ENPM685 Homework #5 – Network Analysis Tools

Version 3.1 – March 11th 2022

Estimated time to complete this assignment: 1 hour.

Scenario: You're a SOC analyst working for a large organization. Someone in your organization alerted you to a suspect executable on their computer that they did not recognize and they have sent it to you for further analysis. Using your malware analysis workstation you created a brand new "victim" Windows VM and after setting up a packet capture for the VM you ran the executable to see what it does from a network perspective.

Now that you have the packet capture you need to analyze it and determine what the suspect executable does from a network perspective when it runs.

Items of note:

- The packet capture is available in the Files section of ELMS and also at https://glue.umd.edu/~kts/enpm685/pcaps/enpm685-bot.pcap
- The victim VM's IP address is 192.168.2.157
- The network gateway for the VM network is 192.168.2.2
- The packet capture is large (1762 packets!) so making use of filters to narrow down what you are analyzing will be helpful. (Review slides and the *Wireshark User's Guide* for more details on filters.)

Answer these questions:

1. Reviewing the network traffic, what is the first thing that the executable does? Why do you think it is doing it?
2. There is a large number of ARP queries, why do you think that is? What might the executable be doing?
3. Does the executable make any call out to a command and control server? If so, what is the IP address, host name, and/or URL it calls out to? What kind of a response does it receive?
4. After reviewing the packet capture of the network traffic generated by the executable and answering questions 1-3 what is your final determination – is the executable malicious? Provide a short write up on why or why not you believe the executable is malicious.

Deliverable

Your answers to the 4 questions above.