Lab Ass -02

Name: Nagendra Chaudhary Roll N: 220cs2259

1. Select the Ethernet header of the 4th TCP packet and fill the table below.

|  |  |
| --- | --- |
| Fields | Values Hex |
| Destination MAC address | d8:9c:67:58:5f:41 |
| Source MAC Address | fe:aa:b6:c6:81:c1 |
| Ethernet Type | IPv4 |

1. Select them IP datagram of the 7th TCP packet and fill the table below and answer the questions.

|  |  |
| --- | --- |
| Fields | Values Hex/Decimal Code |
| Version | 0100 , Version: 4 |
| Internet Header Length | Header Length : 20 bytes (5) |
| Total Length | 1480 |
| Identification | 0xecb0 (60592) |
| Flags | 0 . 1 . 0 [ Reserved Bit , Dont Fragment , More Fragment ] |
| Fragment Offset | 0 |
| Time to Live | 128 |
| Protocol | TCP |
| Header Checksum | 0x2a3c |
| Source Address | 192.168.0.104 |
| Destination Address | 6.89.20.103 |

Exercise:

* 1. Check the flags in the IP header.

**Ans** : 0 . 1 . 0

* 1. Check the fragmentation offset value and what does it mean?

**Ans** : Fragmentation Offset Value = 0

* 1. Check the protocol numbers of ICMP:1 TCP: 6 UDP:17
  2. Calculate the header sizes.

**Ans** : Header Size = 20 Bytes

* 1. Calculate the data size.

**Ans** : The Frame size is the total size of the Data , **1494 Bytes** in total

1. Select TCP segment of the 10th TCP packet and fill the table below:

|  |  |
| --- | --- |
| Fields | Values Hex/Decimal Code |
| Source port | 443 |
| Destination Port | 52717 |
| Sequence Number | 1 |
| Acknowledgement Number | 1441 |
| Header Length | 20 Bytes |
| Flags(indicate which is set) | [ 0,0,0,0,0,1,0,0,0,0] |
| Window size | 2053 |
| Checksum | =0x1068 |

Exercise:

1. Check the TCP 3 way handshake.

**Ans**:

1st Handshake { Client - [ SYN ] - Server ] Synchronous TCP Packet

2nd Handshake [ Server -[ SYN , ACK ] - Client] Acknowledge from Server

3rd Handshake [ Client - [ ACK ]-Server ] ACK from Client

1. Also check the Fin AKK when the connection is closed.

**Ans**:

1st Handshake----Finish Request Packet

2nd Handshake [ Server -[ SYN , ACK ] - Client] Acknowledge from Server

3rd Handshake [ Client - [ ACK ]-Server ] ACK from Client

1. Check the value of Ack when the initial Syn flag is sent.

While connection is being established all except the SYN and ACK flags are set to 0

1st handshake SYN Flag= 1 ACK Flag= 0

2nd Handshake SYN Flag=1 ACK Flag=1

3rd Handshake SYN Flag=0 ACK Flag=1

1. Select the ARP packets and fill the table below.

|  |  |
| --- | --- |
| Fields | Value Hex/Decimal Code |
| Hardware Type | Ethernet (1) |
| Protocol Type | IPv4 |
| Hardware Size | 6 |
| Protocol Size | 4 |
| Opcode | request (1) |
| Sender MAC Address | d8:9c:67:58:5f:41 |
| Sender IP Address | 192.168.0.102 |
| Destination MAC Address | 00:00:00:00:00:00 |
| Destination IP Address | 192.168.0.1 |

Exercise:

1. Check the columns of the summary window.

Frame ( Frame Number ) = 42Bytes

Ethernet II : Src MAC Address , Destination MAC Address

1. Check the destination address when the ARP request is sent.

Destination is the Broadcast MAC address ff:ff:ff:ff:ff:ff

1. Compare the 4th request reply ICMP packet and fill the table below.

|  |  |  |
| --- | --- | --- |
| Fields | Values Hex/Decimal Code | |
| Request | Reply |
| Type | 8 | 0 |
| Code | 0 | 0 |
| Identifier | 254 | 254 |
| Sequence | 4059 | 3024 |
| Data | 2782981e36177231e3272339212e3219379123a56f8987b78b68768d897 | 2782981e36177231e3272339212e3219379123a56f8987b78b68768d897 |

Exercise:

1. Identify the sequence number and the identifier in all the request and response packets.

Request Sequence Number = 4059

Response Sequence Number = 3024

1. Write the type and code for the ICMP packets. (Refer next page for type and code).

Type 0 =Reply ICMP Packet

Type 8 =Request ICMP Packet

Code number signifies the type of message you re sending

1. Select the UDP datagram and fill the table below:

|  |  |
| --- | --- |
| Fields | Values Hex/Decimal Code |
| Source Port | 62835 |
| Destination Port | 443 |
| UDP Length | 1358 |
| Checksum | 0x8300 |

Exercise: Which application layer protocol is using the UDP?

Ans : DNS