Data Communication and Computer Network Laboratory

Master of Computer Application
Second Year, First Semester
Session: 2023-24

Assignment - IV

Date: 24/08/2023

Basic Packet Capturing and Analysis

In this exercise you will be using python `scapy` library for packet capturing and network analysis.

- **Sniff Packets**: Use `scapy`'s `sniff()` function to capture packets from the network. The `sniff()` function allows you to specify the number of packets to capture or the duration for which to capture packets. You can also filter the packets based on specific criteria like source/destination IP addresses or protocols. You can also use `scapy` to sniff packets offline from pcap files.
- **Analyze Packets**: Once the packets are captured, you can access various attributes of each packet to perform your analysis. Some commonly used attributes include:
  - `packet.summary()`: Provides a summary of the packet, including source and destination IP addresses, protocol, and packet size.
  - `packet.show()`: Displays the detailed information of the packet, including the layers and their corresponding values.
  - `packet[TCP].payload`: Accesses the payload data of a TCP packet.
  - `packet[UDP].payload`: Accesses the payload data of a UDP packet.

Further details on scapy usage can be found at https://scapy.readthedocs.io/en/latest/index.html

Using `scapy` do the following:

1. Capture 10000 packets (either online/offline)
2. Count the number of distinct host IP addresses and display them.
3. For each distinct pair of source/destination host IP addresses determine the number of TCP/UDP segments exchanged and also the average payload length.

   Desired output:

Source IP	Destination IP	Protocol	Number of Segments	Average Payload Length
...	...	TCP	...	...
...	...	UDP	...	...

4. For each distinct quadruple of source/destination host IP addresses and source/destination port numbers determine the number of TCP/UDP segments exchanged and also the average payload length.

   Desired output:

Source IP	Destination IP	Protocol	Source Port	Destination Port	Number of Segments	Average Payload Length
...	...	TCP	...	...	...	...
...	...	UDP	...	...	...	...

Your report should contain at least the following sections:

1. Problem Statement
2. Your solution approach, data structures used.
3. Source code (with appropriate comments)
4. Sample run