Assignment - 1

Summer 232 CSE 323/CSE 3711 (A) : Computer Networks

Question: 1.

Step 1: Capture and Analyze Network Traffic

Using Wireshark, capture network traffic on your local network or a specific network interface. Analyze the captured traffic to identify the following:

a) The number of packets captured during the capture session.

b) The most commonly used protocols in the captured traffic.

c) The source and destination IP addresses and ports for the top five network connections.

Step 2: Identify and Analyze a Specific Protocol

Choose a specific protocol from the captured traffic and analyze it in detail. Answer the following questions:

a) What is the purpose of the chosen protocol?

b) What are the common port numbers used by this protocol?

c) Identify and analyze at least three packets that belong to this protocol. Describe the content of each packet and explain their significance in the context of the protocol.

Step 3: Detect and Analyze Network Anomalies

Using the captured traffic, identify any network anomalies or suspicious activities. Answer the following questions:

a) Did you observe any unusual network behavior or suspicious traffic patterns?

b) If yes, describe the anomalies or suspicious activities you identified.

c) Provide recommendations on how to mitigate or investigate these anomalies further.

Note: Please provide screenshots or excerpts from the Wireshark capture to support your answers in each step & make a pdf with proper explanation.

Question: 2. You're tasked with setting up a small network using Packet Tracer. The network consists of three computers (PC1, PC2, and PC3) and a switch. PC1 and PC2 should be in the same subnet network, while PC3 should be in a different network subnet. Using a router makes different network connections.

1. Configure PC1 with the IP address 192.168.1.21 and a subnet mask of 255.255.255.0.
2. Configure PC2 with the IP address 192.168.1.20 and a subnet mask of 255.255.255.0.
3. Configure PC3 with the IP address 192.168.2.10 and a subnet mask of 255.255.255.0.
4. Connect PC1, PC2, and PC3 to the switch using Ethernet cables.
5. Verify connectivity between the computers by pinging PC2 from PC1 and PC3 from PC2.

Note : Submit a screenshot of your Packet Tracer network topology showing the configured IP addresses, subnet masks, and successful pings.

To download and install Wireshark, follow these steps:

1. Visit the official Wireshark website at www.wireshark.org.
2. Go to the "Download" section and select the appropriate version for your operating system (Windows, macOS, or Linux).
3. Once the download is complete, run the installer and follow the on-screen instructions to install Wireshark.
4. After the installation is finished, launch Wireshark.
5. Select the network interface you want to capture packets from (e.g., Ethernet, Wi-Fi) and click on the "Start" button to begin capturing.
6. Wireshark will start capturing network traffic on the selected interface. You can analyze the captured packets by applying various filters, inspecting packet details, and using the built-in tools and features of Wireshark.

Remember to use Wireshark responsibly and in compliance with the law, as it can capture sensitive information.

To download and install Cisco Packet Tracer :
For windows https://drive.google.com/file/d/1rDPWz-CYj9XUG0dn4jSwcMfd3yOwC4y9/view