**LAB REPORT**

Course Code - Course Name: - COMP4039 – Network Foundations

Program: T433 - Cybersecurity

Section: A

Term: - Winter 2024

Lab Number - Topic: Lab 3 – **Investigating the TCP/IP and OSI Models in Action**

Group Number: 06

Student Names - ID:

* Prabhjot Singh Sains – 101495218
* Rahul Patel - 101378458
* Jai Deep Rawat - 101503760
* M. Salmaan Mustafa Shah – 10151007

**Objective:**

In this lab, we will use Packet tracer, to explore the TCP/IP protocol. We will examine various UDP and TCP transmissions. Write a report, to show how to execute the lab procedures. We will use Packet Tracer (PT) Simulation mode to generate web traffic and examine HTTP and examine various protocols.

**Procedure:**

1. Start Packet Tracer and switch from Realtime to Simulation mode. In Simulation mode, packets are displayed as animated envelopes, time is event-driven, and the user can step through networking events.

A diagram of a computer network

Description automatically generated

1. Create the topology shown above and assign both devices the following IP information:
   1. Web Server:
      1. IP: 192.168.1.10
      2. Subnet mask: 255.255.255.0

A screenshot of a computer

Description automatically generated

* 1. Web Client:
     1. IP: 192.168.1.20
     2. Subnet mask: 255.255.255.0
     3. DNS: 192.168.1.10

A screenshot of a computer

Description automatically generated

1. On the Web Server enable HTTP and DNS service (Note that this server provides two services http & DNS)
   1. Select the services tab, then choose HTTP service. Make sure both http and https are enabled ON.

A screenshot of a computer

Description automatically generated

* 1. From services, select DNS service and add the following record.
     1. Domain name: [www.comp4039.local](http://www.comp4039.local)
     2. IP address 192.168.1.10

A screenshot of a computer

Description automatically generated

1. **Generate web traffic.**
2. Click Web Client in the far-left pane.
3. On the web client, click the Desktop tab and click the Web Browser icon to open it.
4. In the URL field, enter www.comp4039.local and click Go.
5. Because time in Simulation mode is event-driven, you must use the Capture/Forward button to display network events (stop when the web page is displayed in the browser).

**A screenshot of a computer

Description automatically generated**

**Question:** What Event Types are displayed? Record all the PDUs listed on the Event list pane.

**Answer:** All the events are listed below:

A screenshot of a computer

Description automatically generated

1. **Explore the content of the DNS packet.**
   1. Click the first colored DNS square box under the **Event List** > **Info** column.

A screenshot of a computer

Description automatically generated

* 1. Ensure that the **OSI Model** tab is selected. Under the **Out Layers** column, ensure that the **Layer 7** box is highlighted

A screenshot of a computer

Description automatically generated

**Question**: What is the text displayed next to the **Layer 7** label? What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes?

**Answer:** The DNS client sends a DNS query to the DNS server

* 1. Click Next Layer. Layer 4 should be highlighted.

A screenshot of a computer

Description automatically generated

**Question:** What is the Dst Port value?

**Answer**: 53 is the Dst Port Value.

* 1. Click Next Layer. Layer 3 should be highlighted.

A screenshot of a computer

Description automatically generated

**Question:** What is the Dst. IP value?

**Answer:** 192.168.1.10 is the Dst IP Value.

* 1. Click Next Layer

A screenshot of a computer

Description automatically generated

**Question:** What information is displayed at this layer?

**Answer:** 3 points were displayed:

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.
2. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table.
3. ﻿﻿﻿The device encapsulates the PDU into an Ethernet frame.
   1. Click the Outbound PDU Details tab.

A screenshot of a computer

Description automatically generated

**Question:** What information is listed in the NAME: in the DNS QUERY section?

**Answer**: [www.comp4039.local](http://www.comp4039.local)

* 1. Click the last DNS Info colored square box in the event list.

A screenshot of a computer

Description automatically generated

**Question:** What is the value listed next to **ADDRESS**: in the DNS ANSWER section of the **Inbound PDU Details**? Which transport layer protocol that DNS use?

**Answer**: DNS uses the UDP transport layer.

1. **Explore the content of the TCP packet.**
   1. Click the first colored square box of the TCP event. Highlight Layer 4 in the OSI Model tab. In the numbered list directly below the In Layers and Out Layers.

A screenshot of a computer

Description automatically generated

**Question:** what is the information displayed under items 4 and 5?

**Answer:** The information displayed is:

1. The device tries to make a TCP connection to 192.168.1.10 on port 80.
2. The device sets the connection state to SYN\_SENT.
3. TCP accepts a window size up to 65535 bytes.
4. Add Maximum Segment Size Option to the TCP SYN header with a Maximum Segment Size equal to 1460 bytes.
5. The device sends a TCP SYN segment.
6. Sent segment information: the sequence number 0, the ACK number 0, and the data length 24.
   1. Click the second colored square box of the TCP event. Highlight Layer 4 in the OSI Model tab. In the numbered list directly below the In Layers and Out Layers.

A screenshot of a computer

Description automatically generated

**Question:** what is the information displayed under item 3?

**Answer:** The information displayed is:

1. The device receives a TCP SYN segment on server port 80.
2. Received segment information: the sequence number 0, the ACK number 0, and the data length 24.
3. TCP retrieves the MSS value of 1460 bytes from the Maximum Segment Size Option in the TCP header.
4. The connection request is accepted.
5. The device sets the connection state to SYN\_RECEIVED.

* 1. Click the last TCP event. Highlight Layer 4 in the OSI Model tab. Examine the steps listed directly below In Layers and Out Layers.

**A screenshot of a computer

Description automatically generated**

**Question:** What is the purpose of this event?

**Answer:** Events in like notifications that quickly tell us what's going on in a system, helping us find and address security issues or possible threats.

1. **Explore the content of the HTTP packet.**
2. Click the first colored square http box under the **Event List** > **Info** column.

A screenshot of a computer

Description automatically generated

1. Ensure that the OSI Model tab is selected. Under the Out Layers column, ensure that the Layer 7 box is highlighted.

A screenshot of a computer

Description automatically generated

1. Click Next Layer. Layer 4 should be highlighted.

A screenshot of a computer

Description automatically generated

1. Click Next Layer. Layer 3 should be highlighted.

A screenshot of a computer

Description automatically generated

1. Click Next Layer.

A screenshot of a computer

Description automatically generated

**Question**: What is the text displayed next to the **Layer 7** label? What information is listed in the numbered steps directly below the **In Layers** and **Out Layers** boxes?

**Answer**: The HTTP client sends a HTTP request to the server

**Question**: What is the Dst Port value?

**Answer**: 80 is the Dst Port Value

**Question**: What is the Dst. IP value?

**Answer**: 192.168.1.10 is the Dst IP Value

**Question**: What information is displayed at this layer?

**Answer**: Layer 2 Ethernet II Header and inbound and outbound MAC addresses.