**Research Report Wireshark**

Adrian Varela

WTAMU

CIDM 6340-70: Network Management and Information Security

Professor Murray Jennex

July 28, 2023

WHAT DID YOU DO

With Wireshark, I was able to complete a packet tracking of the devices that were connected in my network. The first thing I had to do was download Wire shark through my MacBook which was very similar to the startup wizard of NMAP tool. Through this downloading I had to give proper authorization to the use of my specific device to track the network connection and live packet tracing. Through the application menu you could view the WIFI and network options which you could connect to, for viewing of packet activity. When using the software, I decided to go through the tabs otherwise known as the dialog boxes to capture my live connections. Once the results were displayed, I investigated the outputs in which I received. I sorted through the source in which the IP address was given and looking at the results. When completing many of the source results I then filtered through the protocol on which ports were used. I looked through many of the tabs that gave endless information on the packets being traced as well as trying to understand more of the information that was obtained. Through this I specifically found a tab from Analyze that displayed expert information as an option as well as the view Coloring Rules options as well. To view the total packets that were being tracked I went the statistics and pulled up the Capture File Properties option. When analyzing the information through the packets I went through the info tab to see exactly the information that was processed through each source.

What were the Results?

The results were very informative as there were over 1,718 packets that were captured in my home address for the span of five minutes and seven seconds. There were some concerns when looking through the info tab. It seemed that some of my packets that were received may be malicious packets because it looked as if there were packets that were being dropped and then sent again from a suspicious IP address. This led me to investigate some more as well as making sure I was not going to be a victim to a cyber-attack. The results for the protocol were the following such as TLSv1.2 for the Transport Layer Security, TCP with ports mainly in 443 as the destination, UDP for User Datagram Protocol, MDNS for Multicast Doman Name System, ICMPv6, DNS, and ARP Address Resolution Protocol. Most of the concerns came from my TCPs due to the address attempting to continually try to communicate with one of my devices. As I looked through the tabs on top of the screen the results for the colors were described the categories of the protocols. The protocols that gave me concern were the Bad TCP just because it looked as though there was information that was being resent. The other protocol that gave me suspicions as well was the TCP RST which was labeled red for the exercise. As I looked through the results for most of my packets that were transferred the main data populated at the bottom of my screen. The application layer data on the bottom portion of the Wireshark packet capture was the most informative giving detailed information on each packet.

WHAT DID YOU LEARN

The list goes on from the amount of information I learned through the Wireshark packet tracking. This application can become an organization’s best friend or worst enemy if left in the wrong hands. This information that I learned from Wireshark displayed packets being transferred between devices on the network. As I went through this information, I understood that the color coordination was impactful making It easy to follow with the protocols. These rules for the color coordination can easily be restructured from the user, making it user friendly. As I looked through the endless options of information being retrieved, I noticed the bottom of the page broke down specifics of how each data was being transferred. This data pertained the ports being utilized, as well as gave the information from the Mac address to the actual name of the devices.

If people did not have time to look through the details, there were still specific information that is useful in the info tab right in the main display. When it came to where the communication piece is displayed it was as clear as day. The communication even let you filter the destination address and the source address that was trying to give the information out. While looking through the specifics of the of how the information can be received as well, I noticed there were options for a graph display as well for visual learners. This information can be informative to a company breaking it down even easier. This can help the organization for people that do not understand how to read source attacks and the vulnerabilities with the network. If not even worried with the vulnerability and trying to see when the network is the busiest in the workplace it can easily explain how the network traffic is working to their employer. I also learned there were multiple ways to capture the data and once captured there were many variations on how you could filter your data as well. The filtration can come from the bookmarks on the left of a display filter, or if you have something specific you are looking for you can easily just type the information in the textbox.

The final and probably the biggest takeaway I got from this tool specifically for a MacBook was how to stop an attack from happening with the help of Wireshark. When viewing the Bad TCP Protocols, I viewed what the IP address was from the source trying to gain the destination of one of my devices. When doing this I used this and opened my terminal to stop transmitting information to this unfamiliar IP address. This then help me ensure that my personal information was not being transmitted to an unfamiliar device. This tool was very helpful and informative. I believe if companies do not utilize their grey hats using Wire shark, I would recommend just for the safety of their users’ information.