Lab10- Layer 7 Inspection

In this lab, we're going to implement a firewalling system that can inspect the actual data portion of the packet, often referred to as a Layer 7 firewall. These firewall implementations are not limited by basic assumptions made via basic protocols and ports.

Instructions

Perform the following tasks in an environment of your choosing.

1. Bring your C2 system online, ensuring the traffic flows through an intermediary device [firewall]
    a. Your intermediary device could be a pfSense firewall or a *nix distro of your choosing—you pick!
    b. Ensure that your C2 client can communicate with your C2 server
    c. Ensure that your C2 server can request any path or file from your client, requesting it to be uploaded
2. Install Snort or Suricata (or any other type of IDS, if you like) on your intermediary device and configure it to do deep packet inspection of the traffic flowing through the intermediary
3. Create custom rules that will detect the following types of traffic:
    a. Communications, such as check-ins, commands being issued, etc from your C2 server back to the client
    b. Detect the transference of a word document containing a social security number (ie, text in the format of: 867-53-0900, as you'd expect an SSN to look)

What to Submit

This lab is going to be mostly screenshot and documentation based. Ensure all of your screenshots & documentation are contained in a single PDF (not Word) document. Screenshots not contained in a single PDF won't be graded. Include your filters as standalone text files (also, do NOT paste any rule into a Word document).

Turn the following screenshots and other files in to the D2L Dropbox:

1. A screenshot showing that your IDS is up and running
2. A screenshot showing your C2 client uploading a file to the server.
3. A screenshot showing the IDS alert detecting the presence of your C2 client/server communications.
4. A screenshot showing the IDS alert detecting a SSN being transferred across the network.
5. Upload your custom rule file(s) as separate documents to the Dropbox.

Grading

Your grades will be based off of a rubric that includes the following items:

1. Successful implementation of the IDS platform
2. Successful detection of C2 activities based on your own signatures
3. Successful detection of SSNs being transferred across a network
4. Proper formatting, following good technology standards, and meeting submission guidelines.