SURICATA RULES AND LOGS

Task 1 - Examine and Explain Suricata Custom Rules

The /home/analyst directory contains a custom.rules file that defines the network traffic rules and a sample.pcap file.

I use the cat custom.rules command to display the contents of the rules file (my commands highlighted in gray)

```
analyst@4dfdd57d1bcf:~$ cat custom.rules
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:
12345; rev:3;)
analyst@4dfdd57d1bcf:~$
```

The returned file contents:

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;)

Alert is the action which Suricata will take when a packet matches this rule.

Http is the first part of the header and the protocol which Suricata will apply this rule to.

$HOME_NET any is a variable defined in the */etc/suricata/suricata.yaml* definitions file to be a placeholder for a local network while *any* designates any port on the network. In this instance *$HOME_NET* is defined as *172.21.224.0/20*.

The *msg:* option provides the text to output to explain why the alert was triggered, in this case "GET on wire".

The *flow:established,to_server* option determines packets from the client to the server should be matched.

The *content:"GET"* option tells Suricata to look for GET in the content of the http.method part of the packet.

The *sid:12345* option is a unique number to identify the rule while *rev:3* shows this is the third revision of the rule.

TASK 2 - Trigger a Suricata Rule

Run Suricata using the custom.rules and sample.pcap files to generate log files.

The command:

sudo suricata -r sample.pcap -S custom.rules -k none

```
analyst@4dfdd57d1bcf:~$ sudo suricata -r sample.pcap -S custom.rules -k none
9/12/2023 -- 19:52:51 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
9/12/2023 -- 19:52:52 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
9/12/2023 -- 19:52:52 - <Notice> - Signal Received.  Stopping engine.
9/12/2023 -- 19:52:52 - <Notice> - Pcap-file module read 1 files, 200 packets, 54238 bytes
analyst@4dfdd57d1bcf:~$
```

The *-r* option specifies an input file (sample.pcap).

The *-S* instructs Suricata to use the rules defined in custom.rules.

The *-k none* option instructs Suricata to disable checksums.

Examine the logs

As can be seen below Suricata created four log files using the custom rules and sample.pcap.

```
analyst@4dfdd57d1bcf:~$ ls -l /var/log/suricata
total 16
-rw-r--r-- 1 root root 1418 Dec  9 19:52 eve.json
-rw-r--r-- 1 root root  292 Dec  9 19:52 fast.log
-rw-r--r-- 1 root root 3239 Dec  9 19:52 stats.log
-rw-r--r-- 1 root root 1512 Dec  9 19:52 suricata.log
analyst@4dfdd57d1bcf:~$
```

The most useful of these four is usually the eve.json file as it contains the most detailed summary of events. It is a standard json output file and JQuery is used to examine it.

Output of the eve.json file (shortened for space)

```
analyst@4dfdd57d1bcf:~$
analyst@4dfdd57d1bcf:~$ jq . /var/log/suricata/eve.json | less
{
  "timestamp": "2022-11-23T12:38:34.624866+0000",
  "flow_id": 172943641049237,
  "pcap_cnt": 70,
  "event_type": "alert",
  "src_ip": "172.21.224.2",
  "src_port": 49652,
  "dest_ip": "142.250.1.139",
  "dest_port": 80,
  "proto": "TCP",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 12345,
```