**Wireshark**

1. **What Did You Do?**

In the Coursera Wireshark project, I was able to establish my knowledge towards network and protocol identification. This was a brand-new topic to me, so what I might believe is a huge new feat, is actually just the tip of the iceberg. However, here are some detailed processes I went through in learning about Wireshark for the first time. First, we discuss network and protocol identification itself, and this includes understanding what the network environment embodies and how to properly utilize it. Here, I began to familiarize myself with network topology, traffic patterns, and network protocols (such as TCP, HTTP/HTTPS, DNS). For example, a DNS translates domain names into IP addresses and analyzing network packets involves interpreting information sent from one device to another. Upon understanding the purpose of these elements, I was then able to move on to the actual implementation of Wireshark and begin capturing packets in real time. How Wireshark works to do this, is it gains access to an interface, in my case Ethernet, and listens to the network traffic. In a more detailed approach, I was able to open a capture file and analyze the times, sources, destinations, protocols, and packet lengths. When investigating the actual traffic flowing through the interface, I double-clicked on it and was supplied with all the packets and their hosts. Moving on to the next portion of the project, I analyzed an HTTP basic authentication, while HTTPS runs on port 443 and uses TLS, HTTP runs on a non-secure traffic and uses port 80. It uses a challenge and response mechanism and requests authentication information, such as a username and password. Lastly, I captured SSH and Telnet sessions; this included using a capture filter to isolate port 23 for Telnet and a host for SSH.

1. **What Are the Results?**

To start with the basics of what a DNS packet captures using Wireshark, I will break down what each piece of the response means. “No.”, for example “No. 905”, describes that specific packet’s number in the sequence of traffic. It provides a way to reference or identify the packet you are referring to. Next, there is a time, for example- 14.149852. This is simply the time the packet was captured (in seconds) in comparison to the time the capture was initially started. Source, or “10.199.0.2”, is the IP address of the DNS server. Destination, or “10.199.118.84” is the IP address of the client/user that made the request (where the packet is going, rather than where it is coming from). Protocol, “DNS” in my case, is what was used to translate domains into IP addresses. Length, for example “101”, is the packet length measured in bytes. Lastly, the information at the end provides a range of detail such as what domain, a DNS transaction ID, etc.

To identify if packets in a network are signaling a cyber-attack, you would look for abnormal activity such as high traffic volumes (DoS attacks) or unidentifiable port numbers (learning the port numbers for each protocol is vital for this reason). For analyzing an attack surface that could be used as a point of entry to a network, I am going to refer back to Nmap. Nmap is a wonderful tool to use in this situation as it can scan a network and find open ports. Performing regular scans will keep you informed on vulnerabilities and address these issues before they manifest. Unfortunately, ports 80 (HTTP) and 443 (HTTPS) are common web servers that are highly prone to attacks. Implementing security headers and/or deploying firewalls is a good defense to this problem and likewise a good habit to get into. Another result to note derives from the basic authentication portion of the project. Basic authentication yielded credentials that were converted into string format, this feature can pose a significant threat as your passwords can be intercepted and decoded. These results can be used to inform security planning and risk assessment by following best practices learned from this project. One way to do this would be ensuring you have a strong protocol, HTTP rather than HTTPS. Alongside and as previously mentioned, knowing what type of traffic to recognize as a threat and identifying open ports are also healthy acts to mitigate exploitations.

1. **What Did You Learn?**

Overall, I gained a strong understanding of networks, how data communicates, network protocols, and the roles of networks. The concept of attack surfaces allowed me to learn about vulnerabilities in a network and how these tools could be used for exploitational purposes. I learned that packets are essential for a network to perform correctly and coherently as well as how security measures regarding these topics reinforce the integrity of a system. I can utilize this knowledge in the future to manage traffic efficiently. Even on my personal computer, this would be helpful as to keep myself secure and protected against attacks. Lastly, I can use this information in an organizational setting by implementing techniques such as how to ensure data is encrypted during transportation.