Jason Hodge

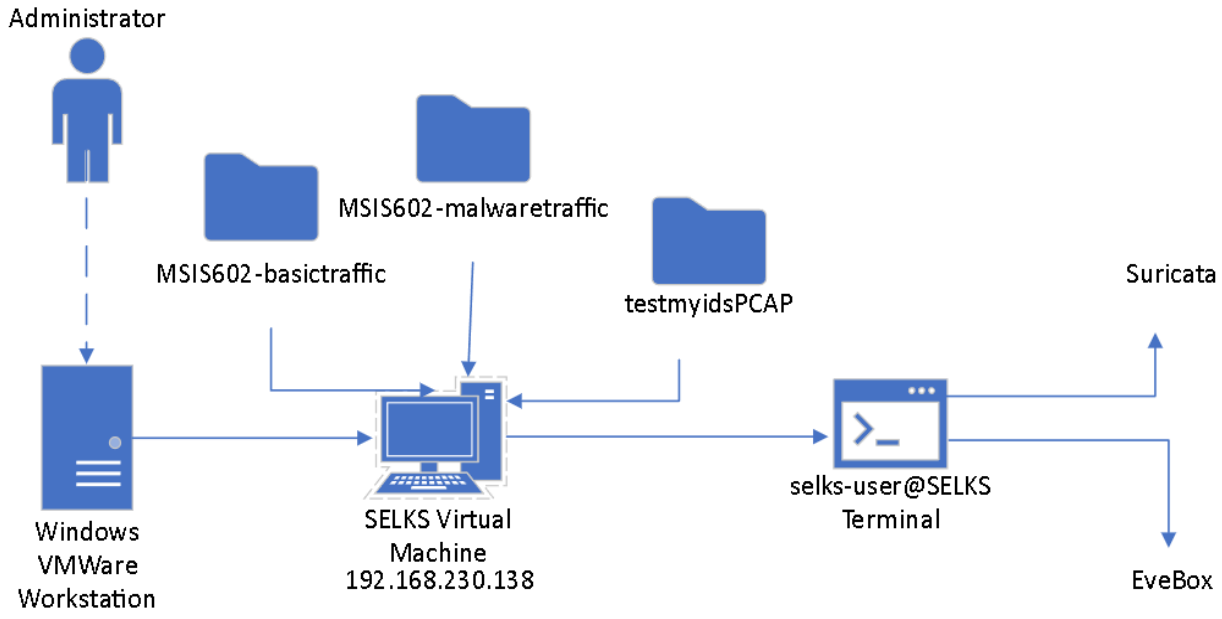
Option 6: SELKS Implementation

December 10, 2023

Description:

In the first part of this lab, I downloaded the SELKS virtual machine (VM) latest version 7 on my VMware Workstation Pro. Then I downloaded a few sample pcap files for both the basic traffic and the malware traffic and put them in their respective folders labeled “MSIS602-basictraffic” and “MSIS602-malwaretraffic”. With all these files I had to ingest the sample pcap files and then open and run them in Evebox. In order to do this, we had to first setup the proper environment by making some changes to the Suricata Yaml file. The primary change was to the rule-set. Once this part was done, I could then ingest the files and analyze the Evebox.json file contents in both folders. I then did the same with the pcap file “testmyids”. With this information I was able to breakdown the contents of these files to their specific log data of the pcap issues.

Topology:



This is an overview of the entire lab’s connections including the tools and resources used.

Key Syntax:

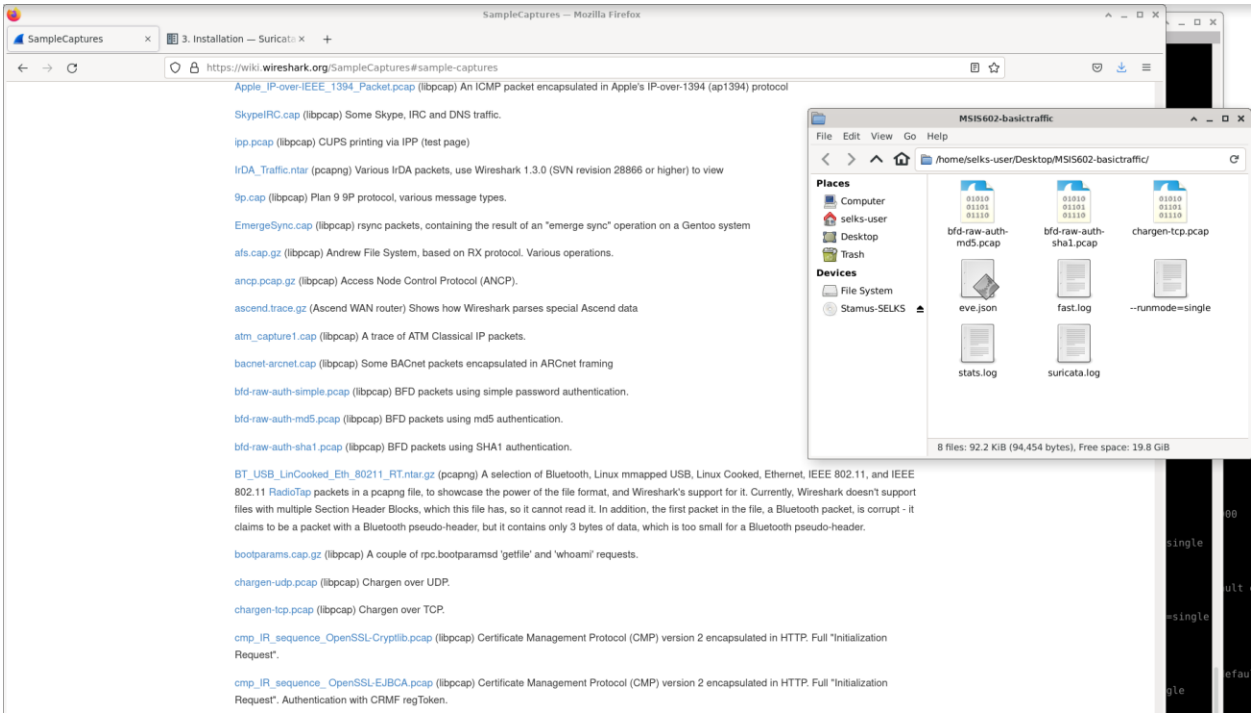
- Esc Key + ":w" Enter Key to Save a Yaml File
- Esc Key + ":x" Enter Key to Quit a Yaml File
- Esc Key "i" to edit a Yaml File
- EveBox timeframe needs to be changed to "All" or some date in the past to view events.

Verification:

TASK ONE: SELKS Initial Setup

Here we see the SELKS virtual machine up and running to serve as both our Network Intrusion Detection System (NIDS) and Network Security Monitor (NSM) system.

TASK TWO: Generate Traffic within SELKS

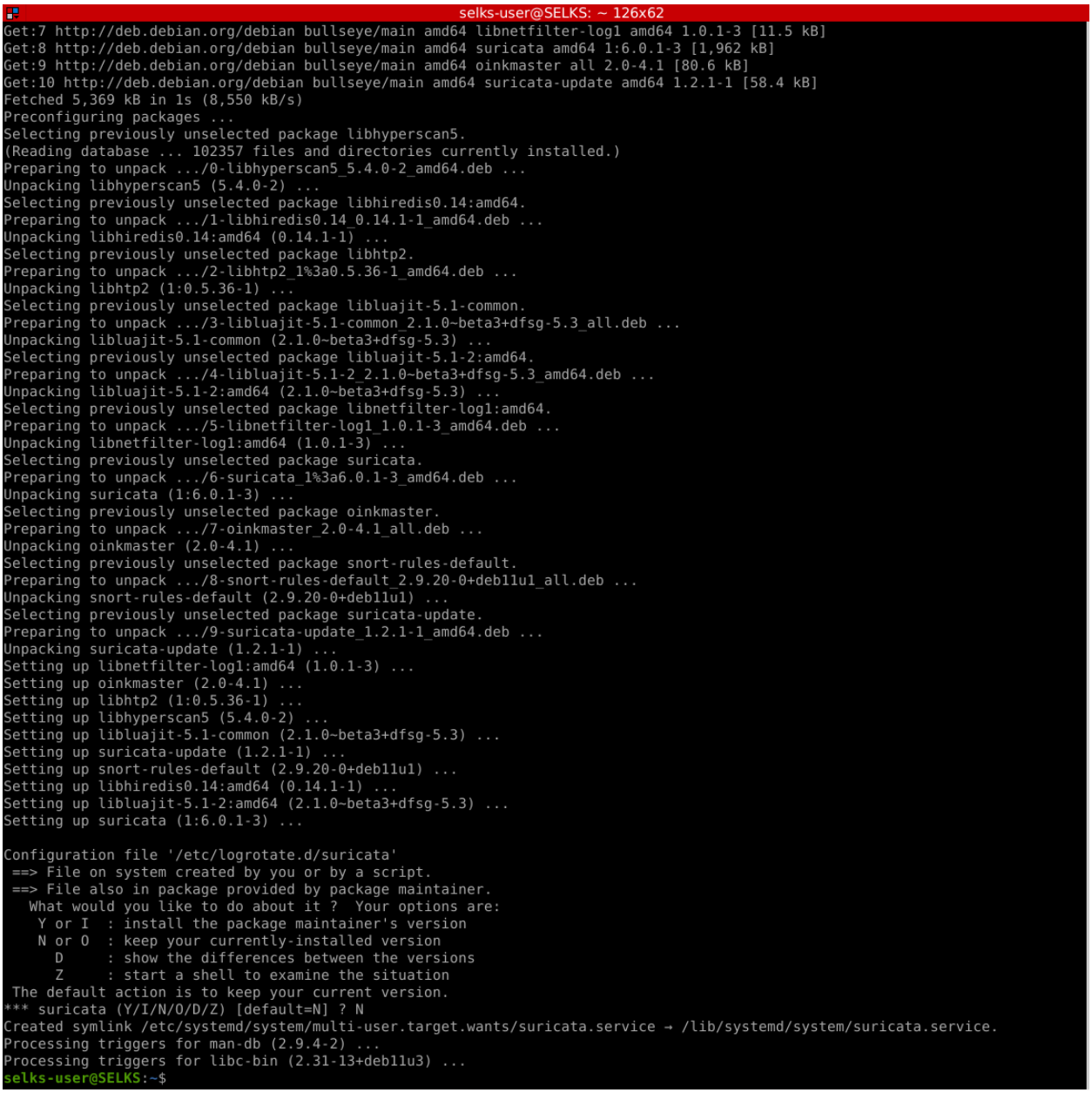


Here we can see the sample Wireshark captures (pcaps) chosen and downloaded to the "MSIS602-basictraffic" folder.

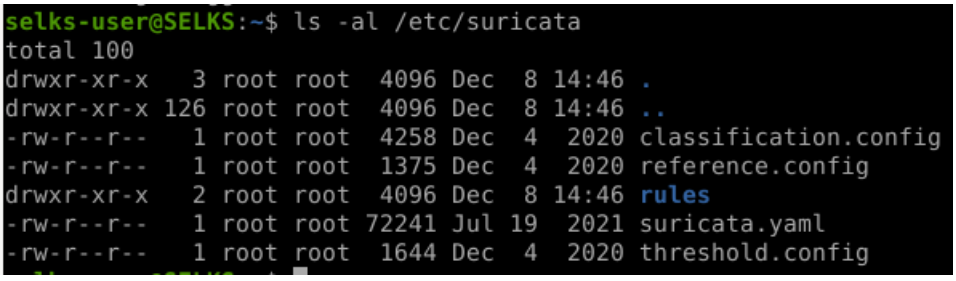
```
selks-user@SELKS: ~ 126x62
selks-user@SELKS:~$ sudo apt-get install software-properties-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python-apt-common python3-apt python3-distro-info python3-pycurl python3-software-properties unattended-upgrades
Suggested packages:
  python3-apt-dbg python-apt-doc libcurl4-gnutls-dev python-pycurl-doc python3-pycurl-dbg bsd-mailx default-mta
  | mail-transport-agent needrestart powermgmt-base
The following NEW packages will be installed:
  python-apt-common python3-apt python3-distro-info python3-pycurl python3-software-properties software-properties-common
  unattended-upgrades
0 upgraded, 7 newly installed, 0 to remove and 252 not upgraded.
Need to get 586 kB of archives.
After this operation, 2,449 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 python-apt-common all 2.2.1 [96.5 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 python3-apt amd64 2.2.1 [190 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 python3-distro-info all 1.0 [8,720 B]
Get:4 http://deb.debian.org/debian bullseye/main amd64 python3-pycurl amd64 7.43.0.6-5 [68.8 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 python3-software-properties all 0.96.20.2-2.1 [49.7 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 software-properties-common all 0.96.20.2-2.1 [83.4 kB]
Get:7 http://deb.debian.org/debian bullseye/main amd64 unattended-upgrades all 2.8 [88.6 kB]
Fetched 586 kB in 0s (3,667 kB/s)
Preconfiguring packages ...
Selecting previously unselected package python-apt-common.
(Reading database ... 102090 files and directories currently installed.)
Preparing to unpack .../0-python-apt-common_2.2.1_all.deb ...
Unpacking python-apt-common (2.2.1) ...
Selecting previously unselected package python3-apt.
Preparing to unpack .../1-python3-apt_2.2.1_amd64.deb ...
Unpacking python3-apt (2.2.1) ...
Selecting previously unselected package python3-distro-info.
Preparing to unpack .../2-python3-distro-info_1.0_all.deb ...
Unpacking python3-distro-info (1.0) ...
Selecting previously unselected package python3-pycurl.
Preparing to unpack .../3-python3-pycurl_7.43.0.6-5_amd64.deb ...
Unpacking python3-pycurl (7.43.0.6-5) ...
Selecting previously unselected package python3-software-properties.
Preparing to unpack .../4-python3-software-properties_0.96.20.2-2.1_all.deb ...
Unpacking python3-software-properties (0.96.20.2-2.1) ...
Selecting previously unselected package software-properties-common.
Preparing to unpack .../5-software-properties-common_0.96.20.2-2.1_all.deb ...
Unpacking software-properties-common (0.96.20.2-2.1) ...
Selecting previously unselected package unattended-upgrades.
Preparing to unpack .../6-unattended-upgrades_2.8_all.deb ...
Unpacking unattended-upgrades (2.8) ...
Setting up python3-pycurl (7.43.0.6-5) ...
Setting up python-apt-common (2.2.1) ...
Setting up python3-distro-info (1.0) ...
Setting up python3-apt (2.2.1) ...
Setting up unattended-upgrades (2.8) ...

Creating config file /etc/apt/apt.conf.d/20auto-upgrades with new version

Creating config file /etc/apt/apt.conf.d/50unattended-upgrades with new version
Created symlink /etc/systemd/system/multi-user.target.wants/unattended-upgrades.service → /lib/systemd/system/unattended-upgra
des.service.
Synchronizing state of unattended-upgrades.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable unattended-upgrades
Setting up python3-software-properties (0.96.20.2-2.1) ...
Setting up software-properties-common (0.96.20.2-2.1) ...
```

Next, I had to make sure all the required software properties versions were available and up to date.

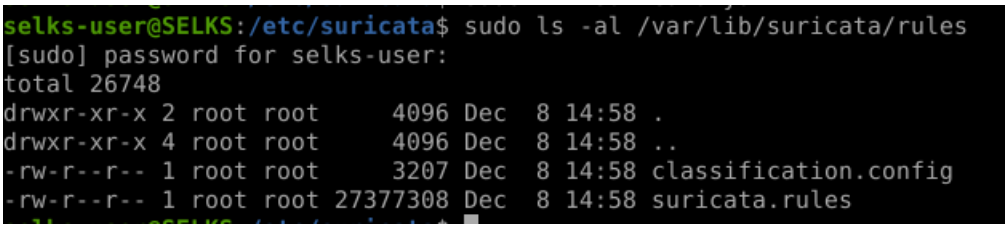
```
Creating config file /etc/apt/apt.conf.d/20auto-upgrades with new version

Creating config file /etc/apt/apt.conf.d/50unattended-upgrades with new version
Created symlink /etc/systemd/system/multi-user.target.wants/unattended-upgrades.service → /lib/systemd/system/unattended-upgra
des.service.
Synchronizing state of unattended-upgrades.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable unattended-upgrades
Setting up python3-software-properties (0.96.20.2-2.1) ...
Setting up software-properties-common (0.96.20.2-2.1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for dbus (1.12.20-2) ...
selks-user@SELKS:~$ sudo apt-get update && sudo apt-get install suricata -y
```



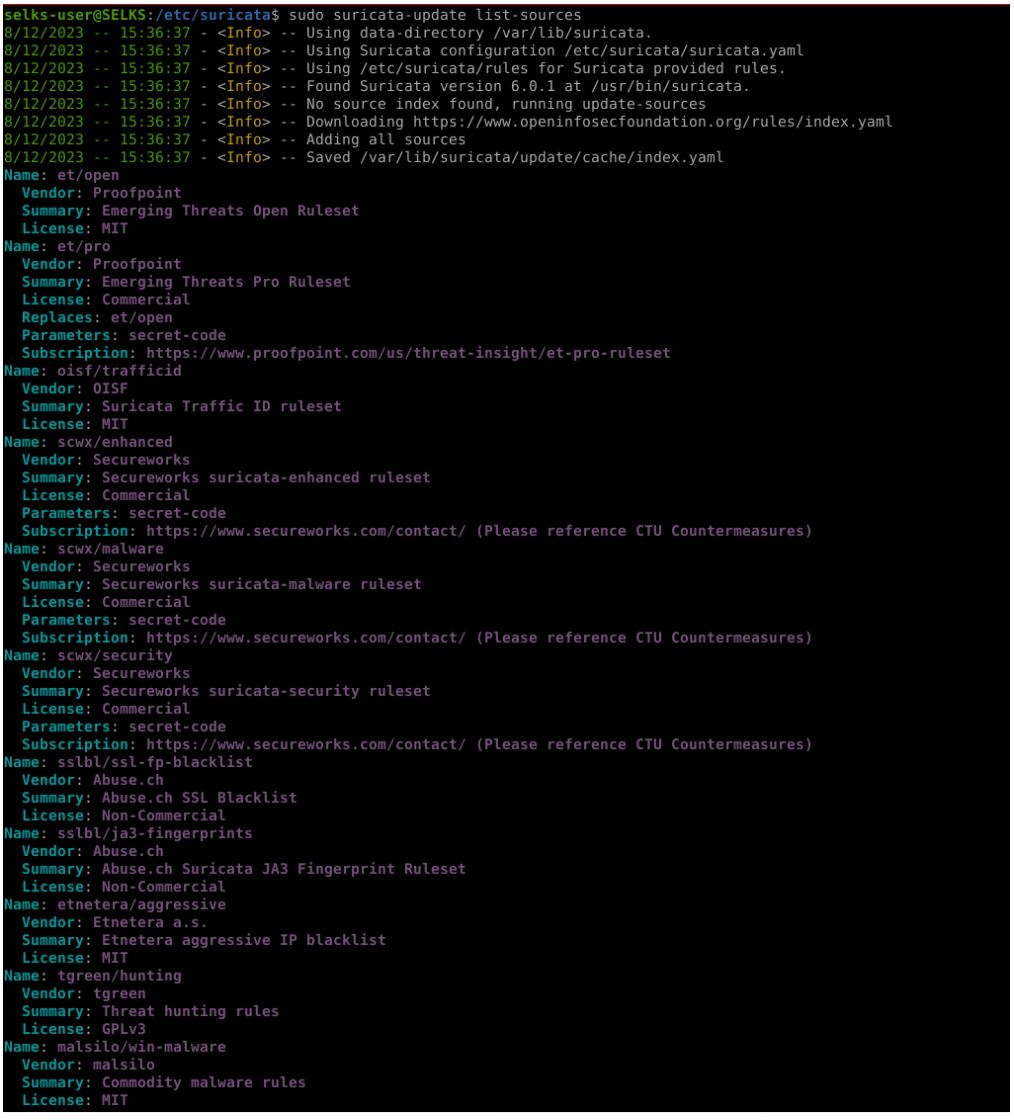
Then I updated the repositories and installed Suricata with the “-y” option to install directly. This machine already has Suricata predownloaded, so no change took place with that part.



This command lists out the contents of the /etc/suricata folder directory. We can see there is a rules folder present.



Next, I listed out the rules and saw that the suricata.rules directory is present. This contains all the rules.



```
Name: malsilo/win-malware
  Vendor: malsilo
  Summary: Commodity malware rules
  License: MIT
Name: stamus/lateral
  Vendor: Stamus Networks
  Summary: Lateral movement rules
  License: GPL-3.0-only
selks-user@SELKS:/etc/suricata$
```

Next, I listed out the sources I can retrieve rule sets from. I used one with an MIT license, but an open sourced licensed source would have worked as well.

```
selks-user@SELKS:/etc/suricata$ sudo suricata-update enable-source malsilo/win-malware
8/12/2023 -- 15:40:30 - <Info> -- Using data-directory /var/lib/suricata.
8/12/2023 -- 15:40:30 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
8/12/2023 -- 15:40:30 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
8/12/2023 -- 15:40:30 - <Info> -- Found Suricata version 6.0.1 at /usr/bin/suricata.
8/12/2023 -- 15:40:30 - <Info> -- Creating directory /var/lib/suricata/update/sources
8/12/2023 -- 15:40:30 - <Info> -- Enabling default source et/open
8/12/2023 -- 15:40:30 - <Info> -- Source malsilo/win-malware enabled
```

Here, I enabled the source “malsilo/win-malware” by specifying it and updating the sources.

```
selks-user@SELKS:/etc/suricata$ sudo suricata-update
8/12/2023 -- 15:42:04 - <Info> -- Using data-directory /var/lib/suricata.
8/12/2023 -- 15:42:04 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
8/12/2023 -- 15:42:04 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
8/12/2023 -- 15:42:04 - <Info> -- Found Suricata version 6.0.1 at /usr/bin/suricata.
8/12/2023 -- 15:42:04 - <Info> -- Loading /etc/suricata/suricata.yaml
8/12/2023 -- 15:42:04 - <Info> -- Disabling rules for protocol http2
8/12/2023 -- 15:42:04 - <Info> -- Disabling rules for protocol modbus
8/12/2023 -- 15:42:04 - <Info> -- Disabling rules for protocol dnp3
8/12/2023 -- 15:42:04 - <Info> -- Disabling rules for protocol enip
8/12/2023 -- 15:42:04 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-6.0.1/emerging.rules.tar.gz.md5.
8/12/2023 -- 15:42:04 - <Info> -- Remote checksum has not changed. Not fetching.
8/12/2023 -- 15:42:04 - <Info> -- Fetching https://malsilo.gitlab.io/feeds/dumps/malsilo.rules.tar.gz.
 100% - 1089/1089
8/12/2023 -- 15:42:05 - <Info> -- Done.
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
8/12/2023 -- 15:42:05 - <Info> -- Ignoring file rules/emerging-deleted.rules
8/12/2023 -- 15:42:06 - <Info> -- Loaded 46241 rules.
8/12/2023 -- 15:42:07 - <Info> -- Disabled 14 rules.
8/12/2023 -- 15:42:07 - <Info> -- Enabled 0 rules.
8/12/2023 -- 15:42:07 - <Info> -- Modified 0 rules.
8/12/2023 -- 15:42:07 - <Info> -- Dropped 0 rules.
8/12/2023 -- 15:42:07 - <Info> -- Enabled 131 rules for flowbit dependencies.
8/12/2023 -- 15:42:07 - <Info> -- Backing up current rules.
8/12/2023 -- 15:42:09 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 46241; enabled: 35937; added
: 14; removed 0; modified: 0
8/12/2023 -- 15:42:10 - <Info> -- Writing /var/lib/suricata/rules/classification.config
8/12/2023 -- 15:42:10 - <Info> -- Testing with suricata -T.
```

I then updated Suricata to ensure I was using the latest.

```
selks-user@SELKS:~$ sudo systemctl stop suricata
```

Here we are stopping the Suricata to make some changes. We can also use “start” to start the service again. We do not want to monitor the current network traffic so this needs to be turned off.

```
selks-user@SELKS: ~
selks-user@SELKS: ~ 109x37
selks-user@SELKS:~$ sudo ifconfig
[sudo] password for selks-user:
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:29:b5:13:3a  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.230.138  netmask 255.255.255.0  broadcast 192.168.230.255
        inet6 fe80::20c:29ff:fe58:e812  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:58:e8:12  txqueuelen 1000  (Ethernet)
        RX packets 2208  bytes 515591 (503.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1946  bytes 210259 (205.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 2044 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 2044 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Then, using the “sudo ifconfig” command I got the ip address information for the machine so I can set the proper variable for HOME_NET subnet address and the interface in the Yaml file. In order to bring up the yaml file I used the command “sudo vim /etc/suricata/suricata.yaml”

```
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.230.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
    FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
    FTP_PORTS: 21
    GENEVE_PORTS: 6081
    VXLAN_PORTS: 4789
    TEREDO_PORTS: 3544
```

Here we can see the subnet address “192.168.230.0/24”, value I set for HOME_NET.

```
##
## Step 3: Configure common capture settings
##
## See "Advanced Capture Options" below for more options, including Netmap
## and PF_RING.
##

# Linux high speed capture support
af-packet:
  - interface: ens33
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
```

Down further in the document I set the interface values for both the Linux high speed capture support and the cross platform libpcap capture support to the proper interface “ens33”.

```
    # Community Flow ID
    # Adds a 'community_id' field to EVE records. These are meant to give
    # records a predictable flow ID that can be used to match records to
    # output of other tools such as Zeek (Bro).
    #
    # Takes a 'seed' that needs to be same across sensors and tools
    # to make the id less predictable.

    # enable/disable the community id feature.
    community-id: true
    # Seed value for the ID output. Valid values are 0-65535.
    community-id-seed: 0
```

Here I enabled the community-id feature value for EVE by changing the value from false to true.

```
##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /etc/suricata/rules

rule-files:
  - /var/lib/suricata/rules/suricata.rules/
```

Lastly, I updated the rule-files by adding the proper ruleset directory path in order to successfully ingest pcap files using Suricata. I then wrote these changes and exited the Yaml document using the “:w” and “:x” commands.

```
selks-user@SELKS:~$ sudo suricata-update
[sudo] password for selks-user:
8/12/2023 -- 18:13:45 - <Info> -- Using data-directory /var/lib/suricata.
8/12/2023 -- 18:13:45 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
8/12/2023 -- 18:13:45 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
8/12/2023 -- 18:13:45 - <Info> -- Found Suricata version 6.0.1 at /usr/bin/suricata.
8/12/2023 -- 18:13:45 - <Info> -- Loading /etc/suricata/suricata.yaml
8/12/2023 -- 18:13:45 - <Info> -- Disabling rules for protocol http2
8/12/2023 -- 18:13:45 - <Info> -- Disabling rules for protocol modbus
8/12/2023 -- 18:13:45 - <Info> -- Disabling rules for protocol dnp3
8/12/2023 -- 18:13:45 - <Info> -- Disabling rules for protocol enip
8/12/2023 -- 18:13:45 - <Info> -- Checking https://malsilo.gitlab.io/feeds/dumps/malsilo.rules.tar.gz.md5.
8/12/2023 -- 18:13:46 - <Info> -- Remote checksum has not changed. Not fetching.
8/12/2023 -- 18:13:46 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-6.0.1/emerging.rules.tar.gz.md5.
8/12/2023 -- 18:13:46 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-6.0.1/emerging.rules.tar.gz.
 100% - 4157294/4157294
8/12/2023 -- 18:13:46 - <Info> -- Done.
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
8/12/2023 -- 18:13:46 - <Info> -- Ignoring file rules/emerging-deleted.rules
8/12/2023 -- 18:13:49 - <Info> -- Loaded 46237 rules.
8/12/2023 -- 18:13:49 - <Info> -- Disabled 14 rules.
8/12/2023 -- 18:13:49 - <Info> -- Enabled 0 rules.
8/12/2023 -- 18:13:49 - <Info> -- Modified 0 rules.
8/12/2023 -- 18:13:49 - <Info> -- Dropped 0 rules.
8/12/2023 -- 18:13:49 - <Info> -- Enabled 131 rules for flowbit dependencies.
8/12/2023 -- 18:13:49 - <Info> -- Backing up current rules.
8/12/2023 -- 18:13:52 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 46237; enabled: 35929; added: 7; removed 11; m
odified: 1202
8/12/2023 -- 18:13:52 - <Info> -- Writing /var/lib/suricata/rules/classification.config
8/12/2023 -- 18:13:52 - <Info> -- Testing with suricata -T.
8/12/2023 -- 18:14:32 - <Info> -- Done.
```

Next, I updated Suricata again with the changes made to the Yaml file.

```
selks-user@SELKS:~$ sudo systemctl status suricata.service
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
     Active: failed (Result: exit-code) since Fri 2023-12-08 15:48:56 EST; 2h 30min ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata-ids.org/docs/
    Main PID: 1003 (code=exited, status=1/FAILURE)
         CPU: 68ms

Dec 08 15:48:56 SELKS systemd[1]: suricata.service: Main process exited, code=exited, status=1/FAILURE
Dec 08 15:48:56 SELKS systemd[1]: suricata.service: Failed with result 'exit-code'.
Dec 08 15:48:56 SELKS systemd[1]: suricata.service: Scheduled restart job, restart counter is at 5.
Dec 08 15:48:56 SELKS systemd[1]: Stopped Suricata IDS/IDP daemon.
Dec 08 15:48:56 SELKS systemd[1]: suricata.service: Start request repeated too quickly.
Dec 08 15:48:56 SELKS systemd[1]: suricata.service: Failed with result 'exit-code'.
Dec 08 15:48:56 SELKS systemd[1]: Failed to start Suricata IDS/IDP daemon.
```

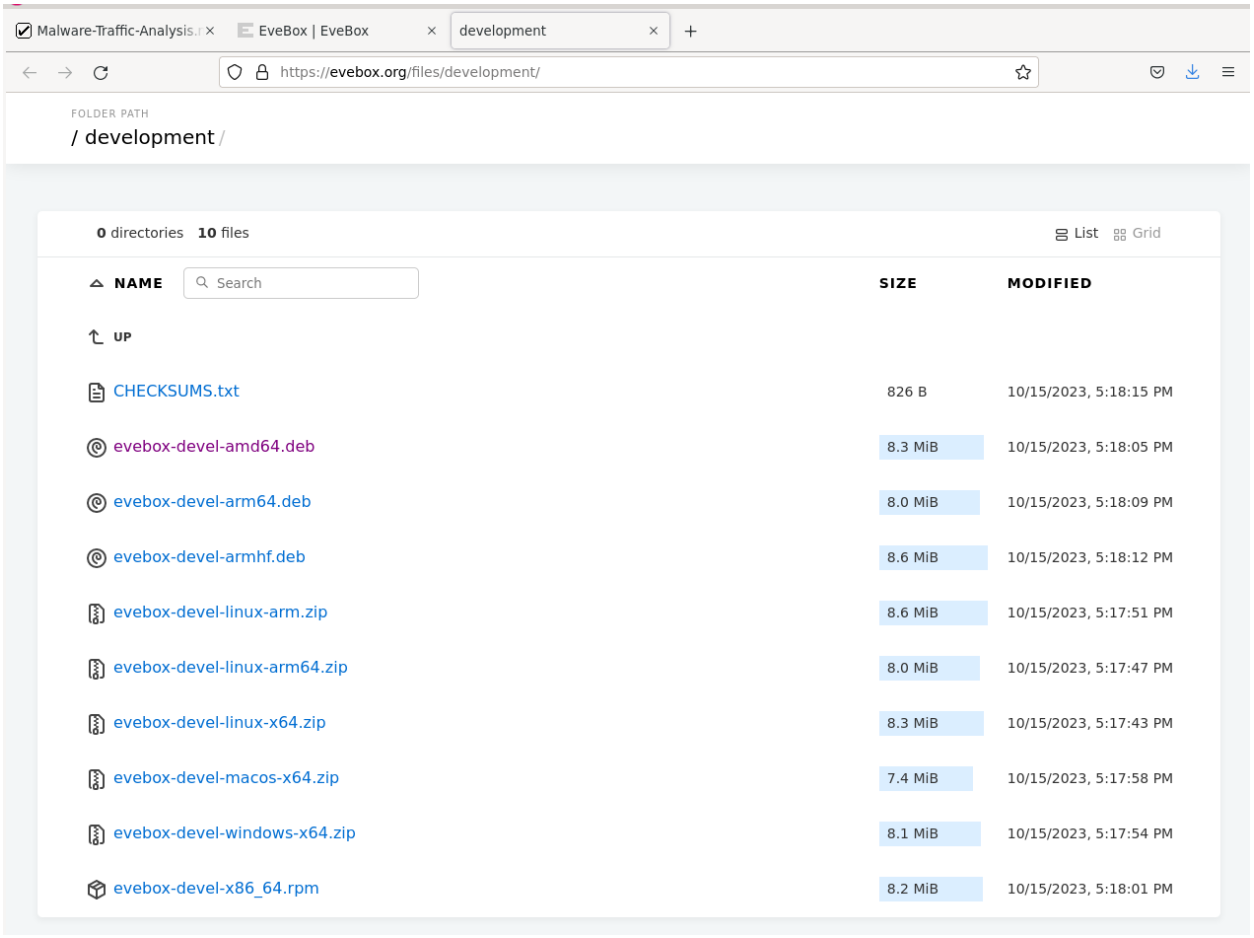
Then, I checked that the status of the suricata service is disabled.

```
selks-user@SELKS:~/Desktop/MSIS602-basictraffic$ sudo suricata -c /etc/suricata/suricata.yaml -k none -r bfd-raw-auth-md5.pcap --runmode=single
8/12/2023 -- 18:55:54 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
8/12/2023 -- 18:56:30 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
8/12/2023 -- 18:56:30 - <Notice> - Signal Received.  Stopping engine.
8/12/2023 -- 18:56:30 - <Notice> - Pcap-file module read 1 files, 31 packets, 2914 bytes
```

```
selks-user@SELKS:~/Desktop/MSIS602-basictraffic$ sudo suricata -c /etc/suricata/suricata.yaml -k none -r bfd-raw-auth-sha1.pcap --runmode=single

8/12/2023 -- 18:58:45 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
8/12/2023 -- 18:59:20 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
8/12/2023 -- 18:59:20 - <Notice> - Signal Received.  Stopping engine.
8/12/2023 -- 18:59:20 - <Notice> - Pcap-file module read 1 files, 25 packets, 2450 bytes
```

```
selks-user@SELKS:~/Desktop/MSIS602-basictraffic$ sudo suricata -c /etc/suricata/suricata.yaml -k none -r chargen-tcp.pcap --runmode=single
8/12/2023 -- 19:06:59 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
8/12/2023 -- 19:07:33 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
8/12/2023 -- 19:07:33 - <Notice> - Signal Received.  Stopping engine.
8/12/2023 -- 19:07:33 - <Notice> - Pcap-file module read 1 files, 22 packets, 14542 bytes
```

Running the command “sudo suricata -c /etc/suricata/suricata.yaml -k none -r <pcapfilename> --runmode=single” had us ingest the chosen pcap files in offline mode to ensure we were not actively monitoring our live network traffic. Here we can see the three pcap files were ingested successfully.



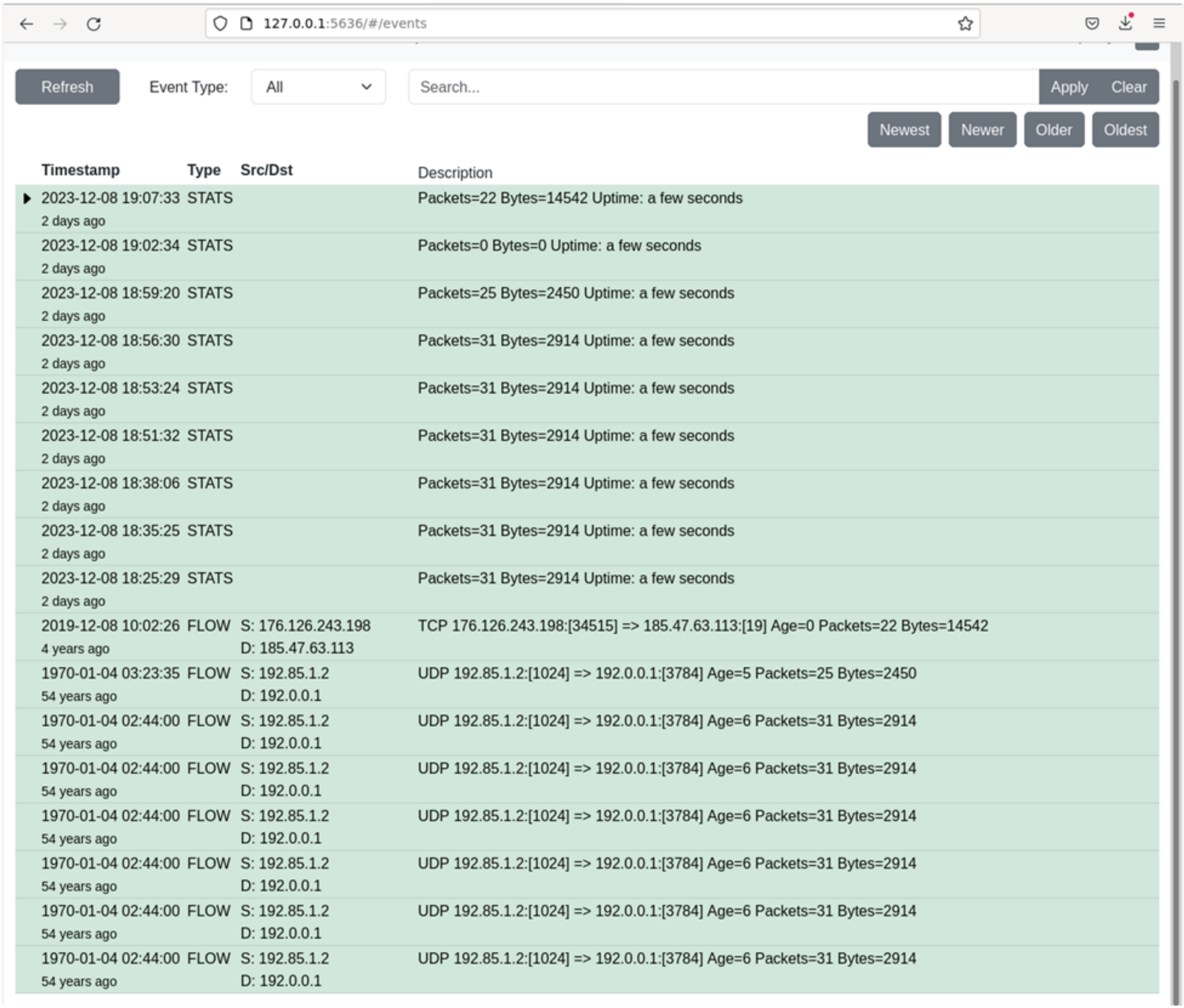
Here, I downloaded the latest version of EveBox from evebox.org.

```
selks-user@SELKS:~/Desktop$ sudo dpkg -i evebox-devel-amd64.deb
Selecting previously unselected package evebox.
(Reading database ... 102677 files and directories currently installed.)
Preparing to unpack evebox-devel-amd64.deb ...
Unpacking evebox (1:0.18.0~dev1697325760) ...
Setting up evebox (1:0.18.0~dev1697325760) ...
+ USERNAME=evebox
+ HOMEDIR=/var/lib/evebox
+ /usr/bin/getent passwd evebox
+ test -e /usr/sbin/adduser
+ /usr/sbin/adduser --system --home /var/lib/evebox --group --disabled-login evebox
Adding system user `evebox' (UID 117) ...
Adding new group `evebox' (GID 124) ...
Adding new user `evebox' (UID 117) with group `evebox' ...
Creating home directory `/var/lib/evebox' ...
```

Here, I downloaded the EveBox file from my Desktop so I would ensure I'd be working with the latest version of EveBox.

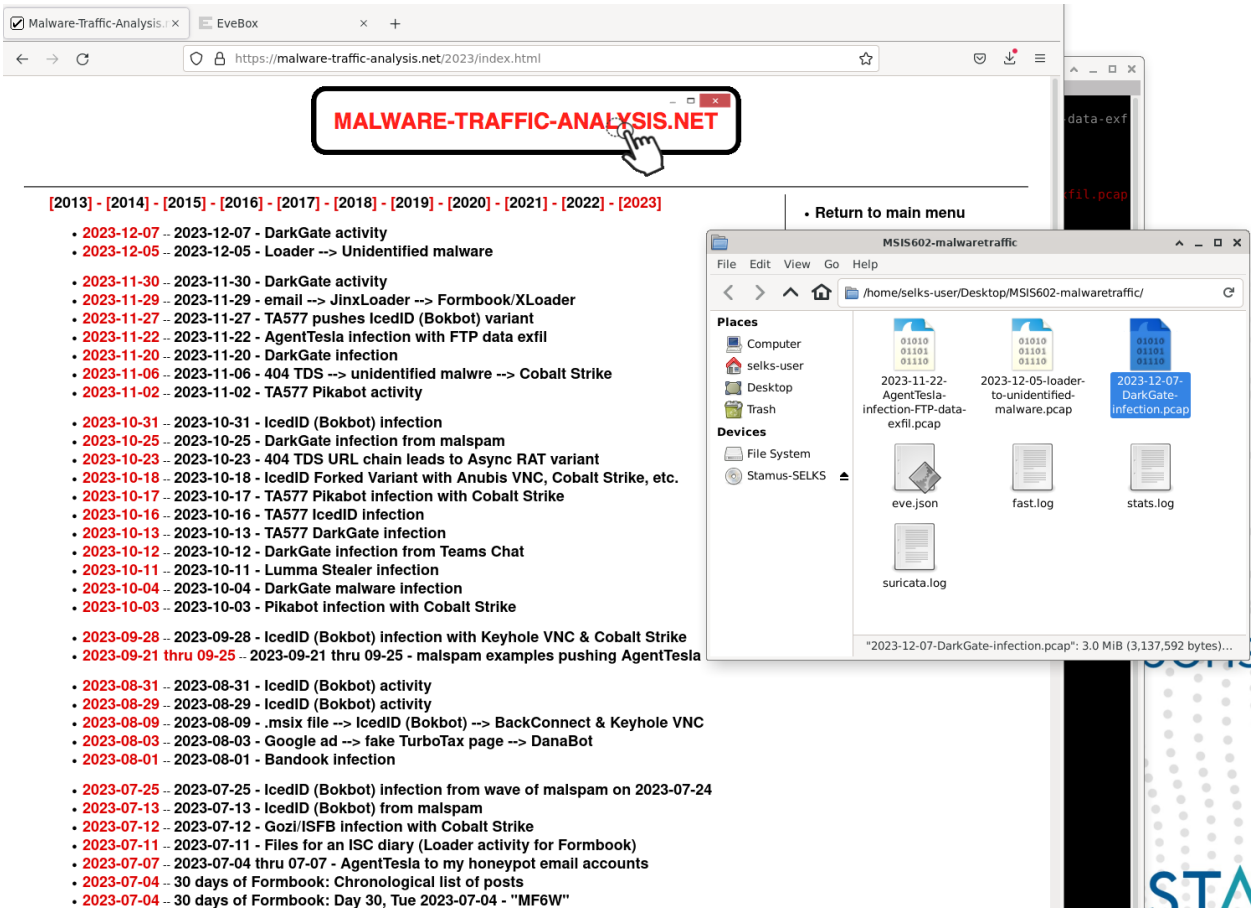
```
selks-user@SELKS:~$ cd /home/selks-user/Desktop/MSIS602-basictraffic/
selks-user@SELKS:~/Desktop/MSIS602-basictraffic$ evebox oneshot eve.json
2023-12-10 15:25:29  INFO evebox::commands::oneshot: Using database filename ./oneshot.sqlite
2023-12-10 15:25:29  INFO evebox::sqlite::connection: Auto-vacuum: 1
2023-12-10 15:25:29  INFO refinery_core::traits: current version: 4
2023-12-10 15:25:29  INFO refinery_core::traits::sync: no migrations to apply
2023-12-10 15:25:29  INFO evebox::sqlite::connection: Updating SQLite indexes
2023-12-10 15:25:29  INFO evebox::commands::oneshot: Reading eve.json (50166 bytes)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 2 events (11%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 3 events (12%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 4 events (22%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 5 events (23%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 6 events (33%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 7 events (34%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 8 events (44%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 9 events (45%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 10 events (55%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 11 events (56%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 12 events (67%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 13 events (68%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 14 events (78%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 15 events (88%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 16 events (89%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: eve.json: 17 events (100%)
2023-12-10 15:25:29  INFO evebox::commands::oneshot: Read 17 events
2023-12-10 15:25:29  INFO evebox::server::main: Using temporary in-memory configuration database
2023-12-10 15:25:29  INFO refinery_core::traits: schema history table is empty, going to apply all migrations
2023-12-10 15:25:29  INFO refinery_core::traits::sync: applying migration: V1__Initial
2023-12-10 15:25:29  INFO evebox::server::main: Starting Axum server on 127.0.0.1:5636
2023-12-10 15:25:29  INFO evebox::commands::oneshot: Server started at http://127.0.0.1:5636
2023-12-10 15:25:29  INFO evebox::commands::oneshot: If your browser didn't open, try connecting to http://127.0.0.1:5636
```

To explore the ingested pcaps with EveBox I first made sure I was in the proper folder with my basic traffic ingested pcaps and the created eve.json file. Then I opened EveBox using the command "evebox oneshot eve.json" and the events were read and EveBox opened on the browser.



Timestamp	Type	Src/Dst	Description
2023-12-08 19:07:33 2 days ago	STATS		Packets=22 Bytes=14542 Uptime: a few seconds
2023-12-08 19:02:34 2 days ago	STATS		Packets=0 Bytes=0 Uptime: a few seconds
2023-12-08 18:59:20 2 days ago	STATS		Packets=25 Bytes=2450 Uptime: a few seconds
2023-12-08 18:56:30 2 days ago	STATS		Packets=31 Bytes=2914 Uptime: a few seconds
2023-12-08 18:53:24 2 days ago	STATS		Packets=31 Bytes=2914 Uptime: a few seconds
2023-12-08 18:51:32 2 days ago	STATS		Packets=31 Bytes=2914 Uptime: a few seconds
2023-12-08 18:38:06 2 days ago	STATS		Packets=31 Bytes=2914 Uptime: a few seconds
2023-12-08 18:35:25 2 days ago	STATS		Packets=31 Bytes=2914 Uptime: a few seconds
2023-12-08 18:25:29 2 days ago	STATS		Packets=31 Bytes=2914 Uptime: a few seconds
2019-12-08 10:02:26 4 years ago	FLOW	S: 176.126.243.198 D: 185.47.63.113	TCP 176.126.243.198:[34515] => 185.47.63.113:[19] Age=0 Packets=22 Bytes=14542
1970-01-04 03:23:35 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=5 Packets=25 Bytes=2450
1970-01-04 02:44:00 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=6 Packets=31 Bytes=2914
1970-01-04 02:44:00 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=6 Packets=31 Bytes=2914
1970-01-04 02:44:00 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=6 Packets=31 Bytes=2914
1970-01-04 02:44:00 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=6 Packets=31 Bytes=2914
1970-01-04 02:44:00 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=6 Packets=31 Bytes=2914
1970-01-04 02:44:00 54 years ago	FLOW	S: 192.85.1.2 D: 192.0.0.1	UDP 192.85.1.2:[1024] => 192.0.0.1:[3784] Age=6 Packets=31 Bytes=2914

On the browser we can see the events log of UDP and a TCP protocol packet transmissions between a source ip address and a destination ip address. The types of pcap sample files I downloaded included BFD packets using md5 authentication, BFD packets using SHA1 authentication, and Chargen over TCP.



Next, I downloaded some recent 2023 malicious sample malware traffic pcap files from malware-traffic-analysis.net and extracted the pcap files out of the zip files using the password "infected" found on the "About this blog" tab. I then put the extracted pcap files in a folder I created called "MSIS602-malwaretraffic" which is saved to my Desktop.

The pcaps I downloaded and ingested are:

2023-12-07 -- 2023-12-07 - DarkGate activity

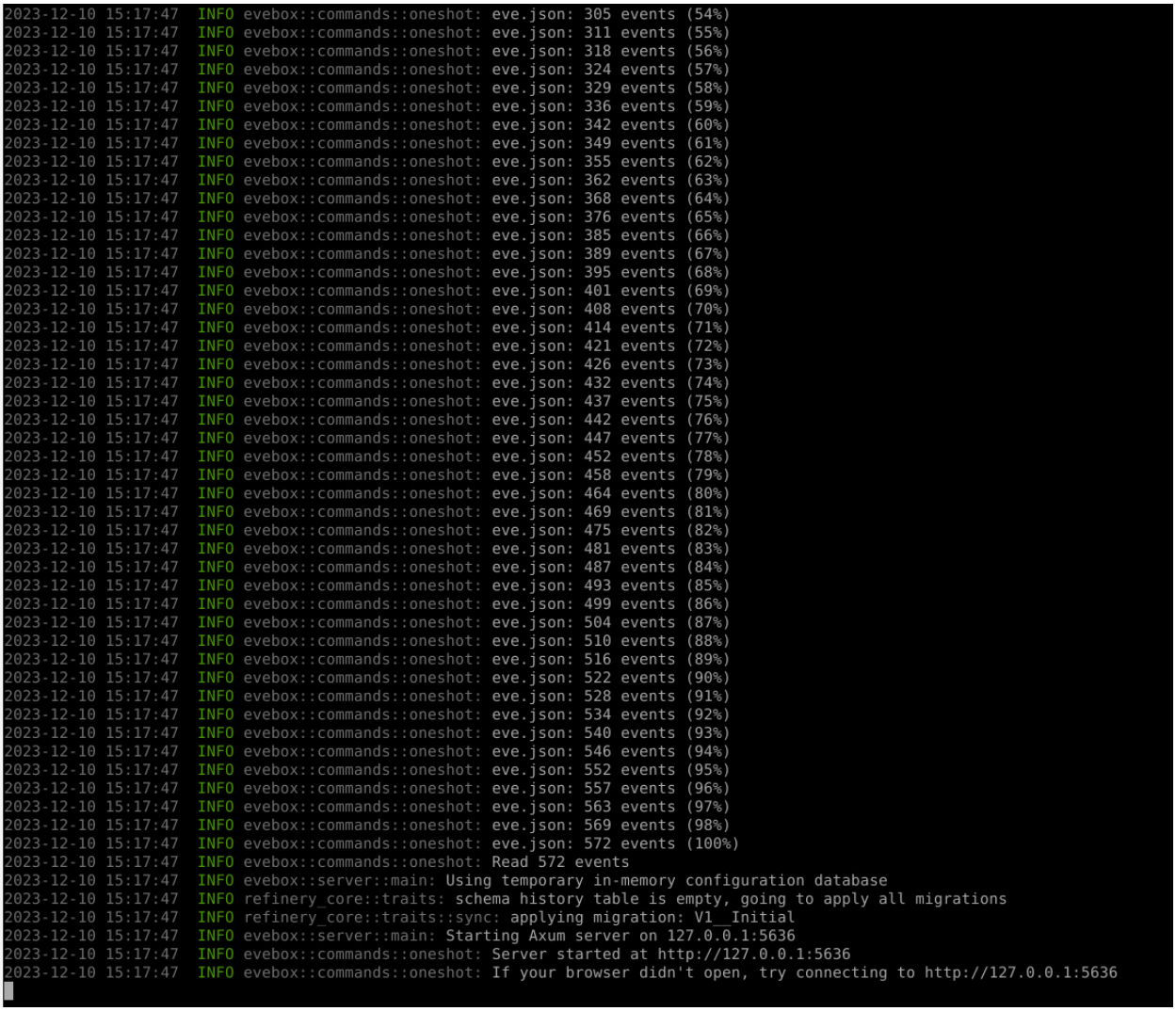
2023-12-05 -- 2023-12-05 - Loader --> Unidentified malware

2023-11-22 -- 2023-11-22 - AgentTesla infection with FTP data exfil

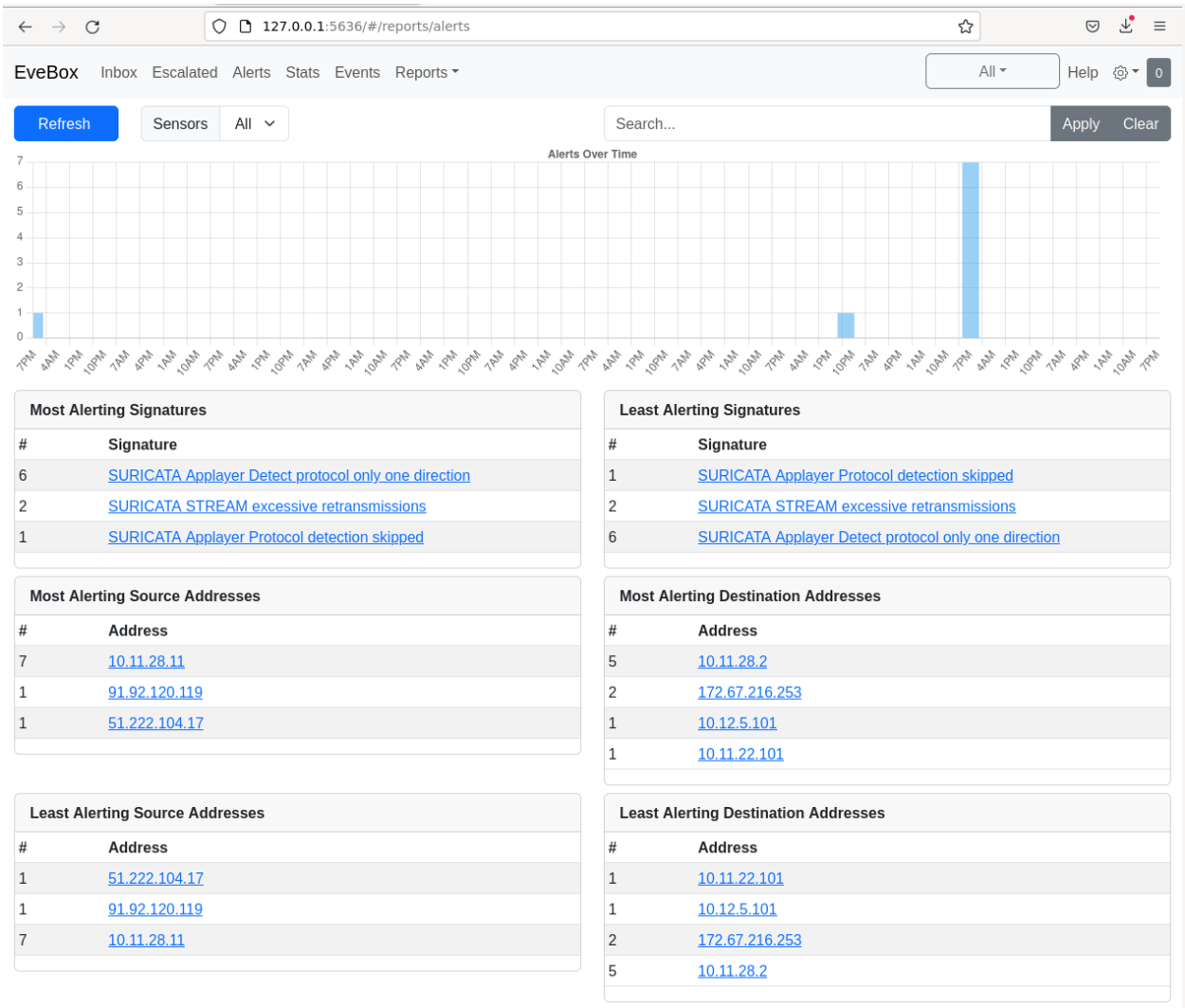
```
selks-user@SELKS:~/Desktop/MSIS602-malwaretraffic$ sudo suricata -c /etc/suricata/suricata.yaml -k none -r 2023-11-22-AgentTesla-infection-FTP-data-exf
il.pcap --runmode=single
10/12/2023 -- 15:06:54 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
10/12/2023 -- 15:07:32 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
10/12/2023 -- 15:07:32 - <Notice> - Signal Received.  Stopping engine.
10/12/2023 -- 15:07:32 - <Notice> - Pcap-file module read 1 files, 9993 packets, 9077142 bytes
selks-user@SELKS:~/Desktop/MSIS602-malwaretraffic$ sudo suricata -c /etc/suricata/suricata.yaml -k none -r 2023-12-05-loader-to-unidentified-malware.pc
ap --runmode=single
10/12/2023 -- 15:08:20 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
10/12/2023 -- 15:08:58 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
10/12/2023 -- 15:08:58 - <Notice> - Signal Received.  Stopping engine.
10/12/2023 -- 15:08:58 - <Notice> - Pcap-file module read 1 files, 2172 packets, 2707975 bytes
selks-user@SELKS:~/Desktop/MSIS602-malwaretraffic$ sudo suricata -c /etc/suricata/suricata.yaml -k none -r 2023-12-07-DarkGate-infection.pcap --runmode
=single
10/12/2023 -- 15:09:35 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
10/12/2023 -- 15:10:13 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
10/12/2023 -- 15:10:13 - <Notice> - Signal Received.  Stopping engine.
10/12/2023 -- 15:10:13 - <Notice> - Pcap-file module read 1 files, 4778 packets, 3061120 bytes
```

Then, using the same command as for the basic traffic pcap files, “sudo suricata -c /etc/suricata/suricata.yaml -k none -r <pcapfilename> --runmode=single”, I ingested the chosen pcap files in offline mode to ensure we were not actively monitoring our live network traffic. Here we can see the three-malware traffic pcap files were ingested successfully.

```
selks-user@SELKS:~$ cd /home/selks-user/Desktop/MSIS602-malwaretraffic/
selks-user@SELKS:~/Desktop/MSIS602-malwaretraffic$ evebox oneshot eve.json
2023-12-10 15:17:46  INFO evebox::commands::oneshot: Using database filename ./oneshot.sqlite
2023-12-10 15:17:46  INFO evebox::sqlite::connection: Auto-vacuum: 1
2023-12-10 15:17:46  INFO refinery_core::traits: current version: 4
2023-12-10 15:17:46  INFO refinery_core::traits::sync: no migrations to apply
2023-12-10 15:17:46  INFO evebox::sqlite::connection: Updating SQLite indexes
2023-12-10 15:17:46  INFO evebox::commands::oneshot: Reading eve.json (339485 bytes)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 6 events (1%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 13 events (2%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 20 events (3%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 26 events (4%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 29 events (5%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 30 events (6%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 35 events (7%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 39 events (9%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 45 events (10%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 48 events (11%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 53 events (12%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 60 events (13%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 65 events (14%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 70 events (15%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 76 events (16%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 81 events (17%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 85 events (18%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 91 events (19%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 96 events (20%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 102 events (21%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 109 events (22%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 115 events (23%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 122 events (24%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 128 events (25%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 134 events (26%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 141 events (27%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 147 events (28%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 154 events (29%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 158 events (30%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 164 events (31%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 171 events (32%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 176 events (33%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 183 events (34%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 190 events (35%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 196 events (36%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 203 events (37%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 209 events (38%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 216 events (39%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 222 events (40%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 227 events (41%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 234 events (42%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 239 events (43%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 245 events (44%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 251 events (45%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 257 events (46%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 263 events (47%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 268 events (48%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 274 events (49%)
2023-12-10 15:17:46  INFO evebox::commands::oneshot: eve.json: 280 events (50%)
2023-12-10 15:17:47  INFO evebox::commands::oneshot: eve.json: 286 events (51%)
2023-12-10 15:17:47  INFO evebox::commands::oneshot: eve.json: 292 events (52%)
2023-12-10 15:17:47  INFO evebox::commands::oneshot: eve.json: 298 events (53%)
2023-12-10 15:17:47  INFO evebox::commands::oneshot: eve.json: 305 events (54%)
```



To explore the ingested malware traffic pcaps with EveBox I first made sure I was in the proper folder with my malware traffic ingested pcaps and the created eve.json file. Then I opened EveBox using the command “evebox oneshot eve.json” and the events were read and EveBox opened on the browser.

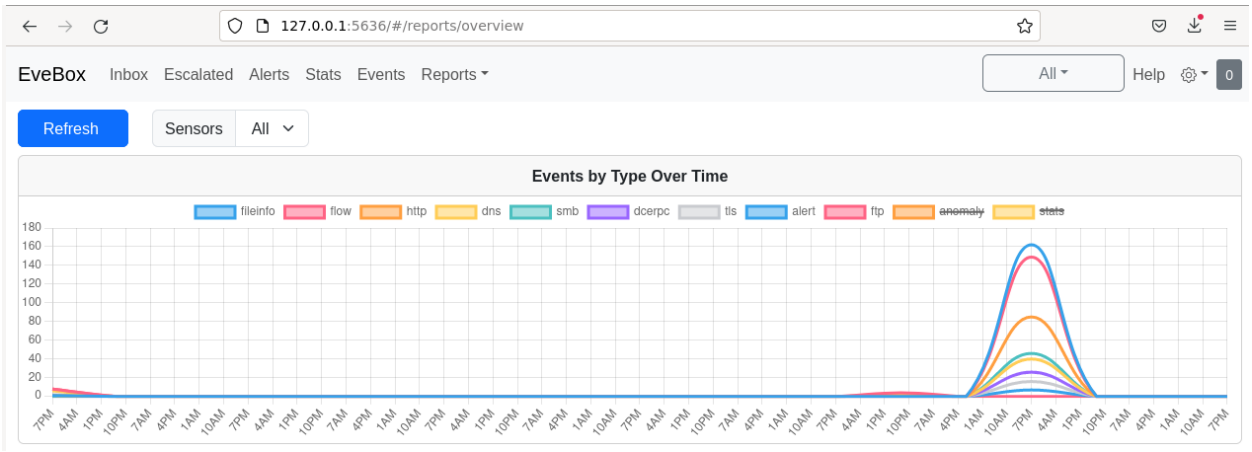


When viewing the reports alerts page, we can see the different events that took place with these file(s) are all nicely laid out for an easier analysis. This provides a much better experience than deciphering the raw json file.

2023-12-07 10:12:43 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	QUERY A wpad.elasticyouth.com
2023-12-07 10:12:42 3 days ago	ALERT	S: 10.11.28.11 D: 172.67.216.253	SURICATA STREAM excessive retransmissions tls Archive
2023-12-07 10:12:42 3 days ago	FILEINFO	S: 142.250.138.94 D: 10.11.28.11	/gtsr1 /ME4wTDBKMEgwRjAJBgUrDgMCGgUABBQwkcLWD4LqGJ7bE7B1XZsEbmfwUAQU5K8rJnEaK0gnhS9SZizv8lkTcT4CDQIDvFCjJ1PwkYAi7fE= Hostname:ocsp.pki.goog Path:/gtsr1 /ME4wTDBKMEgwRjAJBgUrDgMCGgUABBQwkcLWD4LqGJ7bE7B1XZsEbmfwUAQU5K8rJnEaK0gnhS9SZizv8lkTcT4CDQIDvFCjJ1PwkYAi7fE%3D Content-Type:application/ocsp-response http
2023-12-07 10:12:42 3 days ago	HTTP	S: 10.11.28.11 D: 142.250.138.94	GET ocsp.pki.goog /gtsr1 /ME4wTDBKMEgwRjAJBgUrDgMCGgUABBQwkcLWD4LqGJ7bE7B1XZsEbmfwUAQU5K8rJnEaK0gnhS9SZizv8lkTcT4CDQIDvFCjJ1PwkYAi7fE%3D
2023-12-07 10:12:41 3 days ago	FILEINFO	S: 142.250.138.94 D: 10.11.28.11	/gsr1/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6+MgGqMQQUYHtmGkUNl8qJUC99BM00qP/8/UsCEHe9DWzbNvka6iEPxPBY0w0= Hostname:ocsp.pki.goog Path:/gsr1 /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCEHe9DWzbNvka6iEPxPBY0w0%3D Content-Type:application/ocsp-response http
2023-12-07 10:12:41 3 days ago	HTTP	S: 10.11.28.11 D: 142.250.138.94	GET ocsp.pki.goog /gsr1/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCEHe9DWzbNvka6iEPxPBY0w0%3D
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	ANSWER A ocsp.pki.goog
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	QUERY A ocsp.pki.goog
2023-12-07 10:12:41 3 days ago	TLS	S: 10.11.28.11 D: 172.67.216.253	TLS 1.2 - cdn.boxmedrbopdrv.com - CN=boxmedrbopdrv.com
2023-12-07 10:12:41 3 days ago	HTTP	S: 10.11.28.11 D: 172.67.216.253	GET cdn.boxmedrbopdrv.com /boostrap/p.pdf
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	ANSWER A cdn.boxmedrbopdrv.com
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	QUERY A cdn.boxmedrbopdrv.com
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	ANSWER TXT tos.viewdobdrv.com
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	QUERY TXT tos.viewdobdrv.com
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	ANSWER TXT tos.viewdobdrv.com.elasticyouth.com - NXDOMAIN
2023-12-07 10:12:41 3 days ago	DNS	S: 10.11.28.11 D: 10.11.28.2	QUERY TXT tos.viewdobdrv.com.elasticyouth.com
2023-12-07 10:12:41	DNS	S: 10.11.28.11	ANSWER PTR 2.28.11.10.in-addr.arpa

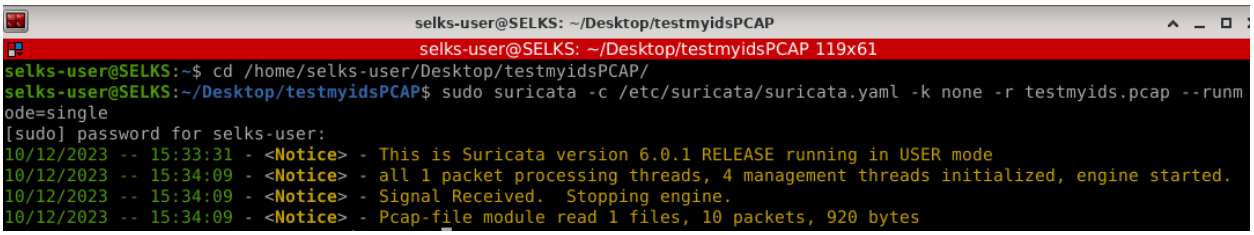
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[64309] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=241	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52248] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[51342] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=241	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[54474] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=197	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52242] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[53355] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=194	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52224] => 46.101.78.238:[443] Age=1 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 239.255.255.250	UDP 10.11.28.11:[53072] => 239.255.255.250:[1900] Age=1 Packets=2 Bytes=434	
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 172.67.216.253	TCP 10.11.28.11:[52105] => 172.67.216.253:[80] Age=2 Packets=10 Bytes=1364	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52267] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52137] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=982	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52124] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[63706] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=632	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[54007] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=295	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52146] => 46.101.78.238:[443] Age=1 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52136] => 46.101.78.238:[443] Age=1 Packets=9 Bytes=982	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 10.11.28.2	UDP 10.11.28.11:[57168] => 10.11.28.2:[53] Age=0 Packets=2 Bytes=315	dns
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52236] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52140] => 46.101.78.238:[443] Age=0 Packets=9 Bytes=983	http
2023-12-07 10:11:56 FLOW 3 days ago	S: 10.11.28.11 D: 46.101.78.238	TCP 10.11.28.11:[52134] => 46.101.78.238:[443] Age=1 Packets=9 Bytes=982	http
2023-12-07 10:11:56 FLOW	S: 10.11.28.11	TCP 10.11.28.11:[52141] => 46.101.78.238:[443] Age=1 Packets=9 Bytes=983	http

Here we can see some of the events that took place within these malicious malware traffic pcap files. In these events we see some UDP and TCP protocol packet transmissions between a source ip address and a destination ip address. We also see some queries with GET and ANSWER requests to likely extract information.

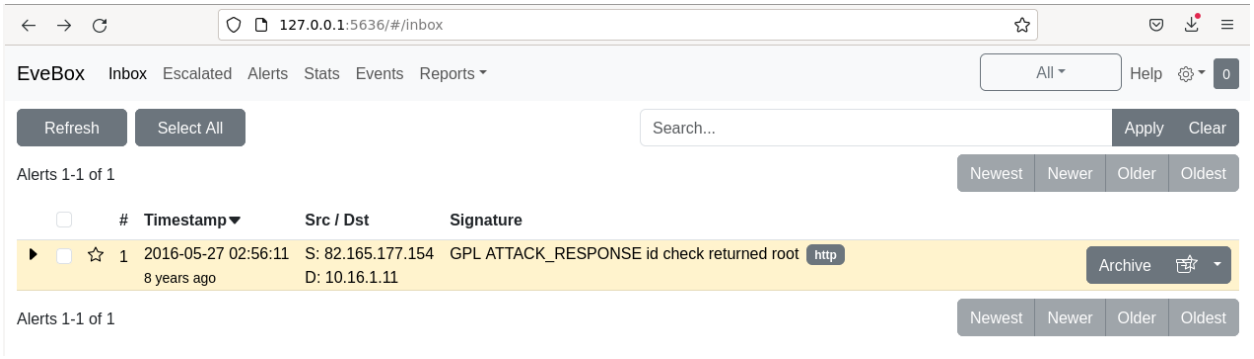


Lastly, we see the reports overview tab with different types of events occurrences labeled by colors.

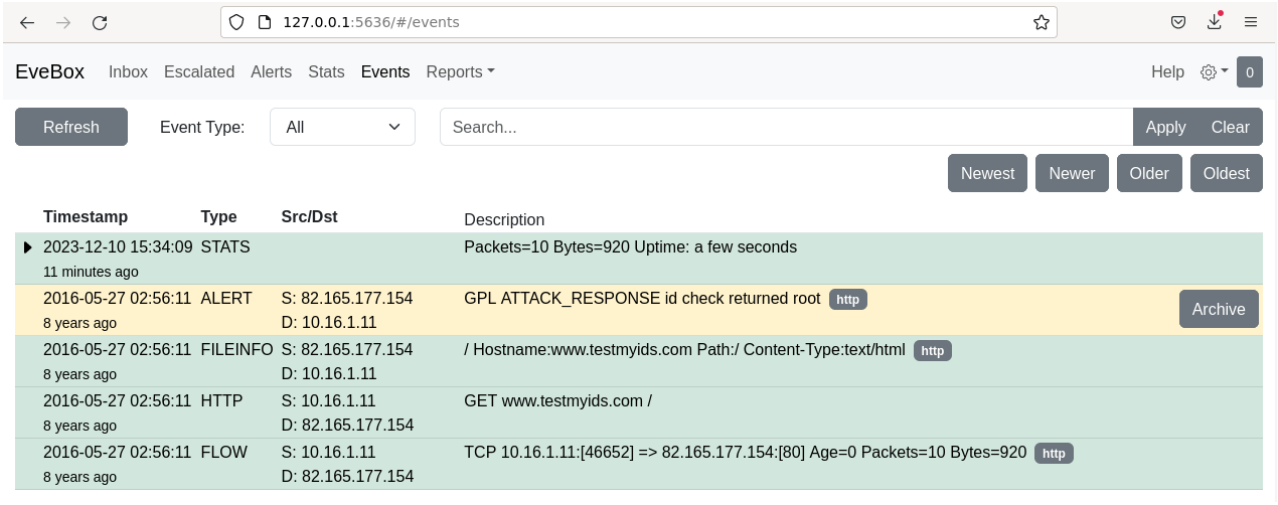
TASK THREE: Generate Alerts within EveBox

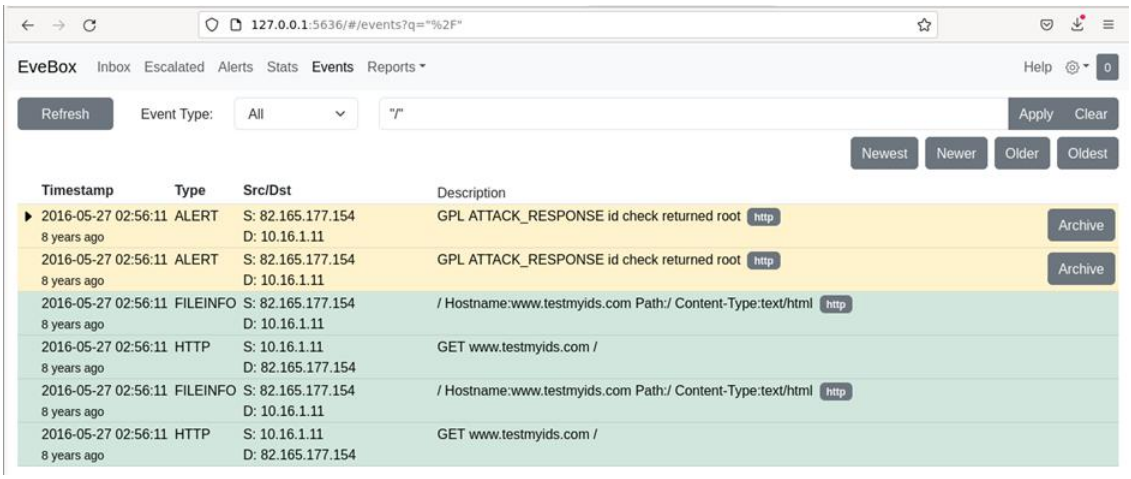


Similarly, to the previous section I downloaded and ingested a pcap file called “testmyids” from redmine.openinfosecfoundation.org. As with the previous two I made a folder called “testmyidsPCAP” to put the downloaded pcap file in. Using the same command, “sudo suricata -c /etc/suricata/suricata.yaml -k none -r <pcapfilename> --runmode=single”, I ingested this pcap file in offline mode to ensure we were not actively monitoring our live network traffic. Here we see this pcap file was ingested successfully.

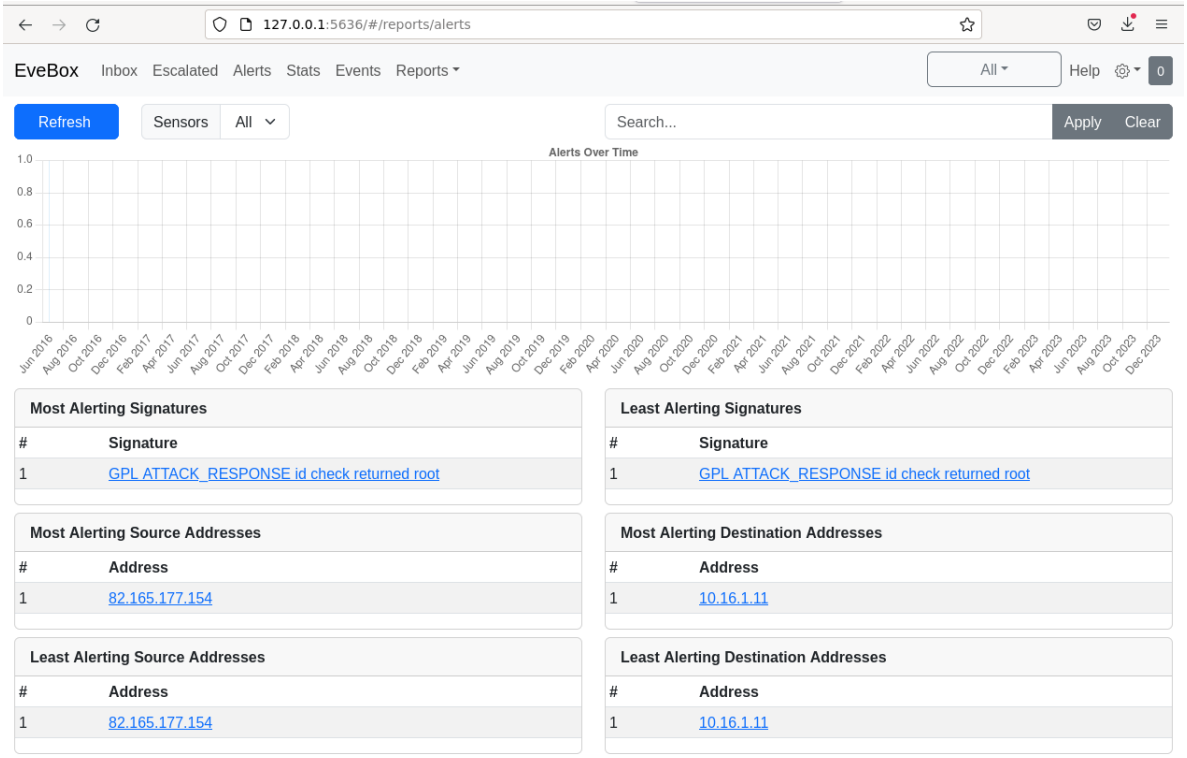


Upon initial opening of EveBox there is an alert generated under inbox that states a GPL ATTACK_RESPONSE id check returned to root.

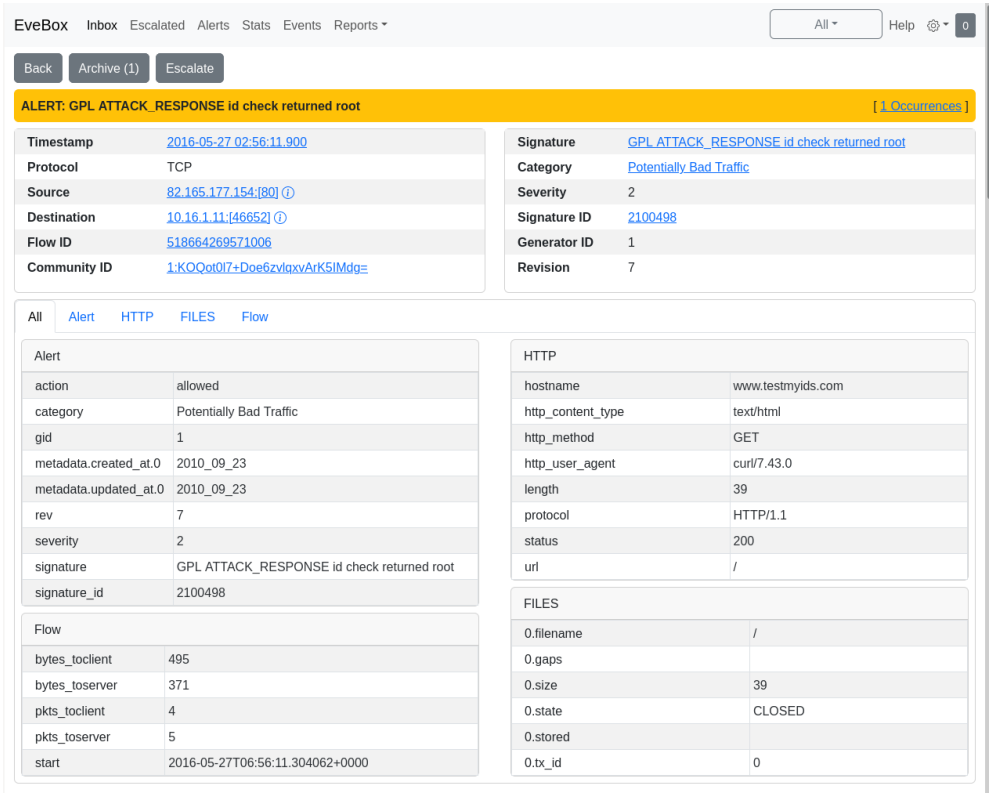




This likely means some user with bad intensions has root privileges and the corresponding website is likely compromised. The protocols involved in this alert include TCP and a GET request. This alert came from the Hostname: “www.testmyids.com” and since we have a TCP and a GET request, I believe this is using an “all” rule set as per “/”.



Here we can see the reports alerts page where the events of this pcap file are nicely laid out for easier analysis. Again, this provides a much better experience than deciphering the raw json file.



Event Listing	
_id	3
_metadata.aggregate	
_metadata.count	1
_metadata.escalated_count	0
_metadata.max_timestamp	2016-05-27T06:56:11.900879+0000
_metadata.min_timestamp	2016-05-27T06:56:11.900879+0000
_source.alert.action	allowed
_source.alert.category	Potentially Bad Traffic
_source.alert.gid	1
_source.alert.metadata.created_at.0	2010_09_23
_source.alert.metadata.updated_at.0	2010_09_23
_source.alert.rev	7
_source.alert.severity	2
_source.alert.signature	GPL ATTACK_RESPONSE id check returned root
_source.alert.signature_id	2100498
_source.app_proto	http
_source.community_id	1:KOQot0l7+Doe6zvlqxvArK5IMdg=
_source.dest_ip	10.16.1.11
_source.dest_port	46652
_source.event_type	alert
_source.files.0.filename	/
_source.files.0.gaps	
_source.files.0.size	39
_source.files.0.state	CLOSED
_source.files.0.stored	
_source.files.0.tx_id	0
_source.flow.bytes_toclient	495
_source.flow.bytes_toserver	371
_source.flow.pkts_toclient	4
_source.flow.pkts_toserver	5
_source.flow.start	2016-05-27T06:56:11.304062+0000
_source.flow_id	518664269571006
_source.http.hostname	www.testmyids.com
_source.http.http_content_type	text/html
_source.http.http_method	GET
_source.http.http_user_agent	curl/7.43.0
_source.http.length	39
_source.http.protocol	HTTP/1.1
_source.http.status	200
_source.http.url	/
_source.pcap_cnt	9
_source.proto	TCP
_source.src_ip	82.165.177.154
_source.src_port	80
_source.timestamp	2016-05-27T06:56:11.900879+0000

When reviewing the inbox alerts page, we can see the event and all the corresponding necessary data nicely laid out for easy analysis providing for a user-friendly experience.

JSON

```
{
   _id: 3,
   _metadata: {
      aggregate: true,
      count: 1,
      escalated_count: 0,
      max_timestamp: "2016-05-27T06:56:11.900879+0000",
      min_timestamp: "2016-05-27T06:56:11.900879+0000"
   },
   _source: {
      alert: {
         action: "allowed",
         category: "Potentially Bad Traffic",
         gid: 1,
         metadata: {
            created_at: [
               "2010_09_23"
            ],
            updated_at: [
               "2010_09_23"
            ]
         },
         rev: 7,
         severity: 2,
         signature: "GPL ATTACK_RESPONSE id check returned root",
         signature_id: 2100498
      },
      app_proto: "http",
      community_id: "1:KOQot0l7+Doe6zvlqxvArK5IMdg=",
      dest_ip: "10.16.1.11",
      dest_port: 46652,
      evebox: {},
      event_type: "alert",
      files: [
         {
            filename: "/",
            gaps: false,
            sid: [],
            size: 39,
            state: "CLOSED",
            stored: false,
            tx_id: 0
         }
      ],
      flow: {
         bytes_toclient: 495,
         bytes_toserver: 371,
         pkts_toclient: 4,
         pkts_toserver: 5,
         start: "2016-05-27T06:56:11.304062+0000"
      },
      flow_id: 518664269571006,
      http: {
         hostname: "www.testmyids.com",
         http_content_type: "text/html",
         http_method: "GET",
         http_user_agent: "curl/7.43.0",
         length: 39,
         protocol: "HTTP/1.1",
         status: 200,
         url: "/"
      },
      pcap_cnt: 9,
      proto: "TCP",
      src_ip: "82.165.177.154",
      src_port: 80,
      tags: [],
      timestamp: "2016-05-27T06:56:11.900879+0000"
   }
}
```


Here we see the json file contents formatted.

A Network Intrusion Detection System (NIDS) and Network Security Monitoring (NSM) system are extremely valuable assets for any organization to have. They help detect and monitor incidents right as they occur early on so potential damages and costs can be minor if any. Security professionals can use data obtained from these to put proper precautions in place and respond to potential threats swiftly in real time. It is important these are in place and monitored so organizations can have little to no downtime as this can be costly and result in loss of sales.

Conclusion:

Everything went smoothly in this lab as I was able to accurately figure out and complete the analysis of the ingested files on the SELKS VM using Suricata and EveBox. It took a little time, but I got through figuring out how to properly make all the necessary configurations within my environment to ingest pcap files as well as how to open the contents with EveBox.

References:

3. installation. 3. Installation - Suricata 8.0.0-dev documentation. (n.d.). https://docs.suricata.io/en/latest/install.html

Gite, V. (2023, August 24). How to: VI / vim save and quit the editor command - nixcraft. Cyberciti. https://www.cyberciti.biz/faq/linux-unix-vim-save-and-quit-command/

How-To: Installing EveBox for Managing Events and Alerts from Suricata. (2021). YouTube. Retrieved December 8, 2023, from https://youtu.be/XXHCs2oZjHw?si=v7xjZdLCgK5IjKXE.

Installing & Configuring Suricata. (2022). YouTube. Retrieved December 7, 2023, from https://youtu.be/UXKbh0jPPpg?si=axAyn4ED0sAfE4qB.

Investigating NullMixer Network Traffic: IDS Rules from Suricata and Evebox. (2023). YouTube. Retrieved December 8, 2023, from https://youtu.be/v_K_zoPGpdk?si=4Ktpp9WkuZiJpDmi.

StamusNetworks. (n.d.). First Time Setup. GitHub. https://github.com/StamusNetworks/SELKS/wiki/First-time-setup#first-time-setup