Lab 07 - Signature Development

The goal of this lab is to write your own custom rules based off of the PCAPs provided. Keep the following in mind:

* Rules can be somewhat subjective; focus on writing signatures that minimize false-positives. Yet at the same time, they should not be overly specific as to exclude likely variations.
* Try to be precise with your rules, but keep in mind that there may be a performance impact depending on how you write them. While this lab does NOT focus on performance, this is a significant factor if writing and using rules on real systems.
* You will only be testing your signatures against the PCAPs provided. However, if you were writing these for a production system, you would want to test on a non-production sensor or large PCAPs of your organization’s traffic.

A lab environment is provided to you in the IA lab, but you are welcome to use other environments you may have access to.

For each, include a clear screenshot as well of both the rule and showing that you got results in the log. All of these should be in a custom.rules file that you create, and each should have a unique SID. **You will upload the custom.rules file.** To receive full credit, your rules must work! If they do not, only partial credit is available.

**Sample 1**

Word-Dropper.pcap

Create a signature that will match on the HTTP requests in frames 3434 and 3437 (client -> server).

**Sample 2**

CryptoLocker.pcap

Create a signature, using flowbits, that will match on the request and response starting at frame 813 (follow HTTP stream to see the request/response). Alert on the response in frame 817.

**Sample 3**

2019-03-29-password-protected-Word-doc-pushes-Dridex

Create a signature that will alert on the response that contains a PE file. Similar to sample 2, this should be two rules, one to match on the request, the other to match (and alert) on the response. Use flowbits to control this sequence. This is similar to one of our in class demos. Here, you will want to refine and improve upon what we did in class.

**Sample 4**

2021-02-05-Spelevo-EK-sends-SmokeLoader.pcap

Create a signature to detect the landing page 2021-02-05-Spelevo-EK-landing-page.

**Deliverables**

Turn in a Word document or PDF with a screenshot of each rule you created along with the alert it generates when using with Suricata.

Turn in the custom.rules that works; each rule should have a unique sid.