National Institute of Technology Calicut
Department of Computer Science and Engineering
Winter Semester: 2021-22

CS3093D: Networks Lab
Assignment – II

Date: 17, Jan.’22

Introduction

The assignment introduces packet sniffer, Wireshark. Wireshark is a free open source network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis.

Wireshark can be downloaded from the location https://www.wireshark.org/download.html

Questions

1) Execute the following command in the terminal, wget https://minerva.nitc.ac.in/sites/default/files/attachments/news/TT_Winter2021-2022%20%281%29.pdf
Parallely run the wireshark tool. Note down your network analysis of the command.

2) Consider the pcap file, File001.pcap. The file contains captured packets sent over the network. It is noticed the system has made a connection to an unsecured host system and the user has sent his credentials over plaintext. Investigate File001.pcap to unearth the login credentials.
    a. Indicate the IP addresses, Source and Destination, of the communicating end systems in which the login credentials are found.
    b. Determine the protocol over which the user credentials are sent.
    c. What are the login credentials?

3) Consider the pcap file, File002.pcap. The file contains captured packets. Consider the packets numbered 27 and 32. Fill up the header details for the packets 27 and 32. The header details are provided in Figure 1.

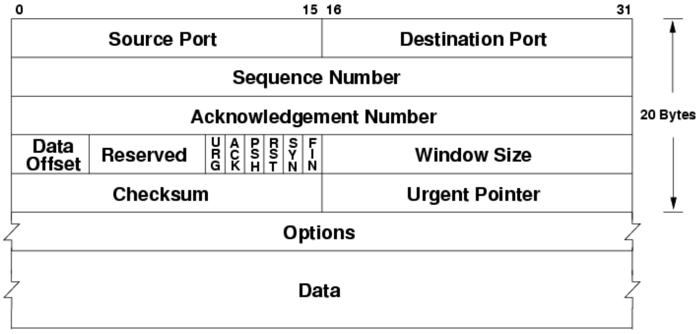

Figure 1: TCP Header