Packet Inspection

In this lab, we’ll use a Palo Alto firewall to analyze packets for information besides traditional Layer 2-4 header values & make security decisions based on the additional information.

Complete the following tasks to setup your firewall:

1. Assign appropriate IP settings to access the internet
2. Ensure that only the SSH protocol is blocked, regardless of port
3. Enable SSL decryption so that all HTTPS traffic will be analyzed by the firewall

Malware Capture

One of the challenges in handling incidents is capturing malware over the wire. Once malware hits a machine, it’s a bit late. For our purposes, we’ll use the EICAR Malware Test File, which is a file created to test the basic function of antivirus. We can access the testfile via: <http://2016.eicar.org/85-0-Download.html> Don’t worry, it’s not real malware, it’s just a string of text.

Your task: Create a rule that will capture a PCAP of any malware transfers. Export the PCAP and extract the malware from the capture. Show that you’ve exported the entire file. (You might want to use a Linux VM for this; Windows will be unhappy about the malware test file)