CSD – 415 – INFORMATION SECURITY LABORATORY

Lab 2 – Batch I

Date: 07-09-2020

Perform the following tasks in Wireshark:

1) Capture live traffic and generate pcap file.
2) Analyze the traffic using I/O graphs.
3) Plot the errors occurred in the traffic.
4) List the transport layer protocols in the traffic and which protocol dominates the captured traffic?
5) What is the highest number of TCP packets/sec observed? What is the peak time (in seconds)?
6) Which protocol is in packet #100? What is the elapsed time from packet #100 to packet #200? How much bytes have been used during this period?
7) List the meaning of the following:
   a) Packet is highlighted in green
   b) Packet is highlighted in dark blue
   c) Packet is highlighted in light blue
   d) Packet is highlighted in black
8) Count the number of packets in HTTP.
9) Sort the packets by Instance ID, IP, object type, and service.

Optional:

10) Capture password of any server/machine/file.

*****