Student Name : ___Tuan Ding Ren_____

Group : ___SCEX_____

Date : ____13 March 2024_____

## LAB 3: SNIFFING AND ANALYSING NETWORK PACKETS

### EXERCISE 3A: PACKETS CAPTURING

List the sequence of all relevant network packets sent and received by your laboratory PC from the time your Rfc865UdpClient initiated a request to the DNS server to resolve the QoD server name till it received the quote of the day. Fill in the MAC and IP address of the packets where appropriate/available.

| Packet | Source MAC | Source IP | Dest. MAC | Dest. IP | Purpose of Packet |
|---|---|---|---|---|---|
| 1. | a4:bb:6d:61:d1:81 | 10.96.183.31 | 00:00:0c:9f:f0:f0 | 155.69.3.8 | DNS request |
| 2. | cc:b6:c8:85:4e:cb | 155.69.3.8 | a4:bb:6d:61:d1:81 | 10.96.183.31 | DNS response |
| 3. | a4:bb:6d:61:d1:81 | - | ff:ff:ff:ff:ff:ff | - | ARP broadcast |
| 4. | a4:bb:6d:43:43:94 | - | a4:bb:6d:61:d1:81 | - | ARP response |
| 5. | a4:bb:6d:61:d1:81 | 10.96.183.31 | 00:bb:6d:61:d1:81 | 155.69.100.96 | UDP request |
| Last. | cc:b6:c8:85:4e:cb | 155.69.100.96 | a4:bb:6d:61:d1:81 | 10.96.183.31 | Quote of the day reply |

Determine the IP address of DNS server. 155.69.3.8
Determine the IP address of the QoD server 155.69.100.96

What is the MAC address of the router? 00:00:0c:9f:f0:f0

## EXERCISE 3B: DATA ENCAPSULATION

| | |
|---|---|
| Complete Captured Data<br><br>(please fill in ONLY 8 bytes in a row, in hexadecimal) | 00 00 0c 9f f0 f0 a4 bb |
| | 6d 61 d1 81 08 00 45 00 |
| | 00 37 b8 df 00 00 80 11 |
| | 00 00 0a 60 b7 1f 9b 45 |
| | 64 60 f0 ed 00 11 00 23 |
| | cf 2f 44 69 6e 67 52 65 |
| | 6e 2c 20 53 43 45 58 2c |
| | 20 31 30 2e 39 36 2e 31 |
| | 38 33 2e 33 31 |
| | |
| | |
| | |
| | |
| | |

## EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
How do you know?
It is carrying a IPV4 data because ethernet protocol sits at the data link layer which is below the network layer that IPV4 is at.

Determine the following from the captured data in Exercise 3B:

| | |
|---|---|
| Destination Address | 00:bb:6d:61:d1:81 |
| Source Address | a4:bb:6d:61:d1:81 |
| Protocol | ARP |
| Frame Data<br><br>(8 bytes in a row, in hexadecimal) | 45 00 00 37 b8 df 00 00 |
| | 80 11 00 00 0a 60 b7 1f |
| | 9b 45 64 60 f0 ed 00 11 |
| | 00 23 cf 2f 44 69 6e 67 |
| | 52 65 6e 2c 20 53 43 45 |
| | 58 2c 20 31 30 2e 39 36 |
| | 2e 31 38 33 2e 33 31 |

## EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?

It is carrying a DNS data because IPV4 sits at the network layer which is below the transport layer that DNS is at.

Does the captured IP header have the field: Options + Padding? How do you know?

No.

The HLEN field in the IPV4 header is 0x5 which is 5 in decimal. Since this field is in multiple of 4 bytes, the header is in total 20 bytes.

Since with Version and HLEN occupying 1 byte, service field occupying 1 byte, total length of packet field occupying 2 bytes,
Identification occupying 2 bytes, flags and fragmentation offset occupying 2 bytes, Time-to-Live and Protocol occupying 2 bytes, Header Checksum occupying 2 bytes, Source IP occupying 4 bytes and finally destination IP occupying 4 bytes.

All these sum up to 20 bytes which means this header contains no option and padding.

Determine the following from the Frame Data field in Exercise 3C:

| | |
|---|---|
| Version | 4 |
| Total Length | 0x0037 which is 55 |
| Identification | 0xb8df which is 47327 |
| Flags<br>(interpret the meanings) | 000 in binary.<br>Bit 0, the first bit is reserved as 0.<br>Bit 1, the second bit, is the Don't Fragment(DF) flag set to 0 means this packet may be fragmented.<br>Bit 2, the thirs bit, is the More Fragments (MF) flag set to 0 means this packet is the last packet and there are no more other fragments. |
| Fragment Offset | 0, since this is the only fragment |
| Protocol | 0x11 which is 17 |
| Source Address | 0x 0a 60 b7 1f which is 10100110000010110111000111111 which is 10.96.183.31 |
| Destination Address | 0x 9b 45 64 60 which is 10011011010001010110010001100000 which is 155.69.100.96 |
| Packet Data<br><br>(8 bytes in a row, in hexadecimal) | f0 ed 00 11 00 23 cf 2f |
| | 44 69 6e 67 52 65 6e 2c |
| | 20 53 43 45 58 2c 20 31 |
| | 30 2e 39 36 2e 31 38 33 |
| | 2e 33 31 |

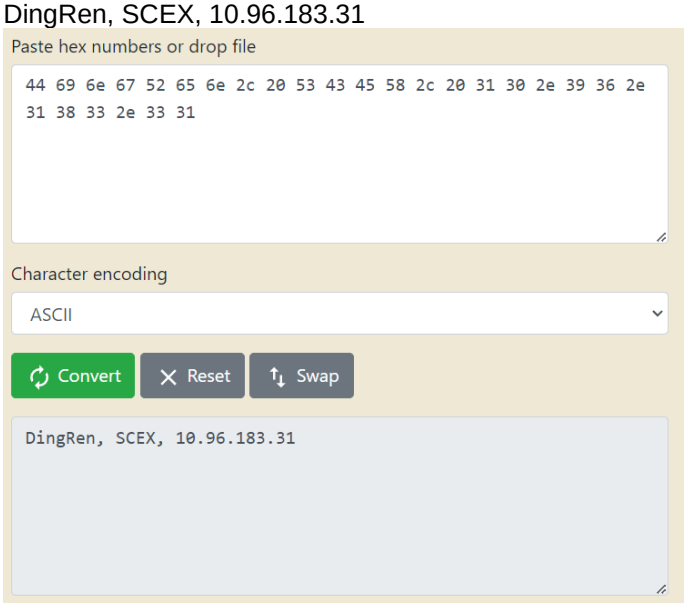
## EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

Determine the following from the Packet Data field in Exercise 3D:

| | |
|---|---|
| Source Port | 0x f0 ed which is 61677 |
| Destination Port | 0x 00 11 which is 17 |
| Length | 0x 00 23 which is 35 |
| Data<br><br>(8 bytes in a row, in hexadecimal) | 44 69 6e 67 52 65 6e 2c |
| | 20 53 43 45 58 2c 20 31 |
| | 30 2e 39 36 2e 31 38 33 |
| | 2e 33 31 |

## EXERCISE 3F: APPLICATION PDU

Interpret the application layer data from the Data field in Exercise 3E:

| | |
|---|---|
| Message | DingRen, SCEX, 10.96.183.31<br>  |

Is this the message that you have sent?

Yes.