Challenge 1

Riccardo Pezzoni 10575577

April 11, 2022

The results of each of the following questions have been verified with the addition of !_ws.malformed to make sure no malformed packages are counted. As this appears to have some inconsistencies from os to os, I would like to clarify that I have taken into consideration Version 3.6.3 of Wireshark on both Linux and macOS, a version that is supposed to have bug fixed compared to the one installed on the provided VM.

1 COAP

1.1 What are the differences between the request with MID: 53533 and the one with MID: 42804

With coap.mid == 53533 and coap.mid == 42804 we find that the former is a confirmable GET request from 10.0.2.15:50593 to 134.102.218.18:5683 while the latter is a non-confirmable DELETE packet from 10.0.2.15:58700 to 10.0.2.15:5683.

1.2 What is the response of message No. 2428, if any?

The message No. 2428 is a DELETE packet with *coap.mid == 12935*. Using that as a filter no response package is shown. This had to be expected as the request was non-confirmable.

1.3 How many replies to requests of type confirmable, having result code "Content" are received by the client "localhost"?

8 responses. ip.dst==127.0.0.1 && coap.code == 69 shows the 8 responses received by localhost having result code "Content"

coap.mid in {63229 4920 23246 13240 29961 25273 48882 21099} && coap.type== 0 shows that all 8 were responses to requests of the Confirmable.

1.4 How many GET requests, excluding OBSERVE requests, have been directed to non existing resources?

6 responses. coap.code == 1 && !coap.opt.observe == 0 shows the 16 GET requests that aren't OBSERVE.

coap.mid in {50515 40665 37038 26970 26969 21718 21444 10123 57705 54030 28357 27097 26629 2441 15597 10267} && coap.code == 132 shows 6 Not Found responses to those requests.

2 MQTT

2.1 How many messages containing the topic "factory/department*/+" are published by a client with user password: "admin"? Where * replaces only the dep. number [0-9], e.g. factory/department1/+, factory/department2/+ and so on. (* is NOT an MQTT wildcard)

0 messages. Considering + as the standard single-level wildcard, none of the messages found with mqtt.topic matches "factory/department[0-9]/" && mqtt.msgtype == 3 have a single level after department[0-9]. Thus even looking at client clients that match the condition on the password is useless.

2.2 How many clients connected to the public broker "mosquitto" have specified a will message?

9 Clients. test.mosquitto.org is resolved by the DNS in the ip 5.196.95.208. With ip.dst == 5.196.95.208 && mqtt.willmsg 9 clients are shown.

2.3 How many publishes with QoS 2 don't receive the PUBREL?

94 publishes. As mqtt.msgtype == 6 shows no PUBREL messages, each of the 94 publishes shown with mqtt.qos == 2 && mqtt.msgtype == 3 haven't received a PUBREL:

2.4 What is the average Will Topic Length specified by clients with empty Client ID?

37,05. mqtt.clientid=="" && mqtt.willtopic_len shows 37 connect commands made by users with empty clientid with existing willtopic_len. Exporting the results in json and using python to extract the date and calculate the average gives a result of 37,05.

2.5 How many ACKs received the client with ID "6M5H8y3HJD5h4EEscWkn What type(s) is(are) it(them)?

5 Acks. mqtt.clientid==6M5H8y3HJD5h4EEscWknTD shows the connect command of the client with that id, from that we can see with tcp.stream eq 281 && mqtt.msgtype in 2 4 9 we can see that in 3 messages it received 1 Connect Ack, 1 Publish Ack and 3 Subscribe Ack.

2.6 What is the average MQTT message length of the CONNECT messages using mqttv3.1 protocol? Why messages have different size?

63,59. mqtt.ver==3 && mqtt.msgtype == 1 shows the CONNECT messages using mqttv3.1. Exporting the 47 messages obtained in json and using python to compute the averages, it comes out to 63,59.