically generatedText

  Description automatically generatedText

  Description automatically generatedText

  Description automatically generatednslookup -type=<type> [caltech.edu](http://www.caltech.edu) in the shell.