Lab #9 - SY310 Traffic Analysis (Layer 5 – Application Layer)

Using the provided `layer5part1.pcap` file in Wireshark, complete the following questions.

Question 1: List the MAC address and IP address for:

- The client device: 192 . 168 . 1 . 11 — 00 : 0c : 29 : 86 : ca : 0f
- The DHCP Server: 192 . 168 . 1 . 1 — f8 : e4 : fb : 2d : 0a : 73
- Local DNS Server: 192 . 168 . 1 . 1 — f8 : e4 : fb : 2d : 0a : 73
- Gateway Router: 192 . 168 . 1 . 1 — f8 : e4 : fb : 2d : 0a : 73

Question 2: What is the network address (in CIDR notation)?

192.168.1.0/24

Question 3: What is the client's hostname?

The clients host name is EVILINSTRUCTORCOMPUTER

Question 4: List all of the URLs and associated webserver IP address that the client connected to.

www.espn.com: 68.71.212.158
www.arstechnica.com 50.31.151.33
www.torproject.org 154.35.132.70
www.bgpmon.net 142.4.204.154

Question 5: For each website list the frame numbers for the initial 3-way handshake.

www.espn.com Frame 1
www.arstechnica.com Frame 50
www.topproject.org Frame 200
www.bgpmon.net Frame 252

Question 6: What was the URL for the first DNS lookup? What was the IP address of the URL? Why is there no associated HTTP traffic in the pcap?

The first URL for the first DNS lookup is espn.com, the IP address of this URL is 158.212.71.68 which is the domain name pointer. The reason why there are not any HTTP traffic in the pcap s because we do not have the data necessary to decipher the TLS into plaintext

Question 7: Which site required HTTPS?

The sites that require HTTPS are arstechnica and topproject

Question 8: What specific article did the client read on the 3rd website?

The specific article is bgp routing incidents in 2014 malicious or not

Using the provided `layer5part2.pcap` file in Wireshark, complete the following questions.

Question 9: What is the physical medium for this capture?

Wires

Question 10: What channel was the SSID in frame 10875 transmitting on?

The SSID channel for this frame is G Note II

Question 11: List all the clients that received probe responses from SSID 'CMY'

Broadcast
RuckusWi
HTC f8:7e:c2
IntelCor_fa:f3:16

Question 12: How many probe requests, response, and beacons were in this capture?

Probe Request: 1896
Probe Response: 1940
Beacons: 947

Question 13: What Access Points has the client 'd8:d1:cb:07:d1:c0' connected to in the past? List at least 5. What are the possible security aspects of this leaked information?

EXTRA CREDIT: Can you figure out what specific type of device sent the probe request in frame 9770?