



LAB :: Install Suricata

- # super user command.
- \$ normal user command.
- Username `apnic` and password `training`.

Topology

```
[group1.apnictraining.net] [192.168.30.1]
[group2.apnictraining.net] [192.168.30.2]
.....
[group10.apnictraining.net] [192.168.30.10]
[group11.apnictraining.net] [192.168.30.11]
.....
[group20.apnictraining.net] [192.168.30.20]
[group21.apnictraining.net] [192.168.30.21]
.....
[group30.apnictraining.net] [192.168.30.30]
```

In this lab you will be installing and configuring Suricata Intrusion Detection System (IDS).

Prerequisites Knowledge of Ubuntu, linux commands, Intrusion Detection Systems.

Lab Tasks

Step 1: Update Ubuntu software

Step 2: Install pre-requisite software

Step 3: Install Suricata

Step 4: Install EveBox

Step 5: Review Suricata configuration

Part 1. Installation

1. Login to the server.

```
ssh apnic@192.168.30.XX
```

Password is `training`

2. Install pre-requisite software

```
sudo apt-get update  
sudo apt-get install -y nano jq software-properties-common
```

Password is

3. Add the Suricata installation repository

```
sudo add-apt-repository ppa:oisf/suricata-stable
```

```
apnic@suricata: ~  
File Edit View Search Terminal Help  
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...  
apnic@suricata:~$ sudo add-apt-repository ppa:oisf/suricata-stable  
Suricata IDS/IPS/NSM stable packages  
http://www.openinfosecfoundation.org/  
http://planet.suricata-ids.org/  
http://suricata-ids.org/  
  
Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.  
  
Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community.  
  
This Engine supports:  
  
- Multi-Threading - provides for extremely fast and flexible operation on multi-core systems.  
- Multi Tenancy - Per vlan/Per interface  
- Uses Rust for most protocol detection/parsing  
- TLS/SSL certificate matching/logging  
- JA3 TLS client fingerprinting  
  
- VXLAN support  
- All JSON output/logging capability  
- IDS runmode  
- IPS runmode  
- IDPS runmode  
- NSM runmode  
- eBPF/XDP  
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRBS, DHCP, IKEv2, SNMP, SIP, RDP  
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS  
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.  
- File MD5/SHA1/SHA256 matching  
- Gzip Decompression  
- Fast IP Matching  
- Datasets matching  
- Rustlang enabled protocol detection  
- Lua scripting  
  
and many more great features -  
http://suricata-ids.org/features/all-features/  
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable  
Press [ENTER] to continue or Ctrl-c to cancel adding it.
```

4. Install Suricata.

```
sudo apt-get update  
sudo apt-get install -y suricata
```

```
apnic@suricata: ~  
File Edit View Search Terminal Help  
Hit:6 http://192.168.30.248:3142/ubuntu focal-security InRelease  
Fetched 20.1 kB in 1s (13.8 kB/s)  
Reading package lists... Done  
apnic@suricata:~$ sudo apt-get update  
Hit:1 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal InRelease  
Hit:2 http://192.168.30.248:3142/ubuntu focal InRelease  
Hit:3 http://192.168.30.248:3142/ubuntu focal-updates InRelease  
Hit:4 http://192.168.30.248:3142/ubuntu focal-security InRelease  
Reading package lists... Done  
apnic@suricata:~$ sudo apt-get install -y suricata  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14  
  libhttp2 libhyperscan5 libjansson4 liblua5.1-2 liblua5.1-common  
  liblzma-dev libmaxminddb0 libnet1 libnetfilter-queue1 libnfnetlink0 libnspr4  
  libnss3 libpcap0.8  
Suggested packages:  
  liblzma-doc mmdns-bin  
The following NEW packages will be installed:  
  libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14  
  libhttp2 libhyperscan5 libjansson4 liblua5.1-2 liblua5.1-common  
  liblzma-dev libmaxminddb0 libnet1 libnetfilter-queue1 libnfnetlink0 libnspr4
```

5. Install EveBox

```
mkdir Downloads  
cd Downloads  
wget https://evebox.org/files/release/0.14.0/evebox_0.14.0_amd64.deb  
sudo dpkg -i evebox_0.14.0_amd64.deb
```

```
apnic@suricata:~$ mkdir Downloads  
cdapnic@suricata:~$ cd Downloads  
apnic@suricata:~/Downloads$ wget https://evebox.org/files/release/0.14.0/evebox_0.14.0_amd64.deb  
sudo dpkg --2021-07-26 03:29:40-- https://evebox.org/files/release/0.14.0/evebox_0.14.0_amd64.deb  
-i eveResolving evebox.org (evebox.org)... box_0.14.0_amd64.deb172.105.5.173  
Connecting to evebox.org (evebox.org)|172.105.5.173|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 7899390 (7.5M) [application/vnd.debian.binary-package]  
Saving to: 'evebox_0.14.0_amd64.deb'  
  
evebox_0.14.0_amd64 100%[=====>] 7.53M 16.0MB/s in 0.5s  
  
2021-07-26 03:29:41 (16.0 MB/s) - 'evebox_0.14.0_amd64.deb' saved [7899390/7899390]  
apnic@suricata:~/Downloads$ sudo dpkg -i evebox 0.14.0 amd64.deb
```

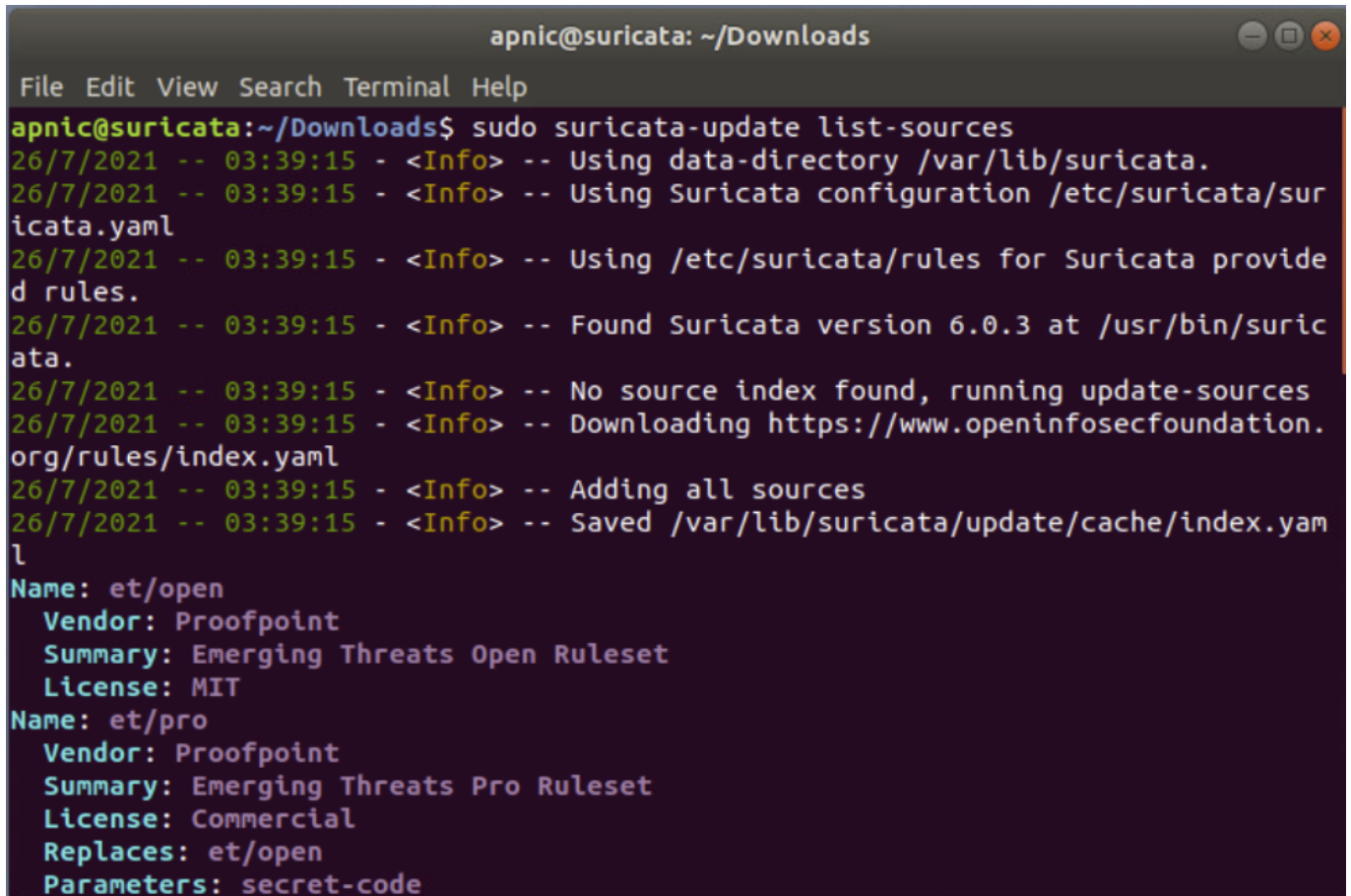
NOTE: Refer to the website for the latest version <https://evebox.org/files/release/latest/>

6. Backup the Suricata configuration file.

```
sudo cp /etc/suricata/suricata.yaml /etc/suricata/suricata.yaml.bak
```

7. Update the Suricata signatures/rules used for detection.

```
sudo suricata-update list-sources
```



```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo suricata-update list-sources
26/7/2021 -- 03:39:15 - <Info> -- Using data-directory /var/lib/suricata.
26/7/2021 -- 03:39:15 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
26/7/2021 -- 03:39:15 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
26/7/2021 -- 03:39:15 - <Info> -- Found Suricata version 6.0.3 at /usr/bin/suricata.
26/7/2021 -- 03:39:15 - <Info> -- No source index found, running update-sources
26/7/2021 -- 03:39:15 - <Info> -- Downloading https://www.openinfosecfoundation.org/rules/index.yaml
26/7/2021 -- 03:39:15 - <Info> -- Adding all sources
26/7/2021 -- 03:39:15 - <Info> -- Saved /var/lib/suricata/update/cache/index.yaml
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
```

NOTE To see just the name of the listed sources

```
sudo suricata-update list-sources | grep Name
```

8. Enable the Suricata rules for identifying and classifying traffic.

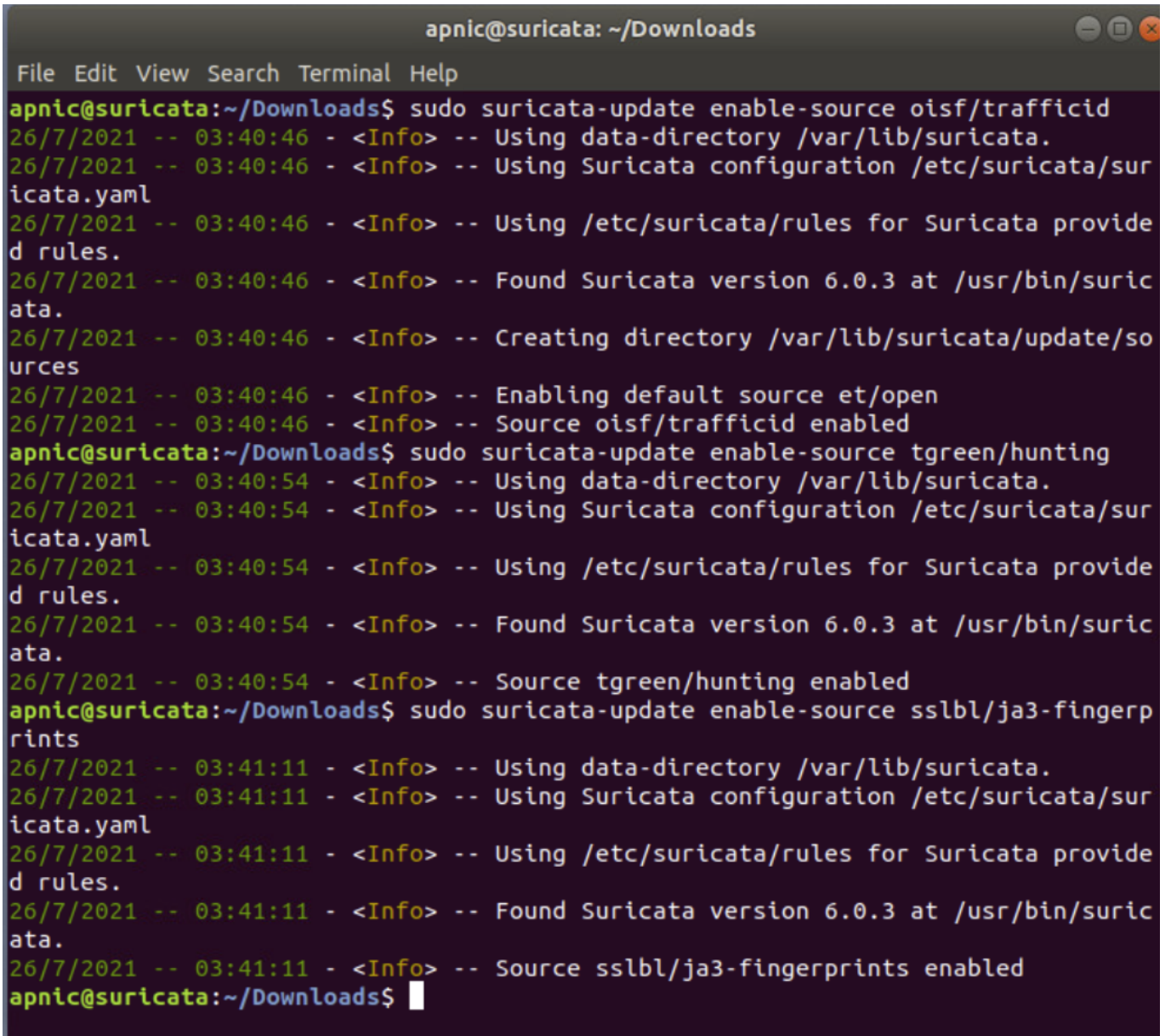
```
sudo suricata-update enable-source oisf/trafficid
```

9. Enable the Suricata rules for network anomaly detection.

```
sudo suricata-update enable-source tgreen/hunting
```

10. Enable the Suricata SSL Certificate Ruleset to detect and/or block malicious SSL connections based on the SSL certificate fingerprint.

```
sudo suricata-update enable-source sslbl/ja3-fingerprints
```

A terminal window titled 'apnic@suricata: ~/Downloads' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows three sequential commands to enable sources in Suricata. Each command is followed by several informational messages indicating the data directory, configuration file, rules, and the current Suricata version (6.0.3). The first command enables 'oisf/trafficid', the second 'tgreen/hunting', and the third 'sslbl/ja3-fingerprints'.

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo suricata-update enable-source oisf/trafficid
26/7/2021 -- 03:40:46 - <Info> -- Using data-directory /var/lib/suricata.
26/7/2021 -- 03:40:46 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
26/7/2021 -- 03:40:46 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
26/7/2021 -- 03:40:46 - <Info> -- Found Suricata version 6.0.3 at /usr/bin/suricata.
26/7/2021 -- 03:40:46 - <Info> -- Creating directory /var/lib/suricata/update/sources
26/7/2021 -- 03:40:46 - <Info> -- Enabling default source et/open
26/7/2021 -- 03:40:46 - <Info> -- Source oisf/trafficid enabled
apnic@suricata:~/Downloads$ sudo suricata-update enable-source tgreen/hunting
26/7/2021 -- 03:40:54 - <Info> -- Using data-directory /var/lib/suricata.
26/7/2021 -- 03:40:54 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
26/7/2021 -- 03:40:54 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
26/7/2021 -- 03:40:54 - <Info> -- Found Suricata version 6.0.3 at /usr/bin/suricata.
26/7/2021 -- 03:40:54 - <Info> -- Source tgreen/hunting enabled
apnic@suricata:~/Downloads$ sudo suricata-update enable-source sslbl/ja3-fingerprints
26/7/2021 -- 03:41:11 - <Info> -- Using data-directory /var/lib/suricata.
26/7/2021 -- 03:41:11 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
26/7/2021 -- 03:41:11 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
26/7/2021 -- 03:41:11 - <Info> -- Found Suricata version 6.0.3 at /usr/bin/suricata.
26/7/2021 -- 03:41:11 - <Info> -- Source sslbl/ja3-fingerprints enabled
apnic@suricata:~/Downloads$
```

11. List enabled sources for rule updates.

```
sudo suricata-update list-enabled-sources
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo suricata-update list-enabled-sources
26/7/2021 -- 03:42:45 - <Info> -- Using data-directory /var/lib/suricata.
26/7/2021 -- 03:42:45 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
26/7/2021 -- 03:42:45 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
26/7/2021 -- 03:42:45 - <Info> -- Found Suricata version 6.0.3 at /usr/bin/suricata.
Enabled sources:
- tgreen/hunting
- et/open
- sslbl/ja3-fingerprints
- oisf/trafficid
apnic@suricata:~/Downloads$
```

12. Update the signature/rules.

```
sudo suricata-update
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo suricata-update
26/7/2021 -- 03:43:38 - <Info> -- Using data-directory /var/lib/suricata.
26/7/2021 -- 03:43:38 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
26/7/2021 -- 03:43:38 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
26/7/2021 -- 03:43:38 - <Info> -- Found Suricata version 6.0.3 at /usr/bin/suricata.
26/7/2021 -- 03:43:38 - <Info> -- Loading /etc/suricata/suricata.yaml
26/7/2021 -- 03:43:38 - <Info> -- Disabling rules for protocol http2
26/7/2021 -- 03:43:38 - <Info> -- Disabling rules for protocol modbus
26/7/2021 -- 03:43:38 - <Info> -- Disabling rules for protocol dnp3
26/7/2021 -- 03:43:38 - <Info> -- Disabling rules for protocol enip
26/7/2021 -- 03:43:38 - <Info> -- Fetching https://openinfosecfoundation.org/rules/trafficid/trafficid.rules.
100% - 9855/9855
26/7/2021 -- 03:43:38 - <Info> -- Done.
26/7/2021 -- 03:43:38 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-6.0.3/emerging.rules.tar.gz.
100% - 2960372/2960372
26/7/2021 -- 03:43:39 - <Info> -- Done.
26/7/2021 -- 03:43:39 - <Info> -- Fetching https://raw.githubusercontent.com/tgreen/hunting-rules/master/hunting.rules.
100% - 62241/62241
26/7/2021 -- 03:43:39 - <Info> -- Done.
26/7/2021 -- 03:43:39 - <Info> -- Fetching https://sslbl.abuse.ch/blacklist/ja3-fingerprints.rules.
100% - 26236/26236
26/7/2021 -- 03:43:39 - <Info> -- Done.
26/7/2021 -- 03:43:39 - <Info> -- Loading distribution rule file /etc/suricata/r
```

```
26/7/2021 -- 03:43:39 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
26/7/2021 -- 03:43:39 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
26/7/2021 -- 03:43:39 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
26/7/2021 -- 03:43:39 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
26/7/2021 -- 03:43:39 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
26/7/2021 -- 03:43:39 - <Info> -- Ignoring file rules/emerging-deleted.rules
26/7/2021 -- 03:43:41 - <Info> -- Loaded 30526 rules.
26/7/2021 -- 03:43:42 - <Info> -- Disabled 14 rules.
26/7/2021 -- 03:43:42 - <Info> -- Enabled 0 rules.
26/7/2021 -- 03:43:42 - <Info> -- Modified 0 rules.
26/7/2021 -- 03:43:42 - <Info> -- Dropped 0 rules.
26/7/2021 -- 03:43:42 - <Info> -- Enabled 130 rules for flowbit dependencies.
26/7/2021 -- 03:43:42 - <Info> -- Creating directory /var/lib/suricata/rules.
26/7/2021 -- 03:43:42 - <Info> -- Backing up current rules.
26/7/2021 -- 03:43:42 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 30526; enabled: 23159; added: 30526; removed 0; modified: 0
26/7/2021 -- 03:43:42 - <Info> -- Writing /var/lib/suricata/rules/classification.config
26/7/2021 -- 03:43:42 - <Info> -- Testing with suricata -T.
26/7/2021 -- 03:44:08 - <Info> -- Done.
apnic@suricata:~/Downloads$
```

Part 2. Review the Suricata configuration

1. To determine the network address used by Suricata, review the variable called **\$HOME_NET** in the **suricata.yaml** file.

```
grep -n HOME_NET /etc/suricata/suricata.yaml
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
Adding new user `evebox' (UID 107) with group `evebox' ...
Creating home directory `/var/lib/evebox' ...
apnic@suricata:~/Downloads$ sudo cp /etc/suricata/suricata.yaml /etc/suricata/suricata.yaml.bak
apnic@suricata:~/Downloads$ grep -n HOME_NET /etc/suricata/suricata.yaml
15: HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
16: #HOME_NET: "[192.168.0.0/16]"
17: #HOME_NET: "[10.0.0.0/8]"
18: #HOME_NET: "[172.16.0.0/12]"
19: #HOME_NET: "any"
21: EXTERNAL_NET: "!$HOME_NET"
24: HTTP_SERVERS: "$HOME_NET"
25: SMTP_SERVERS: "$HOME_NET"
26: SQL_SERVERS: "$HOME_NET"
27: DNS_SERVERS: "$HOME_NET"
28: TELNET_SERVERS: "$HOME_NET"
30: DC_SERVERS: "$HOME_NET"
31: DNP3_SERVER: "$HOME_NET"
32: DNP3_CLIENT: "$HOME_NET"
33: MODBUS_CLIENT: "$HOME_NET"
34: MODBUS_SERVER: "$HOME_NET"
35: ENIP_CLIENT: "$HOME_NET"
36: ENIP_SERVER: "$HOME_NET"
apnic@suricata:~/Downloads$
```

2. Review the variable called **default-rule-path** to determine the path where the rules are stored by Suricata.

```
grep -A 4 -n 'default-rule-path' /etc/suricata/suricata.yaml
```

3. Review the variable **af-packet** to determine which interface suricata will listen for traffic.

```
grep -A 1 -n 'af-packet' /etc/suricata/suricata.yaml
```

4. Review the variable **file-store** to see what storage format is used.

```
grep -A 2 -n 'file-store' /etc/suricata/suricata.yaml
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
27:  DNS_SERVERS: "$HOME_NET"
28:  TELNET_SERVERS: "$HOME_NET"
30:  DC_SERVERS: "$HOME_NET"
31:  DNP3_SERVER: "$HOME_NET"
32:  DNP3_CLIENT: "$HOME_NET"
33:  MODBUS_CLIENT: "$HOME_NET"
34:  MODBUS_SERVER: "$HOME_NET"
35:  ENIP_CLIENT: "$HOME_NET"
36:  ENIP_SERVER: "$HOME_NET"
apnic@suricata:~/Downloads$ grep -A 4 -n 'default-rule-path' /etc/suricata/suricata.yaml
1870: default-rule-path: /var/lib/suricata/rules
1871-
1872- rule-files:
1873-   - suricata.rules
1874-
apnic@suricata:~/Downloads$ grep -A 1 -n af-packet /etc/suricata/suricata.yaml
580: af-packet:
581-   - interface: eth0
apnic@suricata:~/Downloads$ grep -A 2 -n file-store /etc/suricata/suricata.yaml
445:   - file-store:
446-       version: 2
447-       enabled: no
apnic@suricata:~/Downloads$
```

Refer to the documentation for more detail <https://suricata.readthedocs.io/en/latest/quickstart.html>

5. View the downloaded rules.

```
sudo ls -lash /var/lib/suricata/rules
```

Password =

6. Display how many rules in the suricata.rules file.

```
sudo wc -l /var/lib/suricata/rules/suricata.rules
```

7. View the first 2 records of the suricata.rules file.

```
sudo head -n 2 /var/lib/suricata/rules/suricata.rules
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo ls -lash /var/lib/suricata/rules
total 17M
4.0K drwxr-x-- 2 root root 4.0K Jul 26 03:43 .
4.0K drwxr-xr-x 4 root root 4.0K Jul 26 03:43 ..
4.0K -rw-r--r-- 1 root root 3.2K Jul 26 03:43 classification.config
17M -rw-r--r-- 1 root root 17M Jul 26 03:43 suricata.rules
apnic@suricata:~/Downloads$ sudo wc -l /var/lib/suricata/rules/suricata.rules
30526 /var/lib/suricata/rules/suricata.rules
apnic@suricata:~/Downloads$ sudo head -n 2 /var/lib/suricata/rules/suricata.rules
alert ip any any -> any any (msg:"SURICATA Applayer Mismatch protocol both directions"; flow:established; app-layer-event:applayer_mismatch_protocol_both_directions; flowint:applayer.anomaly.count,+,1; classtype:protocol-command-decode; sid:2260000; rev:1;)
alert ip any any -> any any (msg:"SURICATA Applayer Wrong direction first Data"; flow:established; app-layer-event:applayer_wrong_direction_first_data; flowint:applayer.anomaly.count,+,1; classtype:protocol-command-decode; sid:2260001; rev:1;)
apnic@suricata:~/Downloads$
```

8. Count how many rules are for wannacry.

```
sudo grep wannacry /var/lib/suricata/rules/suricata.rules | wc -l
```

9. Display the rules for wannacry.

```
sudo grep -n wannacry /var/lib/suricata/rules/suricata.rules
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo grep -n wannacry /var/lib/suricata/rules/suricata.rules | wc -l
10
apnic@suricata:~/Downloads$ sudo grep -n wannacry /var/lib/suricata/rules/suricata.rules | more
9804:# alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2"; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HrI"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024299; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, malware_family wannacry, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18;)
9805:# alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4"; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HrI"; reference:cve,2017-0144; reference:url,w
```

Refer to the online documentation <https://suricata.readthedocs.io/en/suricata-6.0.3/rules/intro.html>

1. View the classifications for Suricata.

```
sudo head -n 2 /var/lib/suricata/rules/classification.config
```

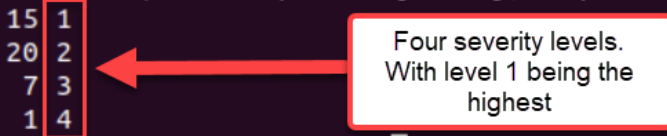
2. Display how many classifications for Suricata

```
sudo wc -l /var/lib/suricata/rules/classification.config
```

3. Display how many of each severity for the classifications

```
sudo cat /var/lib/suricata/rules/classification.config | cut -d "," -f 3 | \
awk '{ $1=$1 }; 1' | sort | uniq -c
```

```
apnic@suricata: ~/Downloads
File Edit View Search Terminal Help
apnic@suricata:~/Downloads$ sudo head -n 2 /var/lib/suricata/rules/classification
n.config
config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
apnic@suricata:~/Downloads$ sudo wc -l /var/lib/suricata/rules/classification.co
nfig
43 /var/lib/suricata/rules/classification.config
apnic@suricata:~/Downloads$ sudo cat /var/lib/suricata/rules/classification.conf
ig | cut -d "," -f 3 | awk '{ $1=$1 };1' | sort | uniq -c
15 1
20 2
7 3
1 4
```



Four severity levels.
With level 1 being the
highest

4. Confirm the status of Suricata.

```
sudo systemctl status suricata
```

Password =

Note: Press to quit from the status output.

END OF EXERCISE