Student Name : Hendy\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Group : A33\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date : 7 March 2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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:5F:C8:F2 | 172.21.148.5 | 00:08:E3:FF:FC:A0 | 155.69.3.8 | DNS request |
| 2. | 00:08:E3:FF:FC:A0 | 155.69.3.8 | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | Reply with IP of domain  (Failed) |
| ... | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | 00:08:E3:FF:FC:A0 | 155.69.3.8 | DNS request  (repeat) |
|  | 00:08:E3:FF:FC:A0 | 155.69.3.8 | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | Reply with IP of domain  (Failed) |
|  | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | 00:08:E3:FF:FC:A0 | 155.69.3.8 | DNS request  (repeat) |
|  | 00:08:E3:FF:FC:A0 | 155.69.3.8 | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | Reply with IP of domain  (Success) |
|  | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | 01:00:5E:00:00:FB | 244.0.0.251 | MDNS  Query  Transmission  Request |
|  | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | 01:00:5E:00:00:FB | 244.0.0.251 | MDNS  Query  Retransmission  Request |
|  | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | 01:00:5E:00:00:FC | 244.0.0.252 | LLMNR  Query request |
|  | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | 01:00:5e:00:00:fc | 244.0.0.252 | LLMNR  Query request  (repeat) |
|  | FE:96:8F:0F:DC:64 | 172.21.148.201 | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | LLMNR Response |
|  | FE:96:8F:0F:DC:64 | 172.21.148.201 | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | LLMNR  Response  (repeat) |
|  | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | FE:96:8F:0F:DC:64 | 172.21.148.201 | UDP request |
| Last. | FE:96:8F:0F:DC:64 | 172.21.148.201 | A4:BB:6D:5F:C8:F2 | 172.21.148.5 | Quote of the day reply  (No human thing is of serious importance - Plato.) |

Determine the IP address of DNS server. 155.69.3.8

Determine the IP address of the QoD server 172.21.148.201

What is the MAC address of the router? 00:08:E3:FF:FC:A0

**Exercise 3B: Data Encapsulation**

|  |  |
| --- | --- |
| Complete Captured Data    (please fill in ONLY 8 bytes in a row, in hexadecimal) | fe 96 8f 0f dc 64 a4 bb |
| 6d 5f c8 f2 08 00 45 00 |
| 00 34 66 72 00 00 80 11 |
| 00 00 ac 15 94 05 ac 15 |
| 94 c9 d9 bf 00 11 00 20 |
| cf 23 48 65 6e 64 79 2c |
| 20 41 33 33 2c 20 31 37 |
| 32 2e 32 31 2e 31 34 38 |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Exercise 3C: DATA LINK PDU - Ethernet Frame**

What type of upper layer data is the captured ethernet frame carrying?

It is using UDP

How do you know?

The client has been programmed to sent it via UDP (through port 17).

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

|  |  |
| --- | --- |
| Destination Address | fe:96:8f:0f:dc:64 |
| Source Address | a4:bb:6d:5f:c8:f2 |
| Protocol | UDP |
| Frame Data  (8 bytes in a row, in hexadecimal) | 45 00 00 34 66 72 00 00 |
| 80 11 00 00 ac 15 94 05 |
| ac 15 94 c9 d9 bf 00 11 |
| 00 20 cf 23 48 65 6e 64 |
| 79 2c 20 41 33 33 2c 20 |
| 31 37 32 2e 32 31 2e 31 |
| 34 38 |
|  |
|  |
|  |
|  |

**Exercise 3D: NETWORK PDU - IP Datagram**

What type of upper layer data is the captured IP packet carrying?

17

How do you know?

It is carrying transport layer data because it contains the destination port.

Does the captured IP header have the field: Options + Padding?

No

How do you know?

Header length is 5, It doesn’t any option of padding field and

There are no options immediately after the destination address, just the data.

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

|  |  |
| --- | --- |
| Version | 4 |
| Total Length | 20 bytes (5) |
| Identification | 0x6672 (26226) |
| Flags  (interpret the meanings) | All bits not set |
| Fragment Offset | 0 |
| Protocol | UDP |
| Source Address | 172.21.148.5 |
| Destination Address | 172.21.148.201 |
| Packet Data  (8 bytes in a row, in hexadecimal) | d9 bf 00 11 00 20 cf 23 |
| 48 65 6e 64 79 2c 20 41 |
| 33 33 2c 20 31 37 32 2e |
| 32 31 2e 31 34 38 |
|  |
|  |
|  |
|  |
|  |

**Exercise 3E: TRANSPORT PDU - UDP DATAGRAM**

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

|  |  |
| --- | --- |
| Source Port | 55743 |
| Destination Port | 17 |
| Length | 32 |
| Data  (8 bytes in a row, in hexadecimal) | 48 65 6e 64 79 2c 20 41 |
| 33 33 2c 20 31 37 32 2e |
| 32 31 2e 31 34 38 |
|  |

**Exercise 3F: Application PDU**

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

|  |  |
| --- | --- |
| Message | Hendy, A33, 172.21.148.5 |

Is this the message that you have sent?

Yes