Yulong Tan

Info 341

10.7.2016

Lab 2: Ethernet/Data Link Frame Capture

During the lab, computers with Wireshark installed were connected via Ethernet cables into Ethernet ports. Wireshark saw all the connections that were happening on the Ethernet connection. After Telnet was used for remote access, we started the frame capture, and then filtered by Telnet. We could see the source IP and the destination IP, which in this case, packets were sent from 192.168.100.11 to 192.168.100.1. The data field of the telnet was where the password was and it displayed one character at a time. Looking through all the telnet data, we were able to see that the password was uwtest.

This lab teaches us how to troubleshoot, see frames, and basics of data capture. A scenario where it would provide useful would be in a location like a coffee shop, which would allow someone to see all the connections on a public, non-encrypted connection. Wireshark is a good tool that to understand network traffic analysis and how communication takes place when certain protocols are involved. At the same time, Wireshark can also reveal some security problems, like what the lab showed us. If there is no encryption, someone could use Wireshark in a more malicious manner, and steal information.