Daniel Picard

CSC 435 Distributed Systems 1

Prof. Clark Elliott

**Network Labs**

The network labs were designed to give students a deeper understanding of how networks operate through the use of several network tools. These tools were designed to give diagnostic views of a network and help network administrators better understand any difficulty they are having in their networks. The tools included were wireshark, nslookup, tracert/traceroute, and a simple web browser. These tools allowed the user to explore their network and better understand how network traffic operates.

Thankfully for myself, I have a strong background in computer security and often use the above mentioned tools in my daily life to troubleshoot any issues I am having. As such these labs were a good refresher into the basics of the operations of the tools and how more information can be gleaned from looking at the actual packet stream.

The most widely used tool for these labs was wireshark. This tool gives the user the capability to capture/record packets being sent from the host computer to other computers on the network. It has the capability to automatically rebuild sessions which made these labs much simpler as I did not have to hunt long for specific packets. The main task in our labs was to look at the packet structure of different types of requests and identify certain aspects of their construction and implementation. We looked closely at http packet requests as our current class focuses heavily on that aspect currently. We are able to see how a request and response were passed between client and server which will help not only in these labs but our upcoming web server in which we have to use firefox to communicate.

We further looked into DNS, UDP, and SSL packets to see how they are constructed and communicate between machines. Through wireshark we are able to see how SSL constructs a handshake in which to both verify the server and pass public keys between machines. Wireshark also allows for the ability to decrypt the encrypted traffic to dive further into the session. With UDP we were able to see how the packets are sent with a checksum to another machine without the need to worry about a response from the server. We were also able to verify the checksum between the packet to just as the remote machine would do to verify that the packet was received correctly. Lastly, we delved into DNS to see how networks translate human readable addresses such as google.com into an ip address. This was accomplished through nslookup where we can further look into all the authoritative servers for this domain.

The last tool that was used was tracert/traceroute which allows the user to discover where their packets are going and what route they take to get there. It will display all jumps along the way by a TTL scheme in which it will look to responses from packets that fail at further and further TTL values. The remote machines will send a ping response which can then be used to build the route in which our packets must travel to reach their final destination.

In all these labs, and question, give the students a good introduction into how a network operates and how information traverses around the internet. The questions helped guide the students to delve deeper into the packets to truly find out what information is being sent and how the information is being received.