CS G513 Network Security
Lab Test 1
Set - B

Duration: 3 hours **Date : 04/03/2022**

Q1) Write a python program using Scapy and SQLITE3 Library to do the following only on Wi-Fi layers of the packets (PCAP file named "master.pcap" contains the Wi-Fi traffic, shared already over Google Classroom).

(2 + 6 + 4 + 4 + 4 = 20)

a) Write a function to create a database file named "master.db" and create three tables in the db. Name the tables as "wifiPacketFetures", "assocPacketFeatures" and "m1PacketFeatures". Select the types of the columns appropriately based on the values you see in the packet fields or as extracted by Scapy.

b) Extract WiFi packet features (or fields) for the following: packet number, **"**time stamp"**,** **"**addr1**"**, **"**addr2**",** **"**addr3**"** and **"**addr4**",** "channel", "ChannelFrequency", "dBm_AntSignal", "proto", "type", "subtype", "pkt.len", "len(pkt)". If a feature value is absent then it should be filled with a "null" or similar. This functionality be implemented in a function called "wifiPacketFeatureExtractor(..)". Extracted packet feature stored in the "wifiPacketFeatures" table.

c) Extract packet features from association request/response frame for the following: packet number, **"**timestamp"**,** **"**addr1**"**, **"**addr2**",** **"**addr3**"** and **"**addr4**"**, "channel", "ChannelFrequency", "dBm_AntSignal", "proto", "type", "subtype", "pkt.len", "len(pkt)", "SC", "fcs", "listen_interval", "[Dot11EltRSN].group_cipher_suite[RSNCipherSuite].cipher", "[Dot11EltRSN].group_cipher_suite[RSNCipherSuite].oui", "[Dot11EltRates].rates", "[Dot11EltVendorSpecific].ID" and "[Dot11EltVendorSpecific].oui". If a feature value is absent then it should be filled with a "null" or similar. Store these packet features in "assocPacketFeatures" table.

d) Extract packet features from handshake message m1 for the following: packet number, timestamp, "addr1", "addr2", "addr3", "addr4"**,** "channel", "ChannelFrequency", "dBm_AntSignal", "proto", "type", "subtype", "SC", "fcs", "A_MSDU_Present", "Ack_policy", "dsap", "ssap", "OUI", "[EAPOL].version", "[EAPOL].type". If a feature value is absent then it should be filled with a "null" or similar. Store these packet features in "m1PacketFeatures" table.

Note: Use the following function to select m1 packets in Scapy program from the pcap file:

```
def isM1Packet(pkt):
    isM1 = False
    if(pkt.haslayer(Raw)):
        if(re.search("\x02\x00\x8a", pkt.load)):
            isM1 = True
    return(isM1)
```

e) Write a function to display the following information: i) count of packets in the pcap file and count of records in the database table in parts b), c) and d), ii) a summary of

differences observed manually in the association req/res present in pcap file or in the table. In the last case, you are expected to write down your thought using print().

Submission: 1) CSG513NetSecLabTest1SetBMarch2022<Id.No.><name>.py

----------End of Question----------