CSC 435 Distributed Systems - Networks Labs

**Wireshark Lab: Getting Started.**

In the Introduction it's about Installation and understanding the interface of the Wireshark tool. There are various tools which can be used for packet sniffing and these are placed above the transport layer to capture all the packets which leaves a system. The installation is fairly simple and easy just click and install a packet capture or pcap which is a services which keeps listening to all the outbound/inbound traffic. The interface of Wireshark consist of a filter to filter the protocols and IP’s, windows which displays captured packets, another window with details of the packet header and packet contents. The tool helps us to analyse a various protocols by checking what data is sent and received. For Example we do a packet capture of HTTP protocol and analyse/view the headers and the message inside the captured packet.

**Wireshark Lab: IP**

In this lab we talk about tracert which is known as traceroute, like we use google maps or some map application to find an address to a destination. Tracert is similar to this, where tracert is the google map which provides the route to the destination IP. So in the lab we run tracert to a destination with different packet sizes of (56, 2000, 3500) bytes also we analyse the sent packets, where we look how the ICMP protocol works and also see how the TTL-exceeded reply is sent to source from the router which removes the 1 and drops the packet as TTL is 0. This shows us how a fragmentation of the data being sent across the network happens and how we can say that this data/message transmission has X number of fragments and the total length of the data.

**Wireshark Lab: DNS**

In this lab we talk about nslookup and ipconfig, both initiate DNS which is used to translate a website address or URL to IP address. nslookup you can get the IP address of the website address and also the NameServers name which is giving the request back for the DNS request for that website URL. It will query back all the NameServers related to the URL. Ipconfig is to see the network details of the Ethernet cards on the system like internal IP address, adapter name and the physical address(MAC address) also it can be used to flush the DNS release the internet connection in the systems and renew it .

**Wireshark Lab: HTTP**

This is something very familiar to me, as it was a part of my previous job role where I used burpsuite security assessment tool which captures the requests and responses and then analyse it. We could see it real time for http and the base64 decoding which in lab we see to view the password, can be done with ease as burpsuite provides an inbuilt decoder.

**Wireshark Lab: UDP**

I felt this lab similar to the DNS lab, as in DNS lab it was already mentioned that UDP packets are sent during nslookup, even though I knew why checksum is used I didn’t know the calculation, so the new learning that I took away from this lab was the calculation of the checksum which I referred was Wikipedia ” <https://en.wikipedia.org/wiki/User_Datagram_Protocol#Checksum_computation>” as I used it for the reference.

**Wireshark Lab: SSL**

Most of my previous working with SSL was in way where the certificate was given from the proxy and I didn’t have to see in detail the working of the SSL but it was more of working of application over SSL.

Here, in this lab I came to know about how an SSL encrypted data comes in from the network and that there are different stages which makes a HTTPS which is SSL HTTP work. Which involves a conversation between the end user client and the SSL enabled server which goes on from greeting, acknowledging, to key exchange and then the server sends the application data which is the web application contents to the server.