Examine signatures with Suricata

Previously, you learned about signature-based analysis.
You also learned how to read signatures used in network-based intrusion detection systems.
Here, we'll use an open source signature-based IDS called Suricata to examine a signature.
Many NIDS technologies come with pre-written signatures.
You can think of these signatures as customizable templates.
Sort of like different templates available in a word processor.
These signature templates provide you with a starting point for writing and defining your rules.
You can also write and add your own rules.
Let's examine a pre-written signature through Suricata.
On this Linux machine running Ubuntu, Suricata is already installed.
Let's examine some of its files by changing directories to the etc directory and into the suricata directory.
This is where all of Suricata's configuration files live.
Next, we'll use the ls command to list the contents of the suricata directory.
There's a couple of different files in here, but we'll focus on the rules folder.
This is where the pre-written signatures are.
You can also add custom signatures here.
We'll use the cd command followed by the name of the folder to navigate to that folder.
Using the ls command, we can observe that the folder contains some rule templates for different protocols and services.
Let's examine the custom.rules file using the less command.
As a quick refresher, the less command returns the content of a file one page at a time which makes it easy to move forward and backward through the content.
We'll use the arrow key to scroll up.
Lines that begin with a pound sign (#) are comments meant to provide context for those who read them and are ignored by Suricata.
The first line says Custom rules example for HTTP connection.
This tells us that this file contains custom rules for HTTP connections.
We can observe that there's a signature.
The first word specifies the signature's ACTION.
For this signature, the action is alert.
This means that the signature generates an alert when all of the conditions are met.
The next part of the signature is the HEADER.
It specifies the protocol http.
The source IP address is HOME_NET and source port is defined as ANY.
The arrow indicates the direction of traffic coming from the home network and going to the destination IP address EXTERNAL_NET and ANY destination port.
So far, we know that this signature triggers an alert when it detects any HTTP traffic leaving the home network and going to the external network.

Let's examine the remainder of the signature to identify if there's any additional conditions the signature looks for.
The last part of the signature includes the RULE OPTIONS.
They're enclosed in parentheses and separated by semicolons.
There's many options listed here, but we'll focus on the message, flow, and content options.
The message option will show the message "GET on wire" once the alert is triggered.
The flow option is used to match on direction of network traffic flow.
Here, it's established.
This means that a connection has been successfully made.
The content option inspects the content of a packet.
Here, between the quotation marks, the text GET is specified.
GET is an HTTP request that's used to retrieve and request data from a server.
This means the signature will match if a network packet contains the text GET, indicating a request.
To summarize, this signature alerts anytime Suricata observes the text GET in an HTTP connection from the home network, going to the external network.
Every environment is different and in order for an IDS to be effective, signatures must be tested and tailored.
As a security analyst, you may test, modify, or create IDS signatures to improve the detection of threats in an environment and reduce the likelihood of false positives.
Coming up, we'll examine how Suricata logs events.
Meet you there.

Revision #1
Created 2023-11-02 12:54:14 UTC by naruzkurai
Updated 2023-11-02 12:54:42 UTC by naruzkurai