Configuration Manual

Kaweesa James

Student ID: 21226385

School of Computing

National college of Ireland

Supervisor: Micheal Pantridge

National College of Ireland

Project Submission Sheet – 2022/2023

Student Name:	……KAWEESA JAMES ……
Student ID:	……21226385……
Programme:	……Cybersecurity…… **Year:** ……2022/2023……
Module:	……MSC……
Lecturer:	…… Micheal Pantridge ……
Submission Due Date:	……14/08/2023……
Project Title:	……An Evaluation of Network Intrusion Detection System / Configuration Manual ……
Word Count:	……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary

action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: ……KAWEESA JAMES ……

Date: ……14/08/2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. You must ensure that you retain a HARD COPY of ALL projects, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. Late submissions will incur penalties.
5. All projects must be submitted and passed in order to successfully complete the year. Any project/assignment not submitted will be marked as a fail.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

1. Introduction

This document provides detailed information about the system specifications, as well as the software and hardware employed in executing the project. Additionally, it outlines the procedures undertaken during the implementation of the research.

2. System Configuration

2.1. Hardware specifications

Host computer

- Lenovo Thinkpad L13 yoga
- Icore 7, 11th Gen, 16GB RAM, 1TB SSD-Hardrive, OS window 11 64-bit.
-

2.2. Software specification

Signature detection

- Virtual environment- virtualbox 6.1.38
- Linux ubuntu 22
- kali linux
- Suricata IDS/IPS version 6.0.13

Anomaly detection

- Anaconda/jupyter notebook
- python3

3. Dataset

Download url: https://www.unb.ca/cic/datasets/ids-2017.html

4. Anomaly detection and evaluation of Isolation Forest algorithm with CICIDS2017 dataset

Jupiter notebook/python 3

Isolation Forest Anomaly detection with CICIDS2017

1. Loading Data/libraries
2. Preprocessing Data
3. Machine Learning Model Isolation Forest to detect anomaly.
4. Evaluation

Loading libraries

```
import numpy as np # linear algebra
import pandas as pd # data processing, CSV file I/O (e.g. pd.read_csv)
# Ignore warnings
import warnings
warnings.filterwarnings('ignore')
```

Loading CSV files

```
#Settings
pd.set_option('display.max_columns', None)
pd.set_option('display.max_rows', None)
#Probably can`t be finished because of huge amount of data
#Load Data

cols = [' Bwd Packet Length Std',' PSH Flag Count',' min_seg_size_forward'
,' Min Packet Length',' ACK Flag Count',' Bwd Packet Length Min',' Fwd IAT
Std','Init_Win_bytes_forward',' Flow IAT Max',' Bwd Packets/s',' URG Flag
Count','Bwd IAT Total',' Label']
df1=pd.read_csv("Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv", usecol
s = cols)#,nrows = 50000
df2=pd.read_csv("Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv", us
ecols = cols)
df3=pd.read_csv("Friday-WorkingHours-Morning.pcap_ISCX.csv", usecols = col
s)
df5=pd.read_csv("Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.c
sv", usecols = cols)
df6=pd.read_csv("Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX.csv",
usecols = cols)

#

df = pd.concat([df1,df2])
del df1,df2
df = pd.concat([df,df3])
del df3
df = pd.concat([df,df5])
del df5
df = pd.concat([df,df6])
del df6

data = df.copy()

y = data[' Label'].copy()
X = data.drop([' Label'],axis=1)
```

statistics and information about a DataFrame “data”

```
# Display basic statistics about the DataFrame 'data'
data_description = data.describe()

# Display information about the DataFrame columns and data types
data_info = data.info()

# Display the number of rows and columns in the DataFrame
num_rows, num_cols = data.shape

print("Data Description:")
print(data_description)

print("\nData Information:")
```

```
print(data_info)

print(f"\nNumber of Rows: {num_rows}")
print(f"Number of Columns: {num_cols}")
```

```
<class 'pandas.core.frame.DataFrame'>
Int64Index: 1162213 entries, 0 to 170365
Data columns (total 13 columns):
 #   Column                  Non-Null Count    Dtype
---  ------                  --------------    -----
 0    Bwd Packet Length Min  1162213 non-null  int64
 1    Bwd Packet Length Std  1162213 non-null  float64
 2    Flow IAT Max           1162213 non-null  int64
 3    Fwd IAT Std            1162213 non-null  float64
 4   Bwd IAT Total           1162213 non-null  int64
 5    Bwd Packets/s          1162213 non-null  float64
 6    Min Packet Length      1162213 non-null  int64
 7    PSH Flag Count         1162213 non-null  int64
 8    ACK Flag Count         1162213 non-null  int64
 9    URG Flag Count         1162213 non-null  int64
 10  Init_Win_bytes_forward  1162213 non-null  int64
 11   min_seg_size_forward   1162213 non-null  int64
 12   Label                  1162213 non-null  object
dtypes: float64(3), int64(9), object(1)
memory usage: 124.1+ MB
Data Description:
        Bwd Packet Length Min   Bwd Packet Length Std   Flow IAT Max  \
count            1.162213e+06            1.162213e+06   1.162213e+06
mean             3.773220e+01            3.155979e+02   5.220704e+06
std              6.570729e+01            9.136183e+02   1.645845e+07
min              0.000000e+00            0.000000e+00  -1.300000e+01
25%              0.000000e+00            0.000000e+00   6.600000e+01
50%              6.000000e+00            0.000000e+00   2.394000e+04
75%              6.600000e+01            0.000000e+00   9.538950e+05
max              1.639000e+03            8.194660e+03   1.200000e+08

        Fwd IAT Std  Bwd IAT Total   Bwd Packets/s   Min Packet Length  \
count  1.162213e+06   1.162213e+06    1.162213e+06        1.162213e+06
mean   1.707842e+06   7.902467e+06    9.647080e+03        1.524134e+01
std    5.894992e+06   2.590312e+07    4.369168e+04        2.312447e+01
min    0.000000e+00   0.000000e+00    0.000000e+00        0.000000e+00
25%    0.000000e+00   0.000000e+00    2.029015e-01        0.000000e+00
50%    0.000000e+00   1.000000e+00    3.195909e+01        2.000000e+00
75%    1.802459e+04   3.101500e+04    1.117318e+04        3.400000e+01
max    8.350000e+07   1.200000e+08    2.000000e+06        1.359000e+03

        PSH Flag Count   ACK Flag Count   URG Flag Count  \
count     1.162213e+06     1.162213e+06     1.162213e+06
mean      4.041092e-01     2.684568e-01     9.252865e-02
std       4.907190e-01     4.431568e-01     2.897709e-01
min       0.000000e+00     0.000000e+00     0.000000e+00
25%       0.000000e+00     0.000000e+00     0.000000e+00
50%       0.000000e+00     0.000000e+00     0.000000e+00
75%       1.000000e+00     1.000000e+00     0.000000e+00
```

```
max       1.000000e+00     1.000000e+00     1.000000e+00

       Init_Win_bytes_forward   min_seg_size_forward
count            1.162213e+06          1.162213e+06
mean             6.883704e+03          2.567379e+01
std              1.299677e+04          6.825600e+00
min             -1.000000e+00          0.000000e+00
25%             -1.000000e+00          2.000000e+01
50%              2.690000e+02          2.000000e+01
75%              8.192000e+03          3.200000e+01
max              6.553500e+04          6.000000e+01

Data Information:
None

Number of Rows: 1162213
Number of Columns: 13
```

Machine Learning Models Isolation Forest

```
from sklearn.ensemble import IsolationForest

rng = np.random.RandomState(42)

model = IsolationForest(max_samples=5000, random_state=rng)
model.fit(X)
y_pred = model.predict(X)
print(y_pred)
print(y_pred.shape)

print("percentage of normal traffic:", (list(y_pred).count(1)/y_pred.shape
[0])*100)
print("percentage of Anomaly traffic:",(list(y_pred).count(-1)/y_pred.shap
e[0])*100)
```

```
[1 1 1 ... 1 1 1]
(1162213,)
percentage of normal traffic: 94.94068643183307
percentage of Anomaly traffic: 5.059313568166936
```

Creating True Data

```
y.unique()
```

```
array(['BENIGN', 'DDoS', 'PortScan', 'Bot', 'Infiltration',
       'Web Attack \ufffd Brute Force', 'Web Attack \ufffd XSS',
       'Web Attack \ufffd Sql Injection'], dtype=object)
```

```
y_true=y.copy()
attack = ['DDoS', 'PortScan', 'Bot', 'Infiltration', 'Web Attack \ufffd Brute
Force', 'Web Attack \ufffd XSS', 'Web Attack \ufffd Sql Injection']
normal = 'BENIGN'
y_true=y_true.replace(attack, -1)
```

```
y_true=y_true.replace(normal, 1)
y_true.unique()
```

```
array([ 1, -1], dtype=int64)
```

Evaluation

```
print (len(y_true))
y_true.value_counts()
```

```
1162213
 1    871074
-1    291139
Name:  Label, dtype: int64
```

```
print(len(y_pred))
pd.Series(y_pred).value_counts()
```

```
1162213
 1    1103413
-1      58800
dtype: int64
```

Calculating a confusion matrix

```
from sklearn.metrics import confusion_matrix
cf_matrix = confusion_matrix(y_true, y_pred)
tn, fp, fn, tp = cf_matrix.ravel()
cf_matrix
```

```
array([[ 11053, 280086],
       [ 47747, 823327]], dtype=int64)
```

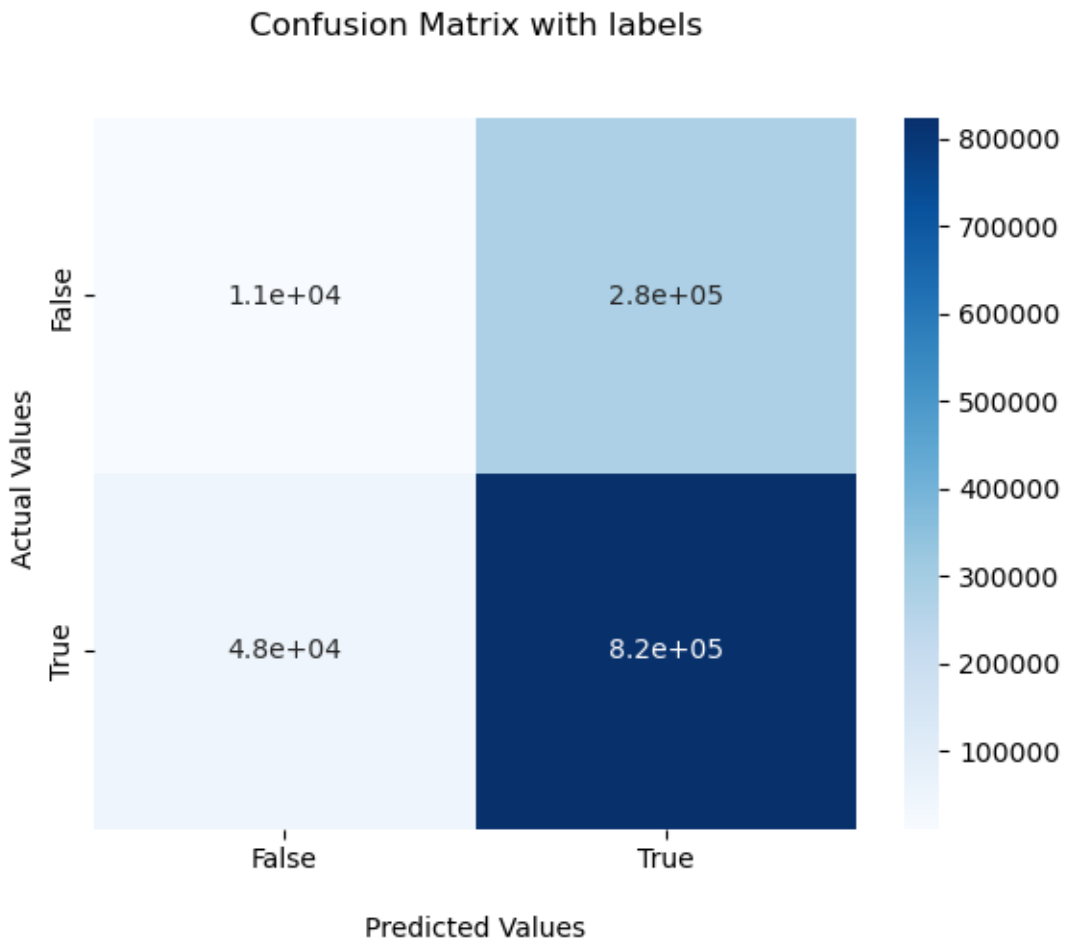
Visual representation of the confusion matrix

```
import seaborn as sns
import matplotlib.pyplot as plt
ax = sns.heatmap(cf_matrix, annot=True, cmap='Blues')

ax.set_title('Confusion Matrix with labels\n\n');
ax.set_xlabel('\nPredicted Values')
ax.set_ylabel('Actual Values ');

## Ticket Labels - List must be in alphabetical order
ax.xaxis.set_ticklabels(['False','True'])
ax.yaxis.set_ticklabels(['False','True'])

## Display the visualization of the Confusion Matrix.
plt.show()
```



Counts of true negatives, true positives, false negatives, and false positives from the confusion matrix

```
print ("True Negetive", tn,
       "\nTrue Positive", tp)
print ("False Negetive", fn,
       "\nFalse Positive", fp)
```

```
True Negetive 11053
True Positive 823327
False Negetive 47747
False Positive 280086
```

Calculating Precision, recall and F1 score

```
recall = tp/(tp+fn)
precision = tp/(tp+fp)
print("Recall", recall, "\nPrecision", precision)
```

```
Recall 0.9451860576713345
Precision 0.7461639476787023
```

```
f1 = 2 * (precision*recall)/(precision+recall)
print("F1 Score", f1)
```

```
F1 Score 0.8357290232102951
```

2. Signature detection with Suricata

Suricata Installation and configuration on Linux ubuntu version 22

Installation from the repository

```
root@suricata:~# sudo add-apt-repository ppa:oisf/suricata-stable
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy main'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.
```

installation

```
root@suricata:~# sudo apt-get install suricata
```

Enabling Suricata to start automatically when the system boots

```
root@suricata:~# sudo systemctl enable suricata.service
```

Verifying Suricata service running

```
root@suricata:~# sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Tue 2023-08-08 11:15:30 IST; 2h 41min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 10 (limit: 6949)
     Memory: 472.9M
        CPU: 4min 31.799s
     CGroup: /system.slice/suricata.service
             └─989 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv

Aug 08 11:15:30 suricata systemd[1]: Starting LSB: Next Generation IDS/IPS...
Aug 08 11:15:30 suricata systemd[1]: Started LSB: Next Generation IDS/IPS.
Aug 08 11:15:30 suricata suricata[837]: Starting suricata in IDS (af-packet) mode... done.
```

configuring to listen to default interface connection using specified ruleset

#Default interface enp0s3

```
root@suricata:~# ip -p -j route show default
[ {
        "dst": "default",
        "gateway": "192.168.1.1",
        "dev": "enp0s3",
        "protocol": "static",
        "metric": 20100,
        "flags": [ ]
```

#changing community-id to true and listening interface through the Suricata configuration file syricata.yaml

```
root@suricata:~# sudo nano /etc/suricata/suricata.yaml
```

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

```
# Linux high speed capture support
af-packet:
  - interface: enp0s3
    # Number of receive threads. "auto" uses the number of cores
```

Updating Suricata ruleset provider

```
root@suricata:~# sudo suricata-update --no-check-certificate update sources
```

listing ruleset provider sources

```
root@suricata:~# sudo suricata-update list-sources
8/8/2023 -- 14:23:57 - <Info> -- Using data-directory /var/lib/suricata.
8/8/2023 -- 14:23:57 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
8/8/2023 -- 14:23:57 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
8/8/2023 -- 14:23:57 - <Info> -- Found Suricata version 6.0.13 at /usr/bin/suricata.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/malware
  Vendor: Secureworks
  Summary: Secureworks suricata-malware ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: scwx/security
  Vendor: Secureworks
  Summary: Secureworks suricata-security ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
Name: sslbl/ssl-fp-blacklist
  Vendor: Abuse.ch
  Summary: Abuse.ch SSL Blacklist
  License: Non-Commercial
Name: sslbl/ja3-fingerprints
  Vendor: Abuse.ch
  Summary: Abuse.ch Suricata JA3 Fingerprint Ruleset
```

check if Suricata is configured with zero errors

```
root@suricata:~# sudo suricata -T -c /etc/suricata/suricata.yaml -v
8/8/2023 -- 14:26:39 - <Info> - Running suricata under test mode
8/8/2023 -- 14:26:39 - <Notice> - This is Suricata version 6.0.13 RELEASE running in SYSTEM mode
8/8/2023 -- 14:26:39 - <Info> - CPUs/cores online: 4
8/8/2023 -- 14:26:39 - <Info> - Setting engine mode to IDS mode by default
8/8/2023 -- 14:26:39 - <Info> - fast output device (regular) initialized: fast.log
8/8/2023 -- 14:26:39 - <Info> - eve-log output device (regular) initialized: eve.json
8/8/2023 -- 14:26:39 - <Info> - stats output device (regular) initialized: stats.log
8/8/2023 -- 14:27:00 - <Info> - 2 rule files processed. 34692 rules successfully loaded, 0 rules failed
8/8/2023 -- 14:27:00 - <Info> - Threshold config parsed: 0 rule(s) found
8/8/2023 -- 14:27:01 - <Info> - 34695 signatures processed. 1311 are IP-only rules, 5248 are inspecting packet payload, 27923 inspect application layer, 108 are decoder event only
8/8/2023 -- 14:27:11 - <Notice> - Configuration provided was successfully loaded. Exiting.
8/8/2023 -- 14:27:11 - <Info> - cleaning up signature grouping structure... complete
```

Installing jq utility to query eve,jsob suricata log file

```
root@suricata:~# sudo apt install jq
```

```
root@suricata:~# chmod +x pcap-offline.sh
root@suricata:~# sudo ./pcap-offline.sh Tuesday-WorkingHours.pcap
```

Running the script above followed by the pcap file.

will running Suricata will analyze the pcap file in offline mode.

#Alerrts generated based on suricata signature in the ruleset

```
17-07-04T20:55:03.630452+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:46875 -> 208.185.118.91:80"
17-07-04T20:55:03.651004+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:33327 -> 23.194.140.205:80"
17-07-04T20:55:03.656174+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:49696 -> 23.60.139.27:80"
17-07-04T20:53:14.700783+0100 | 1:2210038:2 | SURICATA STREAM FIN out of window | Generic Protocol Command Decode | 98.139.225.4
17-07-04T20:55:03.904681+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:49191 -> 23.199.172.185:80"
17-07-04T20:55:14.763673+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.16:59684 -> 172.217.11.14:80"
17-07-04T20:55:14.784396+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.16:59372 -> 72.21.91.29:80"
17-07-04T20:55:04.005620+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:37251 -> 23.50.75.27:80"
17-07-04T20:55:04.189278+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:33328 -> 23.194.140.205:80"
17-07-04T20:53:20.464783+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.15:59572 -> 104.16.21.35:80"
17-07-04T20:55:05.109344+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:34237 -> 151.101.0.249:80"
17-07-04T20:55:05.480529+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:37215 -> 207.123.46.253:80"
17-07-04T20:55:05.968918+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:44404 -> 50.116.194.21:80"
17-07-04T20:55:06.011210+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:37215 -> 207.123.46.253:80"
17-07-04T20:54:53.766448+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:50312 -> 23.194.141.50:80"
17-07-04T20:55:06.025967+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:41607 -> 94.228.133.235:80"
17-07-04T20:54:53.857525+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:50312 -> 23.194.141.50:80"
17-07-04T20:55:06.762094+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:44404 -> 50.116.194.21:80"
17-07-04T20:55:06.823720+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:44803 -> 69.28.157.169:80"
17-07-04T20:54:53.871397+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:51450 -> 52.84.59.171:80"
17-07-04T20:55:08.046063+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:55164 -> 37.157.4.15:80"
17-07-04T20:55:09.400280+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:37251 -> 23.50.75.27:80"
17-07-04T20:54:54.054473+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:54659 -> 172.217.11.14:80"
17-07-04T20:55:09.781948+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:34045 -> 192.35.249.123:80"
17-07-04T20:54:54.293371+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:50312 -> 23.194.141.50:80"
17-07-04T20:53:20.757051+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.15:59575 -> 54.192.39.67:80"
17-07-04T20:55:36.070495+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:37688 -> 172.217.11.14:80"
17-07-04T20:55:36.389611+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:55126 -> 23.60.139.27:80"
17-07-04T20:53:22.007388+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.15:59572 -> 104.16.21.35:80"
17-07-04T20:53:22.024415+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.15:59593 -> 104.16.21.35:80"
17-07-04T20:55:36.578608+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:55126 -> 23.60.139.27:80"
17-07-04T20:55:36.615252+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:51278 -> 178.255.83.1:80"
17-07-04T20:55:36.618314+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:55126 -> 23.60.139.27:80"
17-07-04T20:55:36.741121+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:55126 -> 23.60.139.27:80"
17-07-04T20:55:36.741931+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:37688 -> 172.217.11.14:80"
17-07-04T20:53:22.302964+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.15:59593 -> 104.16.21.35:80"
17-07-04T20:55:36.841096+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:37688 -> 172.217.11.14:80"
17-07-04T20:54:54.612833+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:54659 -> 172.217.11.14:80"
17-07-04T20:54:54.653241+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.19:33334 -> 23.194.140.205:80"
17-07-04T20:55:37.249698+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:37688 -> 172.217.11.14:80"
17-07-04T20:55:38.020383+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:37688 -> 172.217.11.14:80"
17-07-04T20:54:54.846841+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.17:39693 -> 172.217.11.14:80"
17-07-04T20:55:38.735212+0100 | 1:1000005:1 | Bot Activity - Basic Detection |  | 192.168.10.12:37688 -> 172.217.11.14:80"
```

#vieing alerts in evebox

```
2023-08-08 23:12:47  INFO evebox::server::main: Using temporary in-memory configuration database
2023-08-08 23:12:47  INFO refinery_core::traits: schema history table is empty, going to apply all migrations
2023-08-08 23:12:47  INFO refinery_core::traits::sync: applying migration: V1__Initial
2023-08-08 23:12:47  INFO evebox::server::main: Starting Axum server on 127.0.0.1:5636
2023-08-08 23:12:47  INFO evebox::commands::oneshot: Server started at http://127.0.0.1:5636
2023-08-08 23:12:47 ERROR evebox::commands::oneshot: Failed to open http://127.0.0.1:5636 in browser: No valid browsers detected.
2023-08-08 23:12:47  INFO evebox::commands::oneshot: If your browser didn't open, try connecting to http://127.0.0.1:5636
```

Alerts 1-100 of 21413

Newest Newer Older

#	Timestamp	Src / Dst	Signature	
1084	2017-07-07 21:02:33 6 years ago	S: fe80::266e:96ff:fe4a:377a D: ff02::00fb	SURICATA UDPv6 invalid checksum	Archive
1816	2017-07-07 21:02:31 6 years ago	S: fe80::266e:96ff:fe4a:377a D: ff02::0001	SURICATA UDPv6 invalid checksum	Archive
39	2017-07-07 21:02:20 6 years ago	S: 192.168.10.8 D: 184.84.243.218	Bot Activity - Basic Detection http	Archive
7	2017-07-07 21:02:14 6 years ago	S: 23.208.94.86 D: 192.168.10.15	SURICATA STREAM CLOSEWAIT FIN out of window http	Archive
9	2017-07-07 21:02:10 6 years ago	S: 192.168.10.12 D: 23.63.226.81	Bot Activity - Basic Detection http	Archive
7	2017-07-07 21:02:09 6 years ago	S: 52.84.145.230 D: 192.168.10.12	ET INFO TLS Handshake Failure tls	Archive
869	2017-07-07 21:01:51 6 years ago	S: 192.168.10.8 D: 192.168.10.3	SURICATA STREAM CLOSEWAIT FIN out of window krb5	Archive
1613	2017-07-07 21:01:45 6 years ago	S: 192.168.10.3 D: 192.168.10.17	SURICATA Kerberos 5 weak encryption parameters krb5	Archive
469	2017-07-07 21:01:45 6 years ago	S: 192.168.10.3 D: 192.168.10.17	SURICATA TLS invalid record type tls	Archive
469	2017-07-07 21:01:45 6 years ago	S: 192.168.10.17 D: 192.168.10.3	SURICATA TLS invalid record type tls	Archive
30	2017-07-07 21:01:30 6 years ago	S: 192.168.10.12 D: 136.243.33.19	Bot Activity - Basic Detection http	Archive
2919	2017-07-07 21:01:22	S: 192.168.10.25	SURICATA Applayer Detect protocol only one direction smb	Archive