TP Nushell Helec Bastien

```
# TP Nushell Helec Bastien
22/05/2024
```

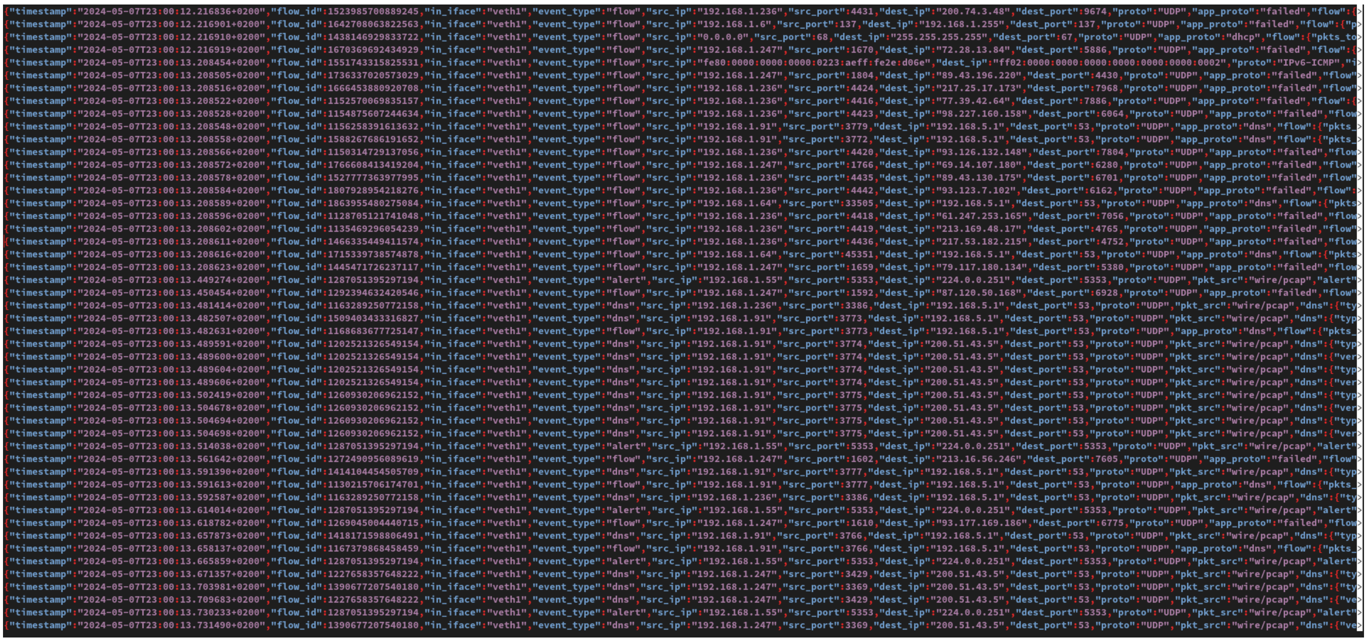
Preparation de l'analyse:

On va analyser le fichier eve2.json avec nushell pour cela on va d'abord devoir transferer le fichiers avec la commande scp :

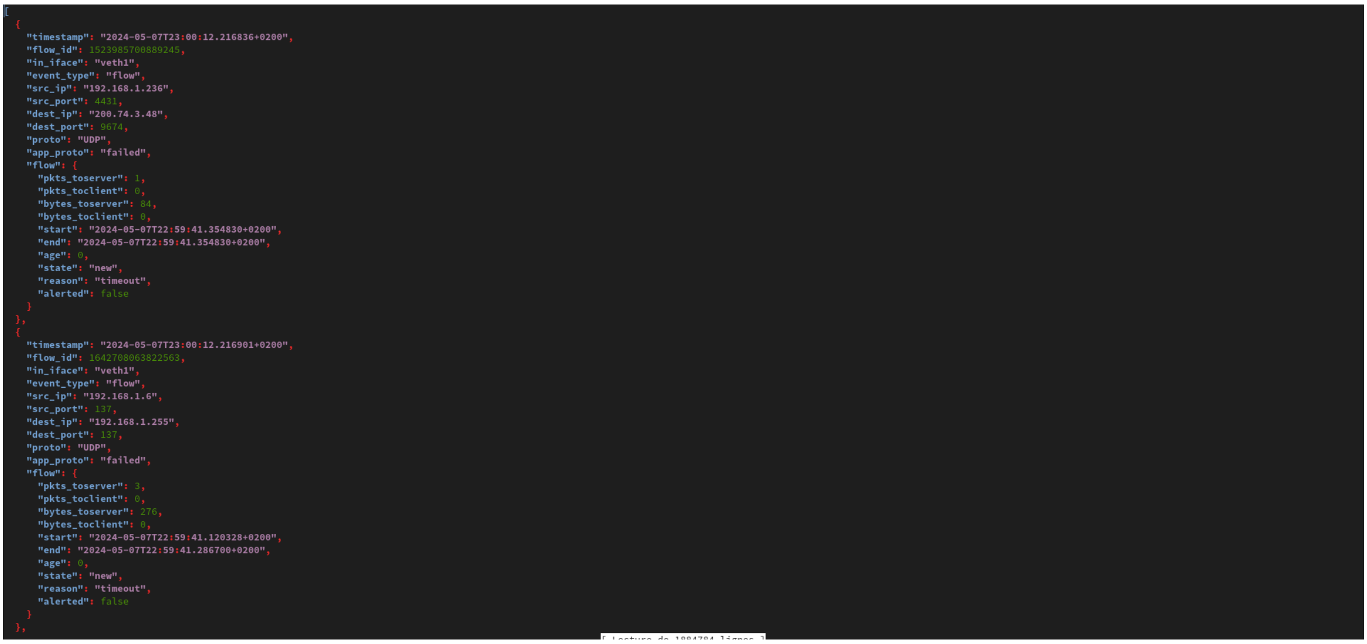
```
scp eve2.json user@ip:/path/to/folder
```

Puis on fait la commande suivante :

```
jq -s '.' eve2.json | save -f eve.json
```



```
{"timestamp":"2024-05-07T23:00:12.216836+0200","flow_id":1523985700889245,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4431,"dest_ip":"200.74.3.48","dest_port":9674,"proto":"UDP","app_proto":"failed","flow":{>
{"timestamp":"2024-05-07T23:00:12.216901+0200","flow_id":1642708063822563,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.6","src_port":137,"dest_ip":"192.168.1.255","dest_port":137,"proto":"UDP","app_proto":"failed","flow":{"p>
{"timestamp":"2024-05-07T23:00:12.216910+0200","flow_id":1438146929833722,"in_iface":"veth1","event_type":"flow","src_ip":"0.0.0.0","src_port":68,"dest_ip":"255.255.255.255","dest_port":67,"proto":"UDP","app_proto":"dhcp","flow":{"pkts_to>
{"timestamp":"2024-05-07T23:00:12.216919+0200","flow_id":1670369692434929,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1670,"dest_ip":"72.28.13.84","dest_port":5886,"proto":"UDP","app_proto":"failed","flow":{>
{"timestamp":"2024-05-07T23:00:13.208454+0200","flow_id":1551743315825531,"in_iface":"veth1","event_type":"flow","src_ip":"fe80:0000:0000:0000:0223:aeff:fe2e:d06e","dest_ip":"ff02:0000:0000:0000:0000:0000:0000:0002","proto":"IPv6-ICMP","i>
{"timestamp":"2024-05-07T23:00:13.208505+0200","flow_id":1736337020573029,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1804,"dest_ip":"89.43.196.220","dest_port":4430,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.208516+0200","flow_id":1666453880920708,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4424,"dest_ip":"217.25.17.173","dest_port":7968,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.208522+0200","flow_id":1152570069835157,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4416,"dest_ip":"77.39.42.64","dest_port":7886,"proto":"UDP","app_proto":"failed","flow":{>
{"timestamp":"2024-05-07T23:00:13.208528+0200","flow_id":1154875607244634,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4423,"dest_ip":"98.227.160.158","dest_port":6064,"proto":"UDP","app_proto":"failed","flow>
{"timestamp":"2024-05-07T23:00:13.208548+0200","flow_id":1156258391613632,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.91","src_port":3779,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_>
{"timestamp":"2024-05-07T23:00:13.208558+0200","flow_id":1588267686191652,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.91","src_port":3772,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_>
{"timestamp":"2024-05-07T23:00:13.208566+0200","flow_id":1150314729137056,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4420,"dest_ip":"93.126.132.148","dest_port":7804,"proto":"UDP","app_proto":"failed","flow>
{"timestamp":"2024-05-07T23:00:13.208572+0200","flow_id":1766608413419204,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1766,"dest_ip":"69.14.107.180","dest_port":6280,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.208578+0200","flow_id":1527777363977995,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4435,"dest_ip":"89.43.130.175","dest_port":6701,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.208584+0200","flow_id":1807928954218276,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4442,"dest_ip":"93.123.7.102","dest_port":6162,"proto":"UDP","app_proto":"failed","flow":>
{"timestamp":"2024-05-07T23:00:13.208589+0200","flow_id":1863955480275084,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.64","src_port":33505,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts>
{"timestamp":"2024-05-07T23:00:13.208596+0200","flow_id":1128705121741048,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4418,"dest_ip":"61.247.253.165","dest_port":7056,"proto":"UDP","app_proto":"failed","flow>
{"timestamp":"2024-05-07T23:00:13.208602+0200","flow_id":1135469296054239,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4419,"dest_ip":"213.169.48.17","dest_port":4765,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.208611+0200","flow_id":1466335449411574,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.236","src_port":4436,"dest_ip":"217.53.182.215","dest_port":4752,"proto":"UDP","app_proto":"failed","flow>
{"timestamp":"2024-05-07T23:00:13.208616+0200","flow_id":1715339738574878,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.64","src_port":45351,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts>
{"timestamp":"2024-05-07T23:00:13.208623+0200","flow_id":1445471726237117,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1659,"dest_ip":"79.117.180.134","dest_port":5380,"proto":"UDP","app_proto":"failed","flow>
{"timestamp":"2024-05-07T23:00:13.449274+0200","flow_id":1287051395297194,"in_iface":"veth1","event_type":"alert","src_ip":"192.168.1.55","src_port":5353,"dest_ip":"224.0.0.251","dest_port":5353,"proto":"UDP","pkt_src":"wire/pcap","alert">
{"timestamp":"2024-05-07T23:00:13.450454+0200","flow_id":1292394632420546,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1592,"dest_ip":"87.120.50.168","dest_port":6928,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.481414+0200","flow_id":1163289250772158,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.236","src_port":3386,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ty>
{"timestamp":"2024-05-07T23:00:13.482507+0200","flow_id":1509403433316827,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3773,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.482631+0200","flow_id":1168683677725147,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.91","src_port":3773,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_>
{"timestamp":"2024-05-07T23:00:13.489591+0200","flow_id":1202521326549154,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3774,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.489600+0200","flow_id":1202521326549154,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3774,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ver>
{"timestamp":"2024-05-07T23:00:13.489604+0200","flow_id":1202521326549154,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3774,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.489606+0200","flow_id":1202521326549154,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3774,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ver>
{"timestamp":"2024-05-07T23:00:13.502419+0200","flow_id":1260930206962152,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3775,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.504678+0200","flow_id":1260930206962152,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3775,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ver>
{"timestamp":"2024-05-07T23:00:13.504694+0200","flow_id":1260930206962152,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3775,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.504698+0200","flow_id":1260930206962152,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3775,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ver>
{"timestamp":"2024-05-07T23:00:13.514038+0200","flow_id":1287051395297194,"in_iface":"veth1","event_type":"alert","src_ip":"192.168.1.55","src_port":5353,"dest_ip":"224.0.0.251","dest_port":5353,"proto":"UDP","pkt_src":"wire/pcap","alert">
{"timestamp":"2024-05-07T23:00:13.561642+0200","flow_id":1272490956089619,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1602,"dest_ip":"213.16.56.246","dest_port":7605,"proto":"UDP","app_proto":"failed","flow">
{"timestamp":"2024-05-07T23:00:13.591390+0200","flow_id":1414104454505709,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3777,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.591613+0200","flow_id":1130215706174701,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.91","src_port":3777,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_>
{"timestamp":"2024-05-07T23:00:13.592587+0200","flow_id":1163289250772158,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.236","src_port":3386,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ty>
{"timestamp":"2024-05-07T23:00:13.614014+0200","flow_id":1287051395297194,"in_iface":"veth1","event_type":"alert","src_ip":"192.168.1.55","src_port":5353,"dest_ip":"224.0.0.251","dest_port":5353,"proto":"UDP","pkt_src":"wire/pcap","alert">
{"timestamp":"2024-05-07T23:00:13.618782+0200","flow_id":1269045004440715,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.247","src_port":1610,"dest_ip":"93.177.169.186","dest_port":6775,"proto":"UDP","app_proto":"failed","flow>
{"timestamp":"2024-05-07T23:00:13.657873+0200","flow_id":1418171598806491,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.91","src_port":3766,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"typ>
{"timestamp":"2024-05-07T23:00:13.658137+0200","flow_id":1167379868458459,"in_iface":"veth1","event_type":"flow","src_ip":"192.168.1.91","src_port":3766,"dest_ip":"192.168.5.1","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"pkts_>
{"timestamp":"2024-05-07T23:00:13.665859+0200","flow_id":1287051395297194,"in_iface":"veth1","event_type":"alert","src_ip":"192.168.1.55","src_port":5353,"dest_ip":"224.0.0.251","dest_port":5353,"proto":"UDP","pkt_src":"wire/pcap","alert">
{"timestamp":"2024-05-07T23:00:13.671357+0200","flow_id":1227658357648222,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.247","src_port":3429,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ty>
{"timestamp":"2024-05-07T23:00:13.703981+0200","flow_id":1390677207540180,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.247","src_port":3369,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ty>
{"timestamp":"2024-05-07T23:00:13.709683+0200","flow_id":1227658357648222,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.247","src_port":3429,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ve>
{"timestamp":"2024-05-07T23:00:13.730233+0200","flow_id":1287051395297194,"in_iface":"veth1","event_type":"alert","src_ip":"192.168.1.55","src_port":5353,"dest_ip":"224.0.0.251","dest_port":5353,"proto":"UDP","pkt_src":"wire/pcap","alert">
{"timestamp":"2024-05-07T23:00:13.731490+0200","flow_id":1390677207540180,"in_iface":"veth1","event_type":"dns","src_ip":"192.168.1.247","src_port":3369,"dest_ip":"200.51.43.5","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"ve>
```

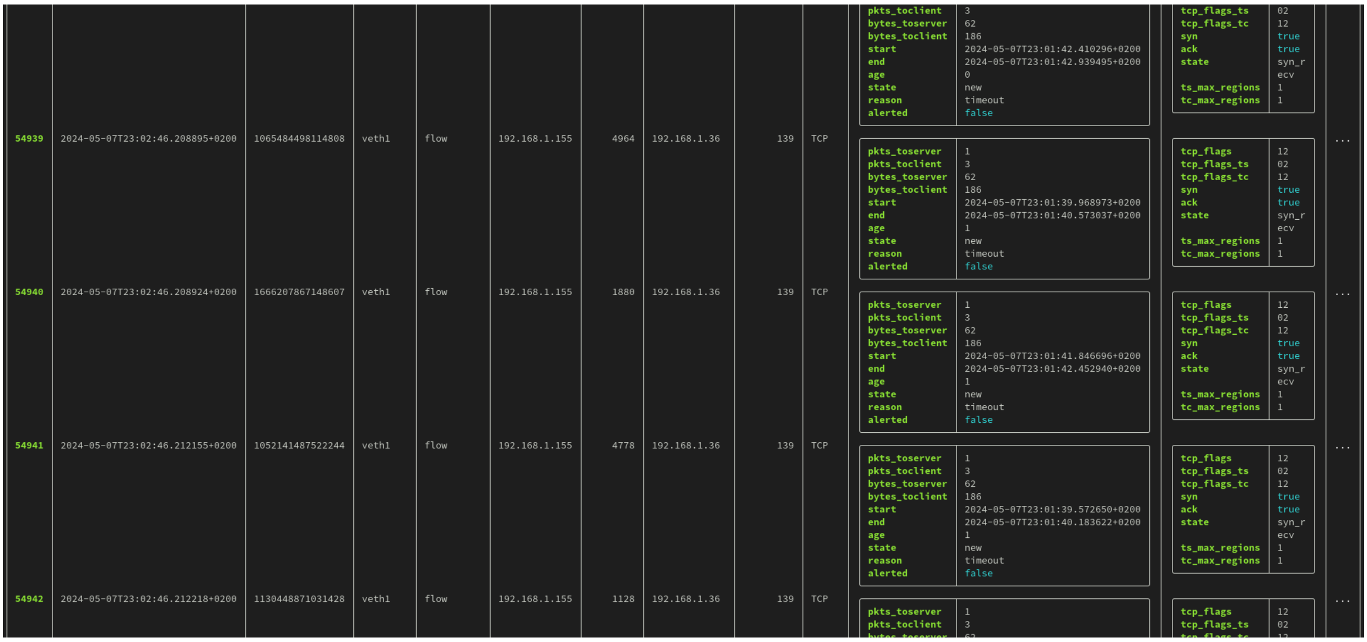


```
[
  {
    "timestamp": "2024-05-07T23:00:12.216836+0200",
    "flow_id": 1523985700889245,
    "in_iface": "veth1",
    "event_type": "flow",
    "src_ip": "192.168.1.236",
    "src_port": 4431,
    "dest_ip": "200.74.3.48",
    "dest_port": 9674,
    "proto": "UDP",
    "app_proto": "failed",
    "flow": {
      "pkts_toserver": 1,
      "pkts_toclient": 0,
      "bytes_toserver": 84,
      "bytes_toclient": 0,
      "start": "2024-05-07T22:59:41.354830+0200",
      "end": "2024-05-07T22:59:41.354830+0200",
      "age": 0,
      "state": "new",
      "reason": "timeout",
      "alerted": false
    }
  },
  {
    "timestamp": "2024-05-07T23:00:12.216901+0200",
    "flow_id": 1642708063822563,
    "in_iface": "veth1",
    "event_type": "flow",
    "src_ip": "192.168.1.6",
    "src_port": 137,
    "dest_ip": "192.168.1.255",
    "dest_port": 137,
    "proto": "UDP",
    "app_proto": "failed",
    "flow": {
      "pkts_toserver": 3,
      "pkts_toclient": 0,
      "bytes_toserver": 276,
      "bytes_toclient": 0,
      "start": "2024-05-07T22:59:41.120328+0200",
      "end": "2024-05-07T22:59:41.286700+0200",
      "age": 0,
      "state": "new",
      "reason": "timeout",
      "alerted": false
    }
  },
                                  [ Lecture de 1884784 lignes ]
```

Cette commande permet de transformer le fichier eve2.json en un fichier eve.json qui est plus lisible. avec les bonnes indentations.

On peu a présent faire l'analyse du fichier eve.json avec nushell :

```
open eve.json
```

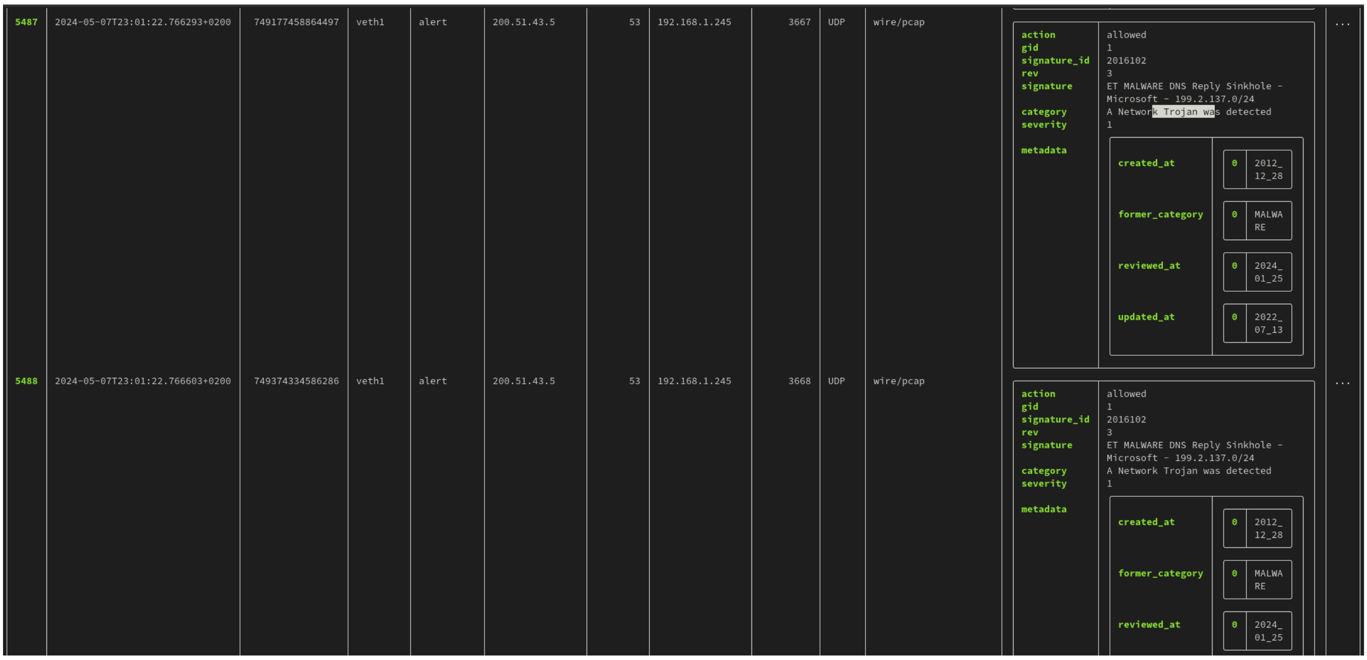


```
                                                                                                    pkts_toclient    3                                      tcp_flags_ts     02
                                                                                                    bytes_toserver   62                                     tcp_flags_tc     12
                                                                                                    bytes_toclient   186                                    syn              true
                                                                                                    start            2024-05-07T23:01:42.410296+0200        ack              true
                                                                                                    end              2024-05-07T23:01:42.939495+0200        state            syn_r
                                                                                                    age              0                                                       ecv
                                                                                                    state            new                                    ts_max_regions   1
                                                                                                    reason           timeout                                tc_max_regions   1
                                                                                                    alerted          false
54939  2024-05-07T23:02:46.208895+0200  1065484498114808  veth1  flow  192.168.1.155  4964  192.168.1.36  139  TCP                                                                     ...
                                                                                                    pkts_toserver    1                                      tcp_flags        12
                                                                                                    pkts_toclient    3                                      tcp_flags_ts     02
                                                                                                    bytes_toserver   62                                     tcp_flags_tc     12
                                                                                                    bytes_toclient   186                                    syn              true
                                                                                                    start            2024-05-07T23:01:39.968973+0200        ack              true
                                                                                                    end              2024-05-07T23:01:40.573037+0200        state            syn_r
                                                                                                    age              1                                                       ecv
                                                                                                    state            new                                    ts_max_regions   1
                                                                                                    reason           timeout                                tc_max_regions   1
                                                                                                    alerted          false
54940  2024-05-07T23:02:46.208924+0200  1666207867148607  veth1  flow  192.168.1.155  1880  192.168.1.36  139  TCP                                                                     ...
                                                                                                    pkts_toserver    1                                      tcp_flags        12
                                                                                                    pkts_toclient    3                                      tcp_flags_ts     02
                                                                                                    bytes_toserver   62                                     tcp_flags_tc     12
                                                                                                    bytes_toclient   186                                    syn              true
                                                                                                    start            2024-05-07T23:01:41.846696+0200        ack              true
                                                                                                    end              2024-05-07T23:01:42.452940+0200        state            syn_r
                                                                                                    age              1                                                       ecv
                                                                                                    state            new                                    ts_max_regions   1
                                                                                                    reason           timeout                                tc_max_regions   1
                                                                                                    alerted          false
54941  2024-05-07T23:02:46.212155+0200  1052141487522244  veth1  flow  192.168.1.155  4778  192.168.1.36  139  TCP                                                                     ...
                                                                                                    pkts_toserver    1                                      tcp_flags        12
                                                                                                    pkts_toclient    3                                      tcp_flags_ts     02
                                                                                                    bytes_toserver   62                                     tcp_flags_tc     12
                                                                                                    bytes_toclient   186                                    syn              true
                                                                                                    start            2024-05-07T23:01:39.572650+0200        ack              true
                                                                                                    end              2024-05-07T23:01:40.183622+0200        state            syn_r
                                                                                                    age              1                                                       ecv
                                                                                                    state            new                                    ts_max_regions   1
                                                                                                    reason           timeout                                tc_max_regions   1
                                                                                                    alerted          false
54942  2024-05-07T23:02:46.212218+0200  1130448871031428  veth1  flow  192.168.1.155  1128  192.168.1.36  139  TCP                                                                     ...
                                                                                                    pkts_toserver    1                                      tcp_flags        12
                                                                                                    pkts_toclient    3                                      tcp_flags_ts     02
```

Analyse du fichier :

Il y a présence d'une faille suricata pour cela on va observer les alertes suricata :

```
open eve.json | where event_type == "alert"
```



```
5487  2024-05-07T23:01:22.766293+0200  749177458864497  veth1  alert  200.51.43.5  53  192.168.1.245  3667  UDP  wire/pcap                                                 ...
                                                                                                    action         allowed
                                                                                                    gid            1
                                                                                                    signature_id   2016102
                                                                                                    rev            3
                                                                                                    signature      ET MALWARE DNS Reply Sinkhole -
                                                                                                                   Microsoft - 199.2.137.0/24
                                                                                                    category       A Network Trojan was detected
                                                                                                    severity       1

                                                                                                    metadata         created_at          0  2012_
                                                                                                                                            12_28

                                                                                                                     former_category     0  MALWA
                                                                                                                                            RE

                                                                                                                     reviewed_at         0  2024_
                                                                                                                                            01_25

                                                                                                                     updated_at          0  2022_
                                                                                                                                            07_13
5488  2024-05-07T23:01:22.766603+0200  749374334586286  veth1  alert  200.51.43.5  53  192.168.1.245  3668  UDP  wire/pcap                                                 ...
                                                                                                    action         allowed
                                                                                                    gid            1
                                                                                                    signature_id   2016102
                                                                                                    rev            3
                                                                                                    signature      ET MALWARE DNS Reply Sinkhole -
                                                                                                                   Microsoft - 199.2.137.0/24
                                                                                                    category       A Network Trojan was detected
                                                                                                    severity       1

                                                                                                    metadata         created_at          0  2012_
                                                                                                                                            12_28

                                                                                                                     former_category     0  MALWA
                                                                                                                                            RE

                                                                                                                     reviewed_at         0  2024_
                                                                                                                                            01_25
```

On voit a premiere vue qu'il ya présence d'une alerte suricata sur trojan DNS.

Analyse avancée :

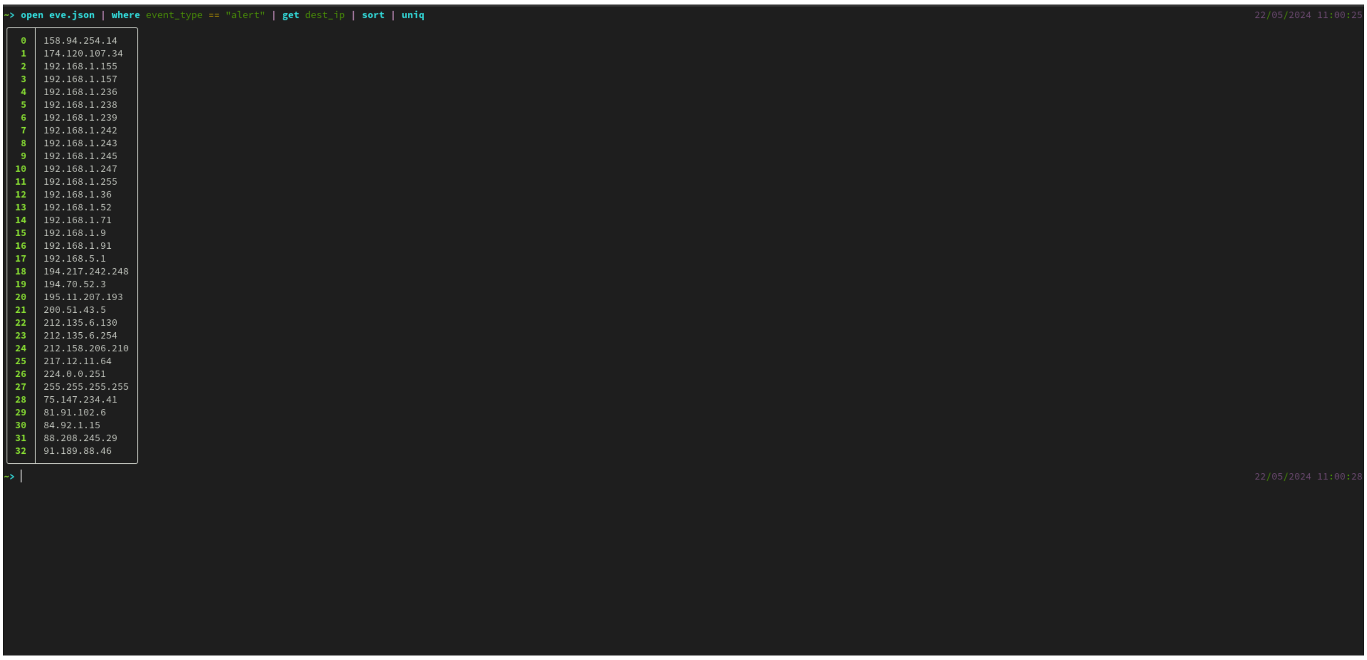
On va maintenant faire une analyse plus pousser sur tous ce qui es lié a ce trojan:

- Adresse IP touchée
- Port touché
- Protocole utilisé

- les types d'events
- La sévérité des events alertes

- Les ip touchées :

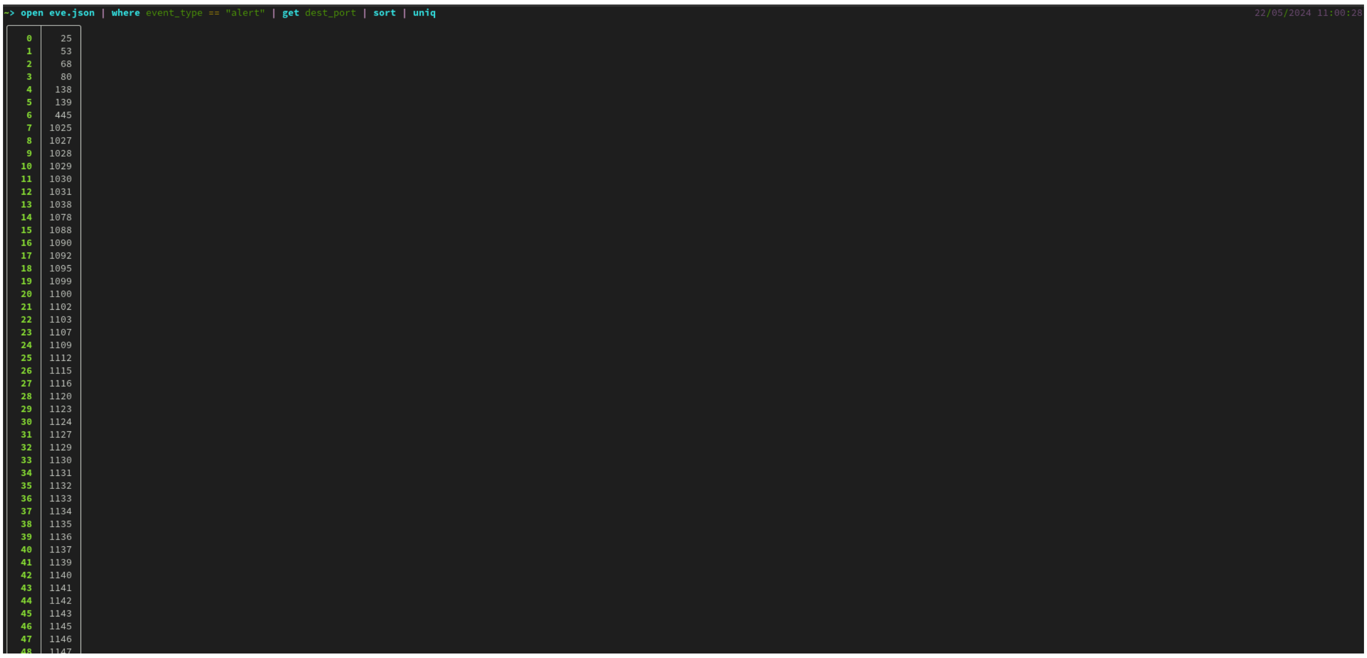
```
open eve.json | where event_type == "alert" | get dest_ip| sort | uniq
```



```
~> open eve.json | where event_type == "alert" | get dest_ip | sort | uniq          22/05/2024 11:00:25
╭────┬─────────────────╮
│  0 │ 158.94.254.14   │
│  1 │ 174.120.107.34  │
│  2 │ 192.168.1.155   │
│  3 │ 192.168.1.157   │
│  4 │ 192.168.1.236   │
│  5 │ 192.168.1.238   │
│  6 │ 192.168.1.239   │
│  7 │ 192.168.1.242   │
│  8 │ 192.168.1.243   │
│  9 │ 192.168.1.245   │
│ 10 │ 192.168.1.247   │
│ 11 │ 192.168.1.255   │
│ 12 │ 192.168.1.36    │
│ 13 │ 192.168.1.52    │
│ 14 │ 192.168.1.71    │
│ 15 │ 192.168.1.9     │
│ 16 │ 192.168.1.91    │
│ 17 │ 192.168.5.1     │
│ 18 │ 194.217.242.248 │
│ 19 │ 194.70.52.3     │
│ 20 │ 195.11.207.193  │
│ 21 │ 200.51.43.5     │
│ 22 │ 212.135.6.130   │
│ 23 │ 212.135.6.254   │
│ 24 │ 212.158.206.210 │
│ 25 │ 217.12.11.64    │
│ 26 │ 224.0.0.251     │
│ 27 │ 255.255.255.255 │
│ 28 │ 75.147.234.41   │
│ 29 │ 81.91.102.6     │
│ 30 │ 84.92.1.15      │
│ 31 │ 88.208.245.29   │
│ 32 │ 91.189.88.46    │
╰────┴─────────────────╯
~> |                                                                                22/05/2024 11:00:28
```

- Les ports touchés :

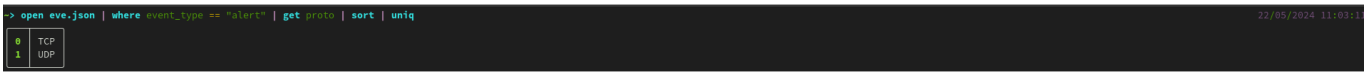
```
open eve.json | where event_type == "alert" | get dest_port | sort | uniq
```



```
~> open eve.json | where event_type == "alert" | get dest_port | sort | uniq        22/05/2024 11:00:28
╭────┬──────╮
│  0 │   25 │
│  1 │   53 │
│  2 │   68 │
│  3 │   80 │
│  4 │  138 │
│  5 │  139 │
│  6 │  445 │
│  7 │ 1025 │
│  8 │ 1027 │
│  9 │ 1028 │
│ 10 │ 1029 │
│ 11 │ 1030 │
│ 12 │ 1031 │
│ 13 │ 1038 │
│ 14 │ 1078 │
│ 15 │ 1088 │
│ 16 │ 1090 │
│ 17 │ 1092 │
│ 18 │ 1095 │
│ 19 │ 1099 │
│ 20 │ 1100 │
│ 21 │ 1102 │
│ 22 │ 1103 │
│ 23 │ 1107 │
│ 24 │ 1109 │
│ 25 │ 1112 │
│ 26 │ 1115 │
│ 27 │ 1116 │
│ 28 │ 1120 │
│ 29 │ 1123 │
│ 30 │ 1124 │
│ 31 │ 1127 │
│ 32 │ 1129 │
│ 33 │ 1130 │
│ 34 │ 1131 │
│ 35 │ 1132 │
│ 36 │ 1133 │
│ 37 │ 1134 │
│ 38 │ 1135 │
│ 39 │ 1136 │
│ 40 │ 1137 │
│ 41 │ 1139 │
│ 42 │ 1140 │
│ 43 │ 1141 │
│ 44 │ 1142 │
│ 45 │ 1143 │
│ 46 │ 1145 │
│ 47 │ 1146 │
│ 48 │ 1147 │
```

- Les protocoles utilisés :

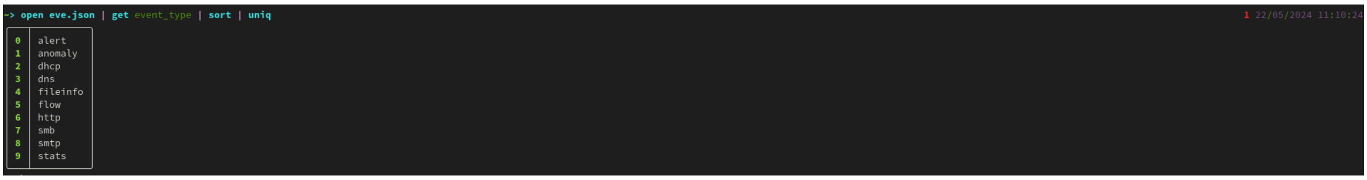
```
open eve.json | where event_type == "alert" | get proto | sort | uniq
```



```
~> open eve.json | where event_type == "alert" | get proto | sort | uniq          22/05/2024 11:03:1
 0 │ TCP
 1 │ UDP
```

- Les event_type :

```
open eve.json |get event_type | sort | uniq
```



```
~> open eve.json | get event_type | sort | uniq          1 22/05/2024 11:10:24
 0 │ alert
 1 │ anomaly
 2 │ dhcp
 3 │ dns
 4 │ fileinfo
 5 │ flow
 6 │ http
 7 │ smb
 8 │ smtp
 9 │ stats
```

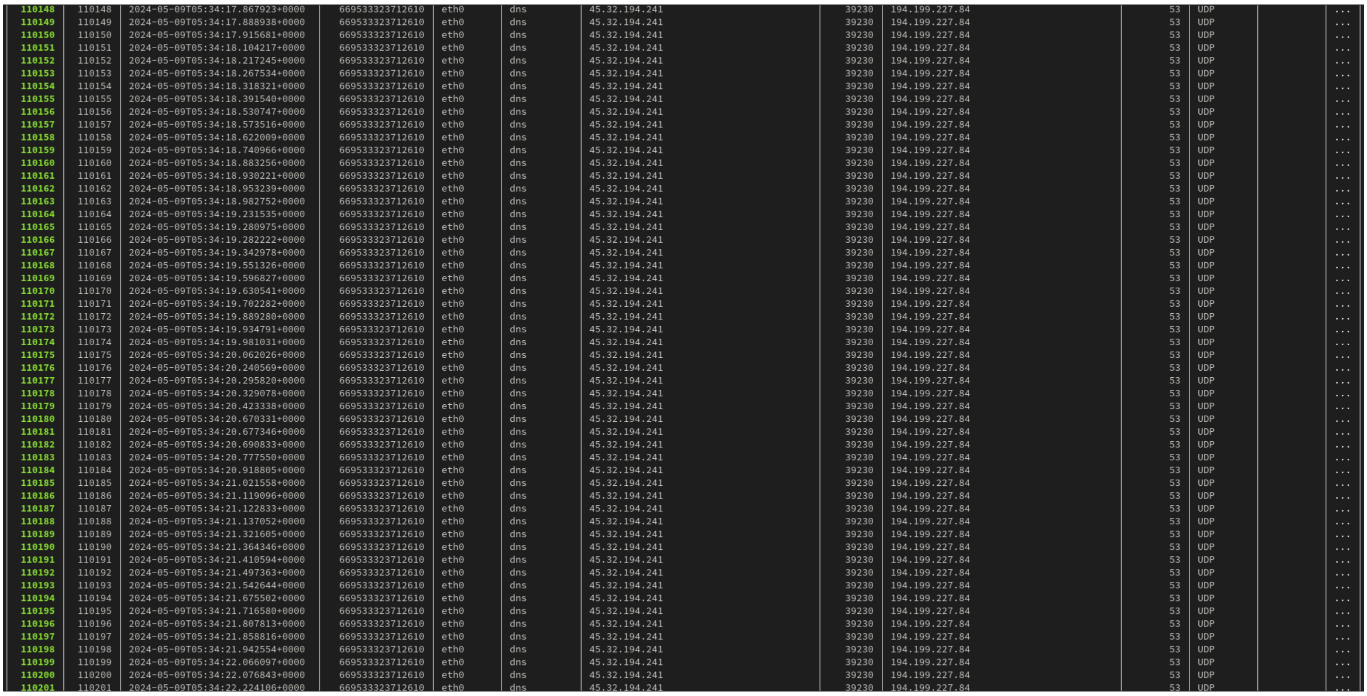
- Les severités des events alertes :

```
open eve.json | get alert.severity | sort | uniq
```

Analyse sur un autre fichier :

On va maintenant refaire l'analyse evetpot.json :

```
open evetpot.json
```



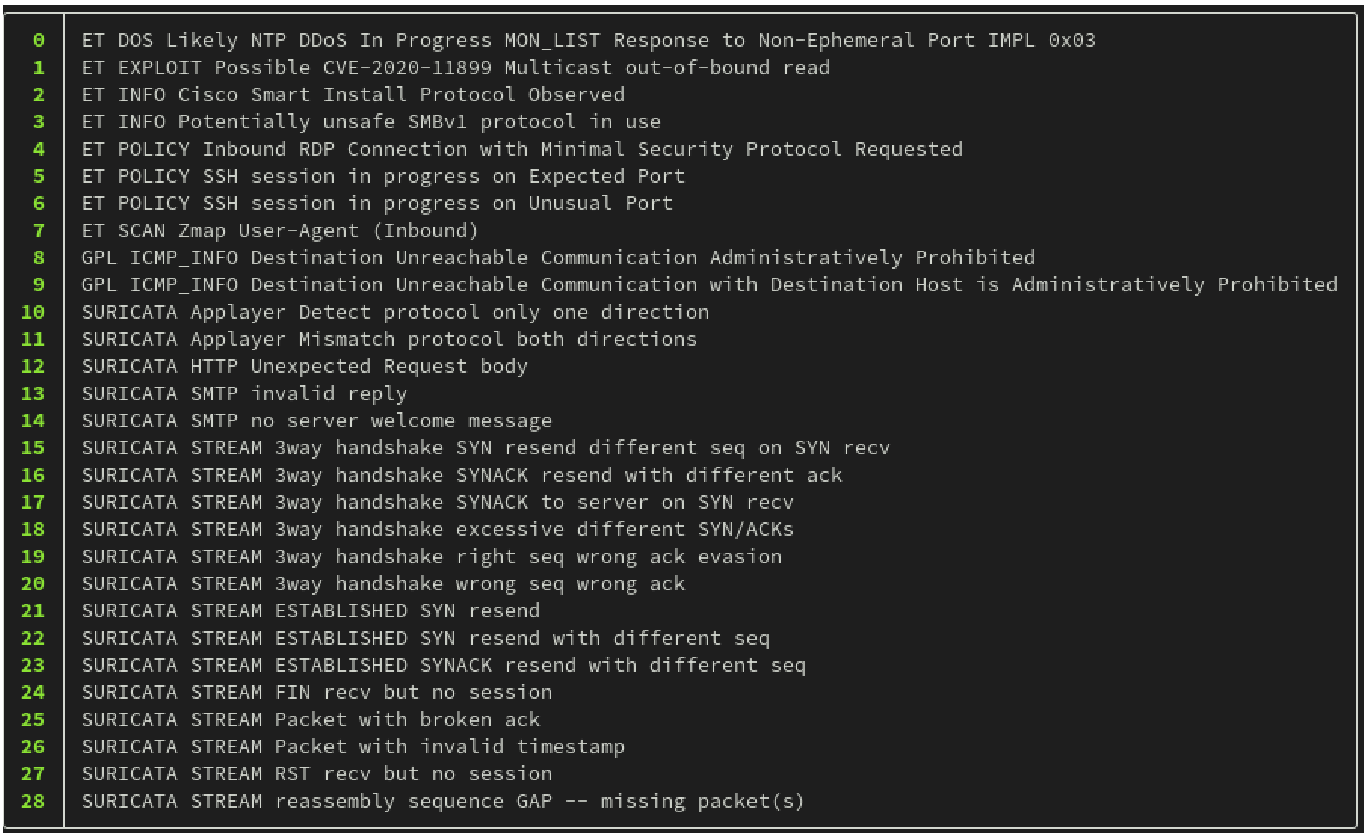
```
 110148 │ 110148 │ 2024-05-09T05:34:17.867923+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110149 │ 110149 │ 2024-05-09T05:34:17.888938+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110150 │ 110150 │ 2024-05-09T05:34:17.915681+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110151 │ 110151 │ 2024-05-09T05:34:18.104217+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110152 │ 110152 │ 2024-05-09T05:34:18.217245+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110153 │ 110153 │ 2024-05-09T05:34:18.267534+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110154 │ 110154 │ 2024-05-09T05:34:18.318321+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110155 │ 110155 │ 2024-05-09T05:34:18.391540+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110156 │ 110156 │ 2024-05-09T05:34:18.530747+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110157 │ 110157 │ 2024-05-09T05:34:18.573516+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110158 │ 110158 │ 2024-05-09T05:34:18.622009+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110159 │ 110159 │ 2024-05-09T05:34:18.740966+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110160 │ 110160 │ 2024-05-09T05:34:18.883256+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110161 │ 110161 │ 2024-05-09T05:34:18.930221+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110162 │ 110162 │ 2024-05-09T05:34:18.953239+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110163 │ 110163 │ 2024-05-09T05:34:18.982752+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110164 │ 110164 │ 2024-05-09T05:34:19.231535+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110165 │ 110165 │ 2024-05-09T05:34:19.280975+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110166 │ 110166 │ 2024-05-09T05:34:19.282222+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110167 │ 110167 │ 2024-05-09T05:34:19.342978+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110168 │ 110168 │ 2024-05-09T05:34:19.551326+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110169 │ 110169 │ 2024-05-09T05:34:19.596827+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110170 │ 110170 │ 2024-05-09T05:34:19.630541+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110171 │ 110171 │ 2024-05-09T05:34:19.702282+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110172 │ 110172 │ 2024-05-09T05:34:19.889280+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110173 │ 110173 │ 2024-05-09T05:34:19.934791+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110174 │ 110174 │ 2024-05-09T05:34:19.981031+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110175 │ 110175 │ 2024-05-09T05:34:20.062026+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110176 │ 110176 │ 2024-05-09T05:34:20.240569+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110177 │ 110177 │ 2024-05-09T05:34:20.295820+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110178 │ 110178 │ 2024-05-09T05:34:20.329078+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110179 │ 110179 │ 2024-05-09T05:34:20.423338+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110180 │ 110180 │ 2024-05-09T05:34:20.670331+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110181 │ 110181 │ 2024-05-09T05:34:20.677346+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110182 │ 110182 │ 2024-05-09T05:34:20.690833+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110183 │ 110183 │ 2024-05-09T05:34:20.777550+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110184 │ 110184 │ 2024-05-09T05:34:20.918805+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110185 │ 110185 │ 2024-05-09T05:34:21.021558+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110186 │ 110186 │ 2024-05-09T05:34:21.119096+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110187 │ 110187 │ 2024-05-09T05:34:21.122833+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110188 │ 110188 │ 2024-05-09T05:34:21.137052+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110189 │ 110189 │ 2024-05-09T05:34:21.321605+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110190 │ 110190 │ 2024-05-09T05:34:21.364346+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110191 │ 110191 │ 2024-05-09T05:34:21.410594+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110192 │ 110192 │ 2024-05-09T05:34:21.497363+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110193 │ 110193 │ 2024-05-09T05:34:21.542644+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110194 │ 110194 │ 2024-05-09T05:34:21.675502+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110195 │ 110195 │ 2024-05-09T05:34:21.716580+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110196 │ 110196 │ 2024-05-09T05:34:21.807813+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110197 │ 110197 │ 2024-05-09T05:34:21.858816+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110198 │ 110198 │ 2024-05-09T05:34:21.942554+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110199 │ 110199 │ 2024-05-09T05:34:22.066097+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110200 │ 110200 │ 2024-05-09T05:34:22.076843+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
 110201 │ 110201 │ 2024-05-09T05:34:22.224106+0000 │ 669533323712610 │ eth0 │ dns │ 45.32.194.241 │ 39230 │ 194.199.227.84 │ 53 │ UDP │ │ ...
```

On va maintenant faire une analyse sur les alertes suricata :

```
open evetpot.json | where event_type == "alert"
```

On liste les alertes suricata :

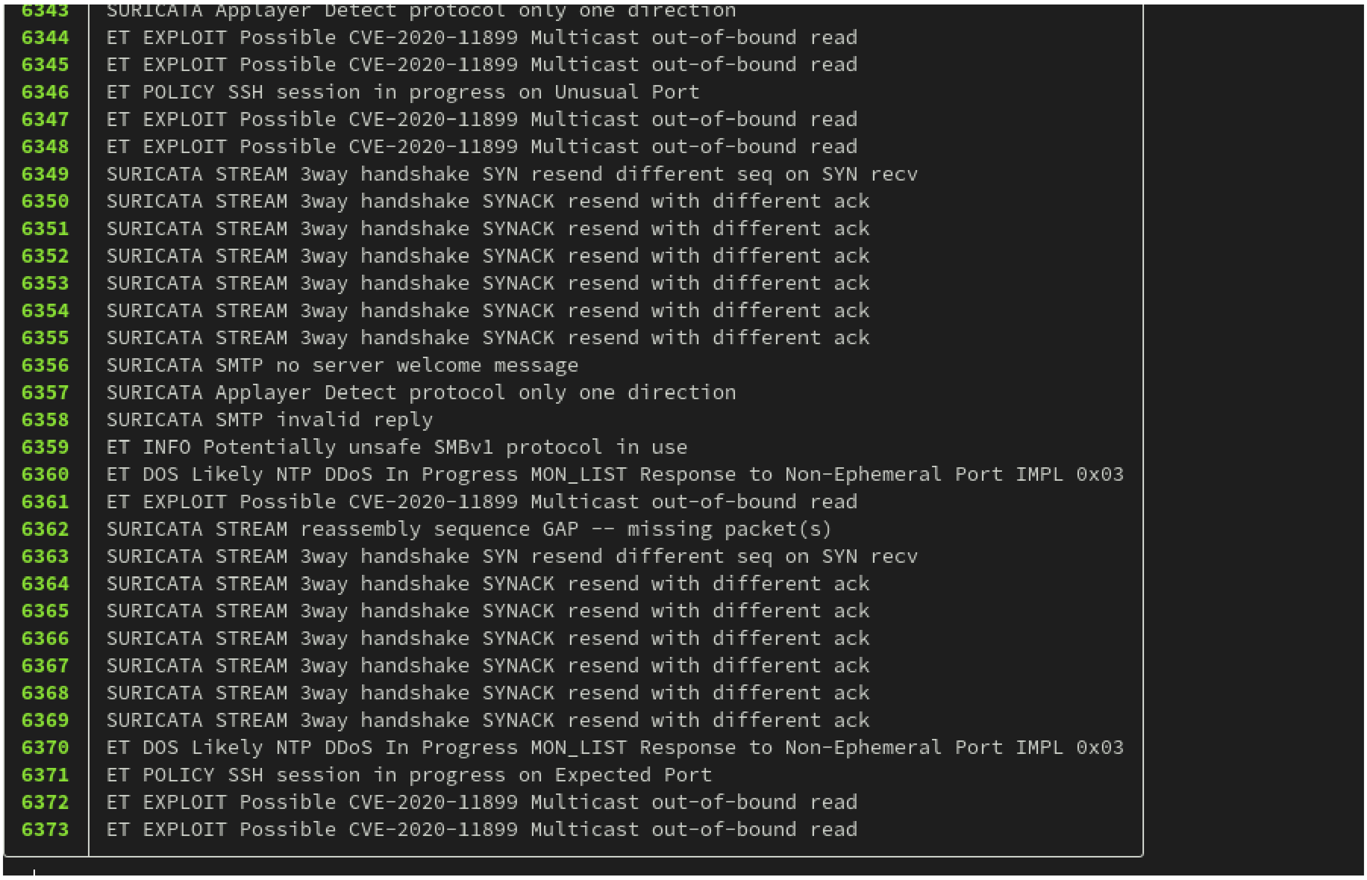
```
open tpot.json | flatten | where "event_type" == "alert" |get
"alert.signature" | sort | uniq
```



```
 0 │ ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x03
 1 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
 2 │ ET INFO Cisco Smart Install Protocol Observed
 3 │ ET INFO Potentially unsafe SMBv1 protocol in use
 4 │ ET POLICY Inbound RDP Connection with Minimal Security Protocol Requested
 5 │ ET POLICY SSH session in progress on Expected Port
 6 │ ET POLICY SSH session in progress on Unusual Port
 7 │ ET SCAN Zmap User-Agent (Inbound)
 8 │ GPL ICMP_INFO Destination Unreachable Communication Administratively Prohibited
 9 │ GPL ICMP_INFO Destination Unreachable Communication with Destination Host is Administratively Prohibited
10 │ SURICATA Applayer Detect protocol only one direction
11 │ SURICATA Applayer Mismatch protocol both directions
12 │ SURICATA HTTP Unexpected Request body
13 │ SURICATA SMTP invalid reply
14 │ SURICATA SMTP no server welcome message
15 │ SURICATA STREAM 3way handshake SYN resend different seq on SYN recv
16 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
17 │ SURICATA STREAM 3way handshake SYNACK to server on SYN recv
18 │ SURICATA STREAM 3way handshake excessive different SYN/ACKs
19 │ SURICATA STREAM 3way handshake right seq wrong ack evasion
20 │ SURICATA STREAM 3way handshake wrong seq wrong ack
21 │ SURICATA STREAM ESTABLISHED SYN resend
22 │ SURICATA STREAM ESTABLISHED SYN resend with different seq
23 │ SURICATA STREAM ESTABLISHED SYNACK resend with different seq
24 │ SURICATA STREAM FIN recv but no session
25 │ SURICATA STREAM Packet with broken ack
26 │ SURICATA STREAM Packet with invalid timestamp
27 │ SURICATA STREAM RST recv but no session
28 │ SURICATA STREAM reassembly sequence GAP -- missing packet(s)
```

Puis on fait une analyse sur tout les events alertes :

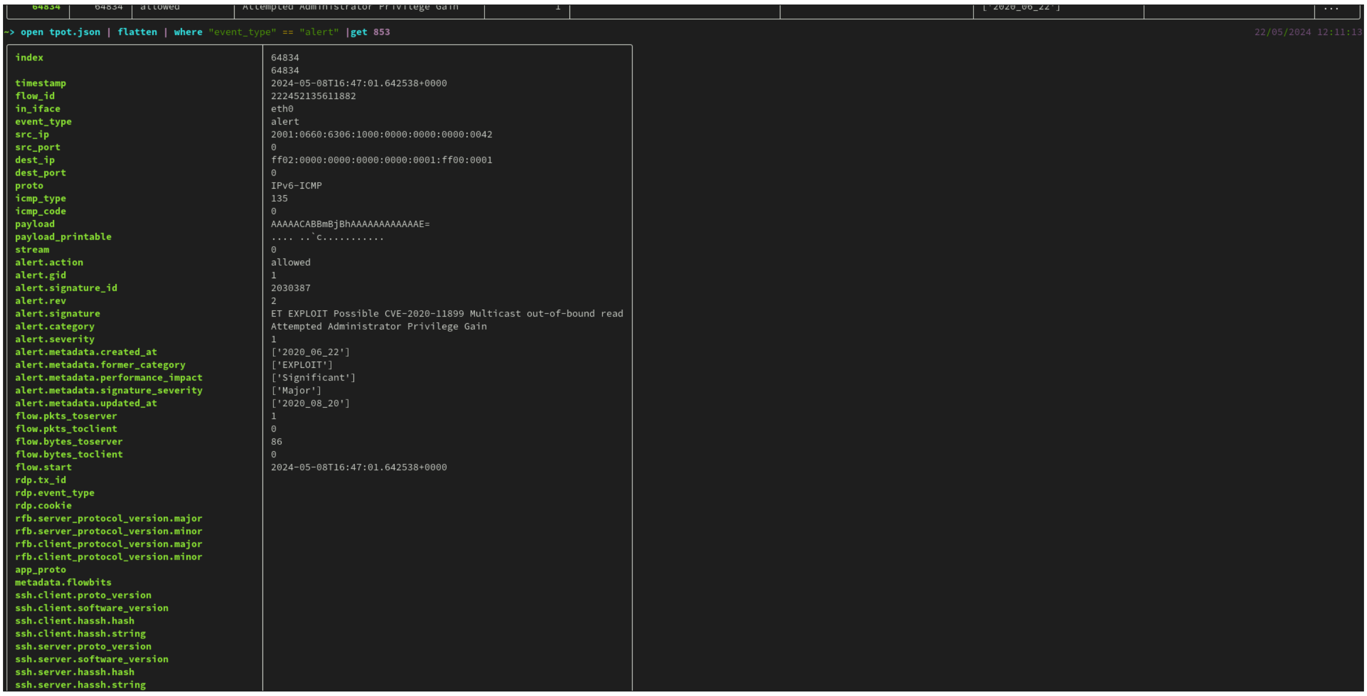
```
open evetpot.json | where "event_type" == "alert" | get "alert.signature"
```



```
6343 │ SURICATA Applayer Detect protocol only one direction
6344 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
6345 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
6346 │ ET POLICY SSH session in progress on Unusual Port
6347 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
6348 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
6349 │ SURICATA STREAM 3way handshake SYN resend different seq on SYN recv
6350 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6351 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6352 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6353 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6354 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6355 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6356 │ SURICATA SMTP no server welcome message
6357 │ SURICATA Applayer Detect protocol only one direction
6358 │ SURICATA SMTP invalid reply
6359 │ ET INFO Potentially unsafe SMBv1 protocol in use
6360 │ ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x03
6361 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
6362 │ SURICATA STREAM reassembly sequence GAP -- missing packet(s)
6363 │ SURICATA STREAM 3way handshake SYN resend different seq on SYN recv
6364 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6365 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6366 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6367 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6368 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6369 │ SURICATA STREAM 3way handshake SYNACK resend with different ack
6370 │ ET DOS Likely NTP DDoS In Progress MON_LIST Response to Non-Ephemeral Port IMPL 0x03
6371 │ ET POLICY SSH session in progress on Expected Port
6372 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
6373 │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
```

puis on analyse un event en particulier :

```
open evetpot.json | where event_type == "alert" | get 853
```



```
  64834 │ 64834 │ allowed │ Attempted Administrator Privilege Gain │ 1 │ │ ['2020_06_22'] │ │ ...
~> open tpot.json | flatten | where "event_type" == "alert" |get 853                    22/05/2024 12:11:13
 index                                    │ 64834
                                          │ 64834
 timestamp                                │ 2024-05-08T16:47:01.642538+0000
 flow_id                                  │ 222452135611882
 in_iface                                 │ eth0
 event_type                               │ alert
 src_ip                                   │ 2001:0660:6306:1000:0000:0000:0000:0042
 src_port                                 │ 0
 dest_ip                                  │ ff02:0000:0000:0000:0000:0001:ff00:0001
 dest_port                                │ 0
 proto                                    │ IPv6-ICMP
 icmp_type                                │ 135
 icmp_code                                │ 0
 payload                                  │ AAAAACABBmBjBhAAAAAAAAAAAAE=
 payload_printable                        │ .... ..`c...........
 stream                                   │ 0
 alert.action                             │ allowed
 alert.gid                                │ 1
 alert.signature_id                       │ 2030387
 alert.rev                                │ 2
 alert.signature                          │ ET EXPLOIT Possible CVE-2020-11899 Multicast out-of-bound read
 alert.category                           │ Attempted Administrator Privilege Gain
 alert.severity                           │ 1
 alert.metadata.created_at                │ ['2020_06_22']
 alert.metadata.former_category           │ ['EXPLOIT']
 alert.metadata.performance_impact        │ ['Significant']
 alert.metadata.signature_severity        │ ['Major']
 alert.metadata.updated_at                │ ['2020_08_20']
 flow.pkts_toserver                       │ 1
 flow.pkts_toclient                       │ 0
 flow.bytes_toserver                      │ 86
 flow.bytes_toclient                      │ 0
 flow.start                               │ 2024-05-08T16:47:01.642538+0000
 rdp.tx_id                                │
 rdp.event_type                           │
 rdp.cookie                               │
 rfb.server_protocol_version.major        │
 rfb.server_protocol_version.minor        │
 rfb.client_protocol_version.major        │
 rfb.client_protocol_version.minor        │
 app_proto                                │
 metadata.flowbits                        │
 ssh.client.proto_version                 │
 ssh.client.software_version              │
 ssh.client.hassh.hash                    │
 ssh.client.hassh.string                  │
 ssh.server.proto_version                 │
 ssh.server.software_version              │
 ssh.server.hassh.hash                    │
 ssh.server.hassh.string                  │
```