Suricata_notebook_etudiant

March 11, 2022

1 Sujet et intérêt

Suricata est un système de détection d'intrusion par signature. Il écoute le réseau, enregistre les flux et génère des alertes.

Si il reconnaît un motif malveillant dans les paquets réseaux, Suricata enregistre l'information dans un fichier eve.json Comme son nom l'indique, eve.json contient des enregistrements au format json.

Ce format s'est imposé au cours des dernières années dans l'échange de données applicatives mais aussi dans le domaine de la sécurité. Il est donc important de comprendre comment extraire des informations intéressantes de ce type de fichier:

jq est un utilitaire capable de parser , filter et afficher d'une manière attrayante les fichiers au format json comme le montre la documentation de Suricata. (voir https://suricata.readthedocs.io/en/latest/output/eve/eve-json-examplesjq.html)

Il vous est demandé dans ce TD de ré-implémenter quelques unes de ces commandes en Python. Le commandes vous sont données, à vous de développer le code Python réalisant à l'identique ce que fait la commande jq.

Vous pouvez installer jq par "apt".

2 Affichez les 3 premiers enregistrements du fichier eve.json

Affichez les 3 premiers enregistrements du fichier comme avec la commande "cat eve.json | jq –slurp '.[:10]' ".

Vous utiliserez le package rich afin de coloriser la sortie comme le fait jq. Il vous faudra charger chaque ligne du fichier eve.json dans une liste au préalable avant d'afficher les les lignes au format json

[ ]:
```
cat eve.json | jq --slurp '.[:3]'
```

```
[
  {
    "timestamp":
"2022-03-06T18:27:36.272016+0000",
    "flow_id": 1743533308628693,
    "in_iface": "enp12s0",
    "event_type": "flow",
    "src_ip":
"2a01:cb1d:8adc:6200:c049:ccc9:ed09:31c6",
    "src_port": 43908,
    "dest_ip":
"2a01:cb1d:8adc:6200:4a29:52ff:fe26:90b0",
    "dest_port": 53,
    "proto": "UDP",
    "app_proto": "dns",
    "flow": {
      "pkts_toserver": 1,
      "pkts_toclient": 1,
      "bytes_toserver": 103,
      "bytes_toclient": 239,
      "start":
"2022-03-06T18:20:51.446165+0000",
      "end":
"2022-03-06T18:20:51.474768+0000",
      "age": 0,
      "state": "established",
      "reason": "timeout",
      "alerted": false
    }
  },
  {
    "timestamp":
"2022-03-06T18:27:36.272067+0000",
    "flow_id": 336201376622743,
    "in_iface": "enp12s0",
    "event_type": "flow",
```

3 Fournissez la liste des signatures comme le fait la commande suivante

Vous pouvez utiliser le module Counter du package collections afin de compter facilement les enregistrements.

[ ]:
```
cat eve.json | jq 'select(.event_type == "alert")|.alert.signature'|sort |uniq␣
↪-c|sort -nr
```

```
   1367 "SURICATA STREAM ESTABLISHED packet out of window"
    467 "ET POLICY Dropbox Client Broadcasting"
    283 "ET INFO Observed DNS Query to .cloud TLD"
    185 "SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Tofsee)"
    110 "SURICATA STREAM Packet with invalid ack"
    107 "SURICATA STREAM ESTABLISHED invalid ack"
     56 "SURICATA Applayer Detect protocol only one direction"
     51 "ET POLICY Dropbox.com Offsite File Backup in Use"
      9 "SURICATA STREAM 3way handshake wrong seq wrong ack"
      8 "SURICATA STREAM excessive retransmissions"
      7 "SURICATA STREAM CLOSEWAIT FIN out of window"
      7 "ET POLICY Dropbox DNS Lookup - Possible Offsite File Backup in Use"
      6 "ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)"
      5 "ET ATTACK_RESPONSE Output of id command from HTTP server"
      4 "SURICATA TLS invalid record/traffic"
      4 "SURICATA TLS invalid handshake message"
      4 "SURICATA STREAM Packet with invalid timestamp"
      3 "TGI HUNT Wget User-Agent to IP Address"
      3 "SURICATA UDPv6 invalid checksum"
      3 "SURICATA STREAM SHUTDOWN RST invalid ack"
      3 "ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package
management"
      2 "SURICATA STREAM pkt seen on wrong thread"
      2 "GPL WEB_SERVER 403 Forbidden"
      2 "ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent"
      1 "TGI HUNT PHP magic bytes in HTTP response"
      1 "SURICATA UDPv4 invalid checksum"
      1 "SURICATA HTTP unable to match response to request"
      1 "SURICATA Applayer Wrong direction first Data"
      1 "ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt"
      1 "ET SCAN PHP Attack Tool Morfeus F Scanner"
      1 "ET POLICY PE EXE or DLL Windows file download HTTP"
      1 "ET INFO Windows OS Submitting USB Metadata to Microsoft"
```

4 Donnez le top 10 des ports de destination comme le fait la commande suivante

[ ]:
```
cat eve.json | jq -c 'select(.event_type=="flow")|[.proto, .dest_port]'|sort␣
↪|uniq -c|sort -nr|head -n10
```

```
  58199 ["UDP",53]
   5010 ["TCP",443]
   4783 ["UDP",15600]
   4527 ["UDP",1900]
   2298 ["UDP",5353]
   2207 ["IPv6-ICMP",null]
   1610 ["UDP",17500]
   1583 ["TCP",4443]
   1148 ["UDP",547]
    823 ["UDP",443]
```