MSDS 7349

Data and Network Security

Homework 1 - Wireshark

*Submitted by: Apurv Mittal*

**Collaborated with Ravi Sivaraman on this exercise**

1. Exercise 1
   1. Step1: Wireshark Protocol Layers

Text

Description automatically generated

* 1. Step 2

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

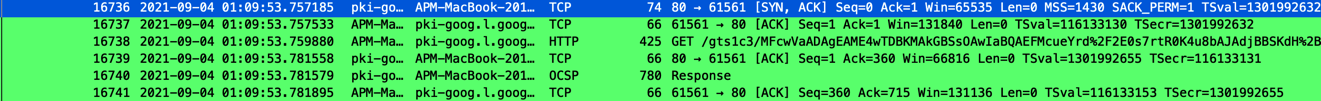
* 1. Step 3:

Graphical user interface

Description automatically generated

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TCP Segment Header Format** | | | | |
| **0 7** | | **8 15** | **16 23** | **24 31** |
| Source Port 80 | | | Destination Port 59256 | |
| Sequence Number 14181 | | | | |
| Acknowledgement Number 79 | | | | |
| Data Offset | Res | Flags 0x018 | Window Size 65536 | |
| Header and Data Checksum 0x6f30 | | | Urgent Pointer 0 | |
| Options 12 bytes | | | | |
| Data | | | | |
|  |
|  |
|  |
|  |

* 1. Step 4:



Above screenshot shows the sequence of packets. We can notice the Get request is bigger size at 425 bytes. The response is of 780 bytes. Though its not a big payload but when compared to other packets it does feel to be big overhead, because the get request is just for us to pass the IP address and information we need to fetch.

* 1. Step 5:

1.Text

Description automatically generated

The demultiplexing key for Ethernet is the Type field. It holds 0x800 when the higher layer is IP.

2.

Graphical user interface, text

Description automatically generated

The demultiplexing key for IP is the Protocol field. It has value 6 when the higher layer is TCP.

Reference: <https://kevincurran.org/com320/labs/wireshark/lab-protocol-layers.pdf>

1. Exercise 2
   1. Step 1:

Text

Description automatically generated

Step 2:

Graphical user interface, text

Description automatically generated

Step 3:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP Header Format** | | | | | | |
| Version  4 | Header Length 20 | Service Type 0x00 | Packet Length 543 | | | |
| Identification 0xa84d | | | Reserved 0 | DF 0 | MF 0 | Fragment Offset 0 |
| Time to Live 56 | | Transport 6 | Header Checksum 0x12d6 | | | |
| Source IP Address 172.217.1.228 | | | | | | |
| Destination IP Address 192.168.86.80 | | | | | | |
| Options | | | | | Padding | |
| Data | | | | | | |
|  |
|  |
|  |
|  |

Text

Description automatically generated

1. IP Address of Computer: 192.168.86.80 and Remote Server: 172.217.1.228
2. Yes, it includes the length of the IP header
3. In the instances of incoming traffic, the identification field has values while its 0 for the outgoing. There is a pattern in the incoming traffic, the values are in sequence and increment by 1.
4. Always 64 from my machine to the destination and always 53 in return
5. Fragment offset is 0. So, it’s not fragmented
6. 20 bytes

Step 4:

Text

Description automatically generated



Exercise 3 : Wireshark DNS

Step 1:

Text

Description automatically generated

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Query** | **IP Address** | **Interim IP Address received** | **Destination IP** |
| **1** | dig @@202.12.27.33 www.smu.edu | 202.12.27.33 | 192.5.6.30 |  |
| 2 | dig @@192.5.6.30 www.smu.edu | 192.5.6.30 | 129.119.64.8 |  |
| 3 | dig @@129.119.64.8 www.smu.edu | 129.119.64.8 |  | 129.119.70.166 |

smu.edu. IP address is 129.119.70.166

Step 2:

A picture containing text

Description automatically generated

Step 3:

1. Transaction ID: 0x5fc2. 16 bits long. Likely to be used for concurrent transactions

Text

Description automatically generated

1. In flag “0” indicates query and “1” as response. Below is a Query

Text

Description automatically generated

1. The DNS header is 12 bytes long.
2. Additional section carries the Nameserver

A picture containing text

Description automatically generated

1. IP address is in the Additional Section
2. Domain name is in the Answer section

Graphical user interface, text

Description automatically generated