Wireshark Assignment

Jim Kinter

CIDM6340

1. What did you do – Completed the Introduction to Cybersecurity Tools & Cyberattacks in Coursera course then used WireShark to interrogate traffic on my local network. I started with the NMAP output to identify which hosts are active on the network. I think chose several interesting hosts (Amazon Echo Dot, Windows PC, Ring Camera, and an iPhone). I then used the WireShark utility to systematically monitor the activity for each of these devices. To perform the task I selected the Wi-Fi adapter for the Orbi Mesh network connection that most of my devices connect to, applied a capture filter like “ether host 1C:4D:66:17:49:37” which is the MAC Address of the Amaxon Echo Show in my kitchen, then pressed enter to start capturing traffic associated with that particular device. Using this approach, once I started the capture for a particular device I would then go use the device to see what traffic was generated. After a few minutes I came back and saved the capture file for later review. I should note that I am running iOS Beta version 18.3 on my iPhone 15 Pro Max and, in order to get this to work I had to turn off Rotation of the Wi-Fi [MAC] Address as well as the “Limit IP Address Tracking” feature. I reviewed packet captures for interesting devices and conversations, diffing into the packet contents and trying to ascertain the payload.
2. What are the results – After reviewing an hour-long capture of traffic while the network was at peak utilization I don’t find anything that indicates any suspicious activity. I live in a remote location and the possibility of someone using my network without my knowledge is pretty slim; however the risk of a virus, malware, ransomware, et. al. attack is moderate to high. Specifically my youngest son, daughter, and in-law’s use cases are a real threat. I find a significant volume of MDNS (Multicast DNS) as well as HTTPS and TLS traffic. I also noticed a number of other protocols like NBNS (NetBios Naming Service), SSDP (Simple Service Discovery Protocol), and ARP (Address Resolution Protocol). I noticed some (~3%) re-transmissions and need to spend some time understanding their causes.
3. What did you learn – Wireshark captures and logs all traffic on the network, decomposing it per the OSI layers, exposing the data for each applicable layer for each packet. This exposed a notable volume of broadcast traffic associated with name resolution. In this exercise I learned a lot about how to identify what applications on my LAN might be misconfigured by looking for patterns of chattiness. I also learned how to use WireShark to monitor all of the traffic on one of the smart speakers or my phone to determine what information is actually being shared with Amazon or Apple. I learned that more information is being shared about me and my family than I realized and that, even though I have systematically reduced the attack surface of all of the devices in my house, I’m close to a point where I need to assess whether the benefits of having a voice interface to the internet is worth the risk/personal intrusion that I’m exchanging for that feature. I re-learned that networks are really chatty environments and that network performance on my home network, where there are often multiple concurrent streams happening, could be improved by using wireshark to determine where there is packet re-transmission happening, where there is persistent and pervasive name resolution dialogs happening, and how I might segment the network to improve performance. I learned that using NMAP and WIreShark together I can troubleshoot network issues using a fact-based/scientific approach rather than the “experience” and “hunch” approach that I’ve always used before. The most significant attack surface that I have on my home network is associated with the computers and email traffic used by my wife, kids, and in-laws. One of the key learnings from this exercise is that I need to be more vigilant about making sure that their devices are patched, that everyone understands best practices to prevent cyber-attacks, and that everyone knows what to do if they see something strange.