IA612: Intrusion Detection and Prevention

St. Cloud State University

LAB-04: Suricata IDS/IPS Installation and Configuration

Sample LAB Report

Section-01: Suricata Installation

Step 1: Initial Environmental Preparations

In order to install Suricata, we need to make sure all the packages that are required should be updated. So, we will proceed with installing the required dependencies

1) apt-get update –y

2) apt-get install rustc cargo make libpcre3 libpcre3-dbg libpcre3-dev build-essential autoconf automake libtool libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 make libmagic-dev libjansson-dev libjansson4 pkg-config –y

3) apt-get install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0 –y

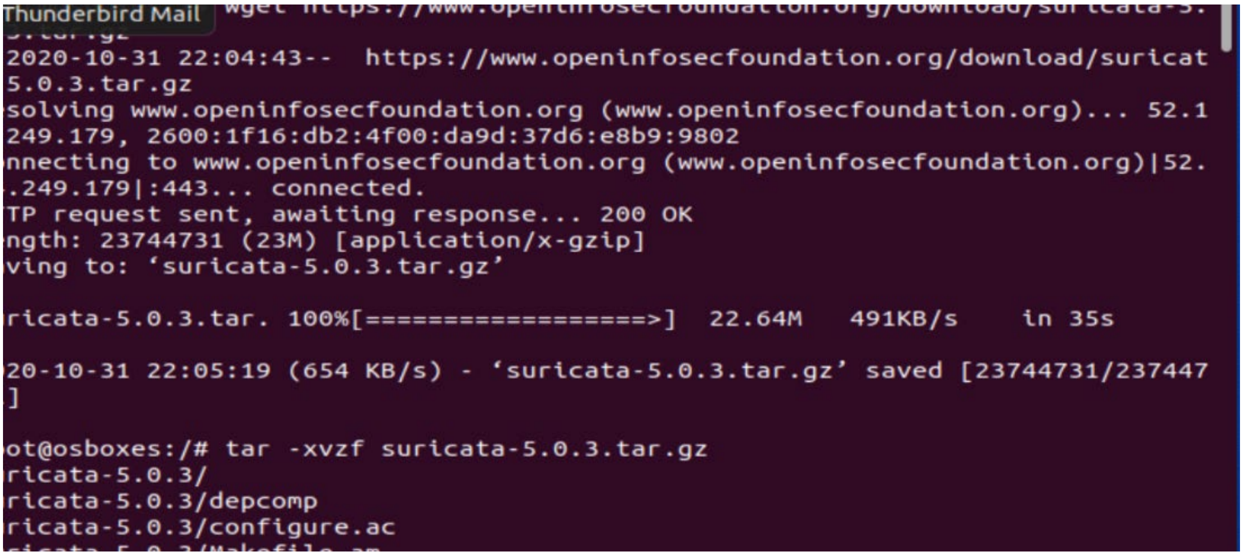
4) apt-get install python3-pip5) pip3 install --upgrade suricata-update6)ln -s /usr/local/bin/suricata-update /usr/bin/suricata-update

By this step we have all required dependencies for suricata

Step 2: Downloading the Suricata File

1)wget https://www.openinfosecfoundation.org/download/suricata-5.0.3.tar.gz

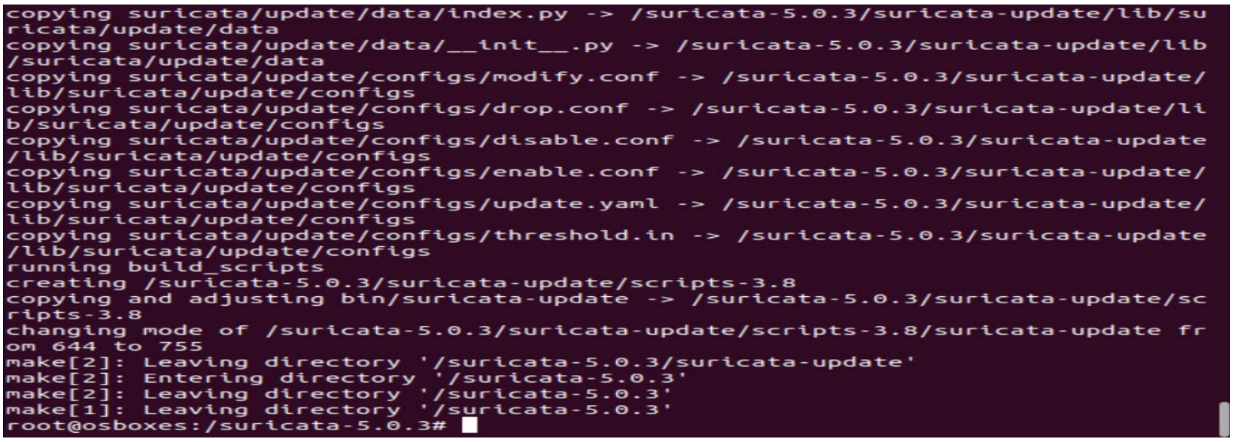
2) Extract the file: tar -xvzf suricata-5.0.3.tar.gz



```
 wget https://www.openinfosecfoundation.org/download/suricata-5.
5.tar.gz
2020-10-31 22:04:43--  https://www.openinfosecfoundation.org/download/suricat
5.0.3.tar.gz
solving www.openinfosecfoundation.org (www.openinfosecfoundation.org)... 52.1
249.179, 2600:1f16:db2:4f00:da9d:37d6:e8b9:9802
nnecting to www.openinfosecfoundation.org (www.openinfosecfoundation.org)|52.
.249.179|:443... connected.
TP request sent, awaiting response... 200 OK
ngth: 23744731 (23M) [application/x-gzip]
ving to: ‘suricata-5.0.3.tar.gz’

ricata-5.0.3.tar. 100%[===================>]  22.64M   491KB/s    in 35s

20-10-31 22:05:19 (654 KB/s) - ‘suricata-5.0.3.tar.gz’ saved [23744731/237447
]

ot@osboxes:/# tar -xvzf suricata-5.0.3.tar.gz
ricata-5.0.3/
ricata-5.0.3/depcomp
ricata-5.0.3/configure.ac
```

3) Changing the directory : cd suricata-5.0.34) ./configure --enable-nfqueue --prefix=/usr --sysconfdir=/

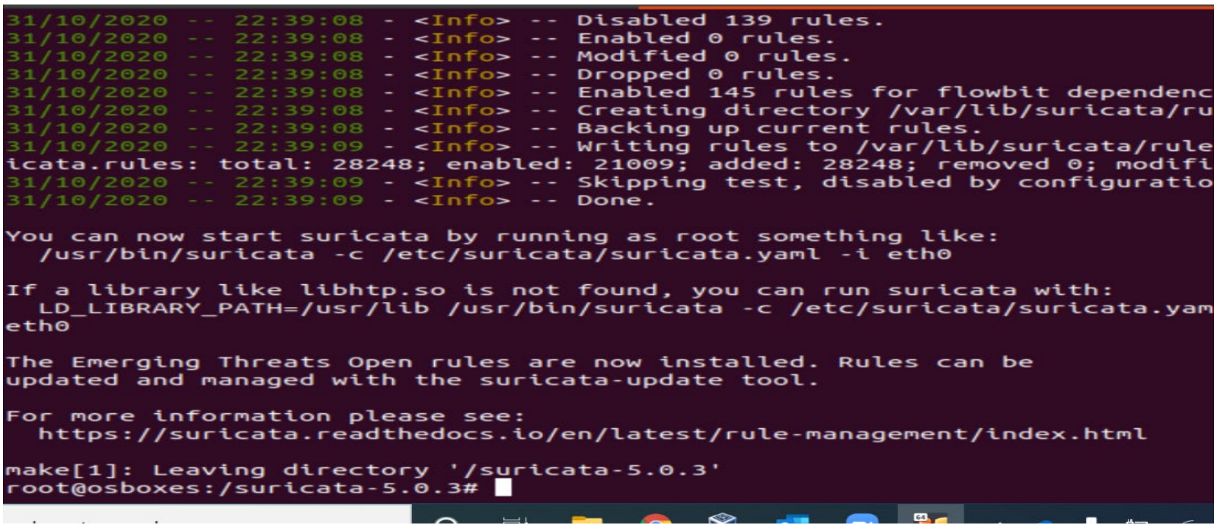
5) make



```
copying suricata/update/data/index.py -> /suricata-5.0.3/suricata-update/lib/su
ricata/update/data
copying suricata/update/data/__init__.py -> /suricata-5.0.3/suricata-update/lib
/suricata/update/data
copying suricata/update/configs/modify.conf -> /suricata-5.0.3/suricata-update/
lib/suricata/update/configs
copying suricata/update/configs/drop.conf -> /suricata-5.0.3/suricata-update/li
b/suricata/update/configs
copying suricata/update/configs/disable.conf -> /suricata-5.0.3/suricata-update
/lib/suricata/update/configs
copying suricata/update/configs/enable.conf -> /suricata-5.0.3/suricata-update/
lib/suricata/update/configs
copying suricata/update/configs/update.yaml -> /suricata-5.0.3/suricata-update/
lib/suricata/update/configs
copying suricata/update/configs/threshold.in -> /suricata-5.0.3/suricata-update
/lib/suricata/update/configs
running build_scripts
creating /suricata-5.0.3/suricata-update/scripts-3.8
copying and adjusting bin/suricata-update -> /suricata-5.0.3/suricata-update/sc
ripts-3.8
changing mode of /suricata-5.0.3/suricata-update/scripts-3.8/suricata-update fr
om 644 to 755
make[2]: Leaving directory '/suricata-5.0.3/suricata-update'
make[2]: Entering directory '/suricata-5.0.3'
make[2]: Leaving directory '/suricata-5.0.3'
make[1]: Leaving directory '/suricata-5.0.3'
root@osboxes:/suricata-5.0.3#
```

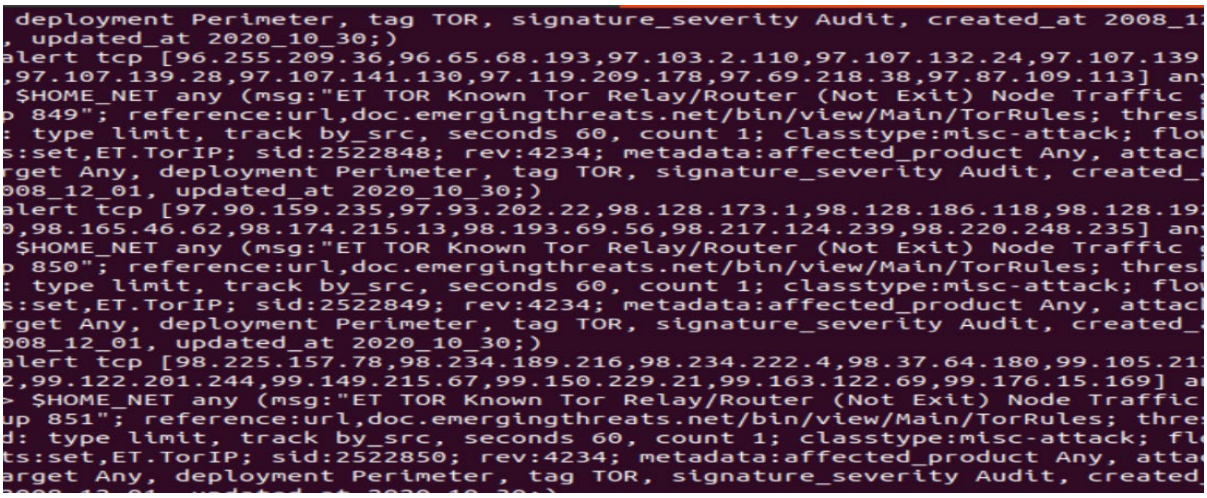
6) make install-full

7) make install-rules



```
31/10/2020 -- 22:39:08 - <Info> -- Disabled 139 rules.
31/10/2020 -- 22:39:08 - <Info> -- Enabled 0 rules.
31/10/2020 -- 22:39:08 - <Info> -- Modified 0 rules.
31/10/2020 -- 22:39:08 - <Info> -- Dropped 0 rules.
31/10/2020 -- 22:39:08 - <Info> -- Enabled 145 rules for flowbit dependenc
31/10/2020 -- 22:39:08 - <Info> -- Creating directory /var/lib/suricata/ru
31/10/2020 -- 22:39:08 - <Info> -- Backing up current rules.
31/10/2020 -- 22:39:09 - <Info> -- Writing rules to /var/lib/suricata/rule
icata.rules: total: 28248; enabled: 21009; added: 28248; removed 0; modifi
31/10/2020 -- 22:39:09 - <Info> -- Skipping test, disabled by configuratio
31/10/2020 -- 22:39:09 - <Info> -- Done.

You can now start suricata by running as root something like:
  /usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth0

If a library like libhtp.so is not found, you can run suricata with:
  LD_LIBRARY_PATH=/usr/lib /usr/bin/suricata -c /etc/suricata/suricata.yam
eth0

The Emerging Threats Open rules are now installed. Rules can be
updated and managed with the suricata-update tool.

For more information please see:
  https://suricata.readthedocs.io/en/latest/rule-management/index.html

make[1]: Leaving directory '/suricata-5.0.3'
root@osboxes:/suricata-5.0.3#
```

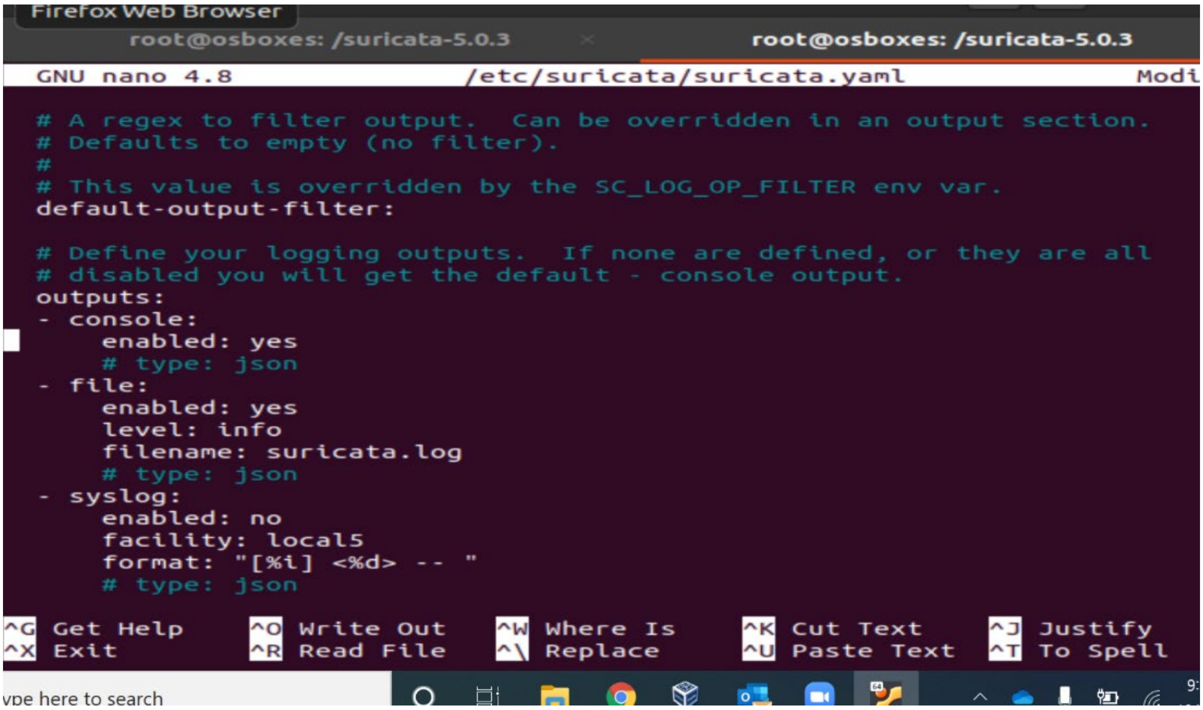
8) cat /var/lib/suricata/rules/suricata.rules



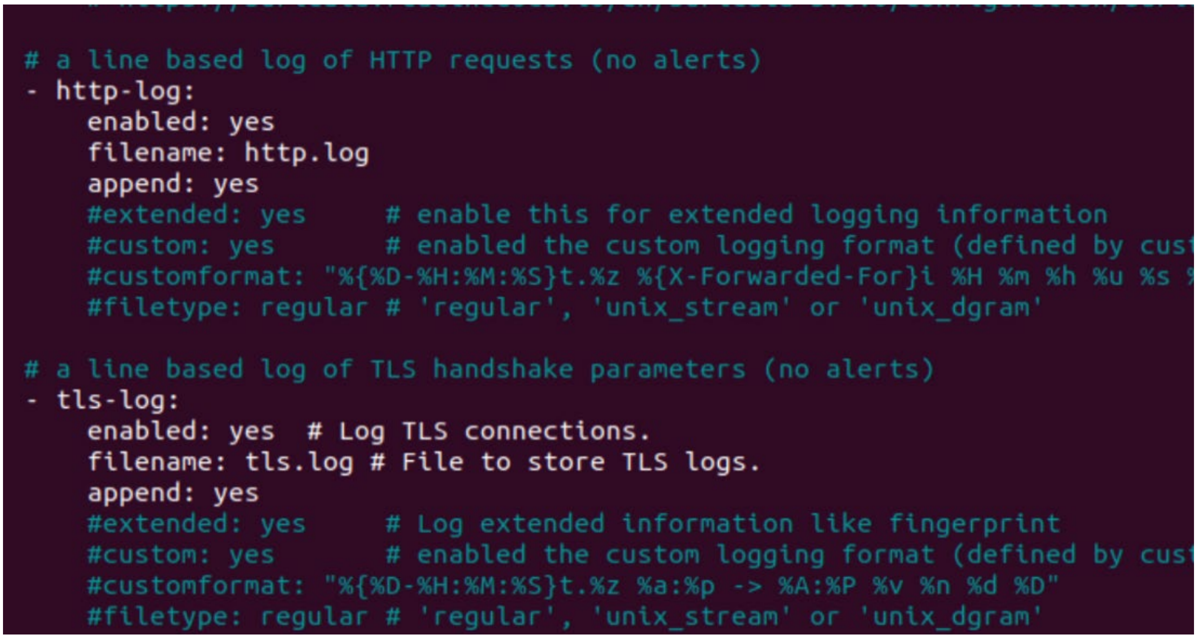
```
 deployment Perimeter, tag TOR, signature_severity Audit, created_at 2008_1
, updated_at 2020_10_30;)
alert tcp [96.255.209.36,96.65.68.193,97.103.2.110,97.107.132.24,97.107.139
,97.107.139.28,97.107.141.130,97.119.209.178,97.69.218.38,97.87.109.113] an
 $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit) Node Traffic
p 849"; reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; thres
: type limit, track by_src, seconds 60, count 1; classtype:misc-attack; flo
s:set,ET.TorIP; sid:2522848; rev:4234; metadata:affected_product Any, attac
rget Any, deployment Perimeter, tag TOR, signature_severity Audit, created_
008_12_01, updated_at 2020_10_30;)
alert tcp [97.90.159.235,97.93.202.22,98.128.173.1,98.128.186.118,98.128.19
9,98.165.46.62,98.174.215.13,98.193.69.56,98.217.124.239,98.220.248.235] an
 $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit) Node Traffic
p 850"; reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; thres
: type limit, track by_src, seconds 60, count 1; classtype:misc-attack; flo
s:set,ET.TorIP; sid:2522849; rev:4234; metadata:affected_product Any, attac
rget Any, deployment Perimeter, tag TOR, signature_severity Audit, created_
008_12_01, updated_at 2020_10_30;)
alert tcp [98.225.157.78,98.234.189.216,98.234.222.4,98.37.64.180,99.105.21
2,99.122.201.244,99.149.215.67,99.150.229.21,99.163.122.69,99.176.15.169] a
> $HOME_NET any (msg:"ET TOR Known Tor Relay/Router (Not Exit) Node Traffic
up 851"; reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; thre
d: type limit, track by_src, seconds 60, count 1; classtype:misc-attack; fl
ts:set,ET.TorIP; sid:2522850; rev:4234; metadata:affected_product Any, atta
arget Any, deployment Perimeter, tag TOR, signature_severity Audit, created
```

Section-02: Configuring and testing Suricata

1. “suricata.yaml” file is updated as shown below .Logging is enabled. Console log, syslog and http-log are all configured appropriately.



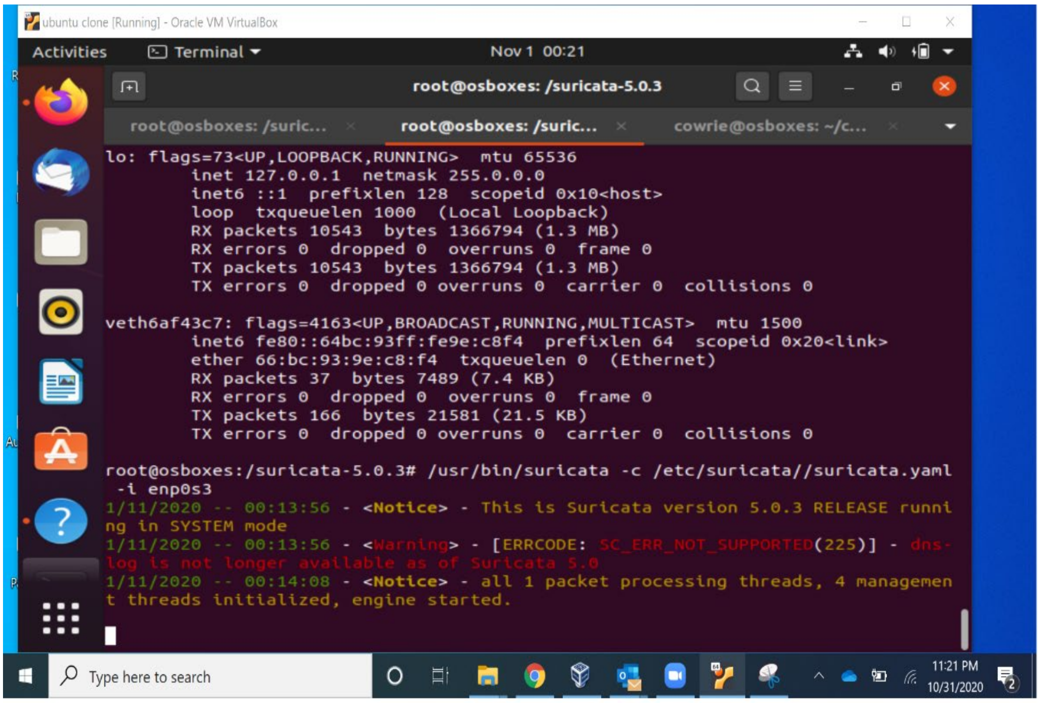
```
  GNU nano 4.8              /etc/suricata/suricata.yaml              Modi

  # A regex to filter output.  Can be overridden in an output section.
  # Defaults to empty (no filter).
  #
  # This value is overridden by the SC_LOG_OP_FILTER env var.
  default-output-filter:

  # Define your logging outputs.  If none are defined, or they are all
  # disabled you will get the default - console output.
  outputs:
  - console:
      enabled: yes
      # type: json
  - file:
      enabled: yes
      level: info
      filename: suricata.log
      # type: json
  - syslog:
      enabled: no
      facility: local5
      format: "[%i] <%d> -- "
      # type: json

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell
```



```
# a line based log of HTTP requests (no alerts)
- http-log:
    enabled: yes
    filename: http.log
    append: yes
    #extended: yes     # enable this for extended logging information
    #custom: yes       # enabled the custom logging format (defined by cust
    #customformat: "%{%D-%H:%M:%S}t.%z %{X-Forwarded-For}i %H %m %h %u %s %
    #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

# a line based log of TLS handshake parameters (no alerts)
- tls-log:
    enabled: yes  # Log TLS connections.
    filename: tls.log # File to store TLS logs.
    append: yes
    #extended: yes     # Log extended information like fingerprint
    #custom: yes       # enabled the custom logging format (defined by cust
    #customformat: "%{%D-%H:%M:%S}t.%z %a:%p -> %A:%P %v %n %d %D"
    #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
```

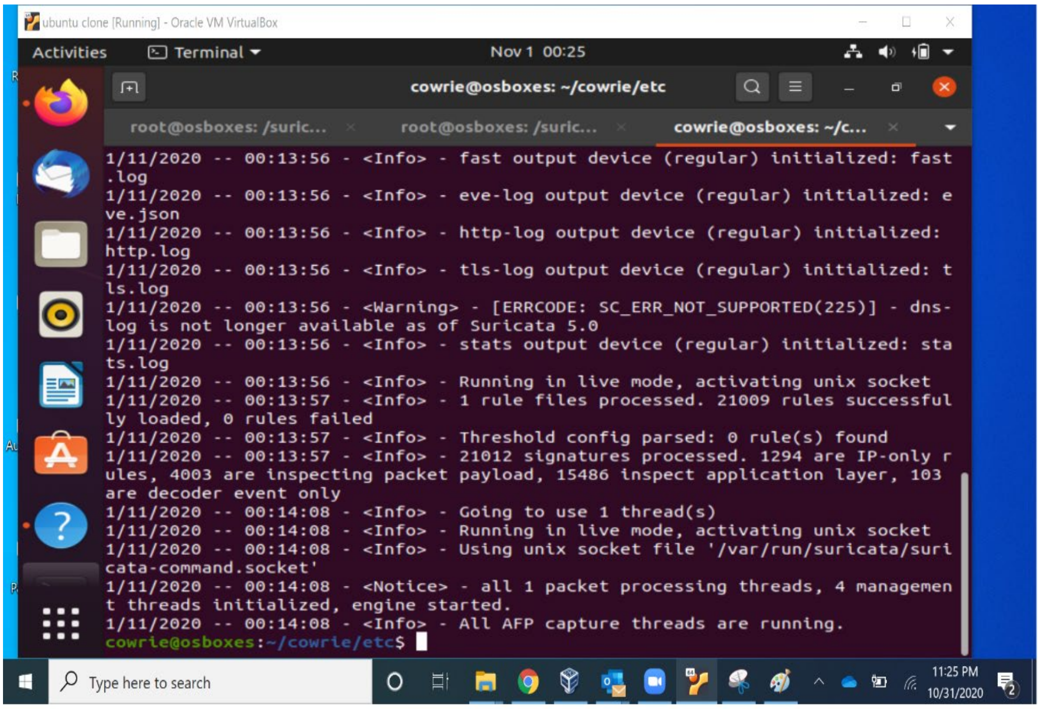
2. Starting suricata with the update suricata.yaml file .

Below screenshot shows engine is started I.e suricata service is running.It also mentions the suricata version being used . We come to know that dns.log is not supported by suricata 5.0.3



```
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 10543  bytes 1366794 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10543  bytes 1366794 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth6af43c7: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::64bc:93ff:fe9e:c8f4  prefixlen 64  scopeid 0x20<link>
        ether 66:bc:93:9e:c8:f4  txqueuelen 0  (Ethernet)
        RX packets 37  bytes 7489 (7.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 166  bytes 21581 (21.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@osboxes:/suricata-5.0.3# /usr/bin/suricata -c /etc/suricata//suricata.yaml
 -i enp0s3
1/11/2020 -- 00:13:56 - <Notice> - This is Suricata version 5.0.3 RELEASE runni
ng in SYSTEM mode
1/11/2020 -- 00:13:56 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)] - dns-
log is not longer available as of Suricata 5.0
1/11/2020 -- 00:14:08 - <Notice> - all 1 packet processing threads, 4 managemen
t threads initialized, engine started.
```

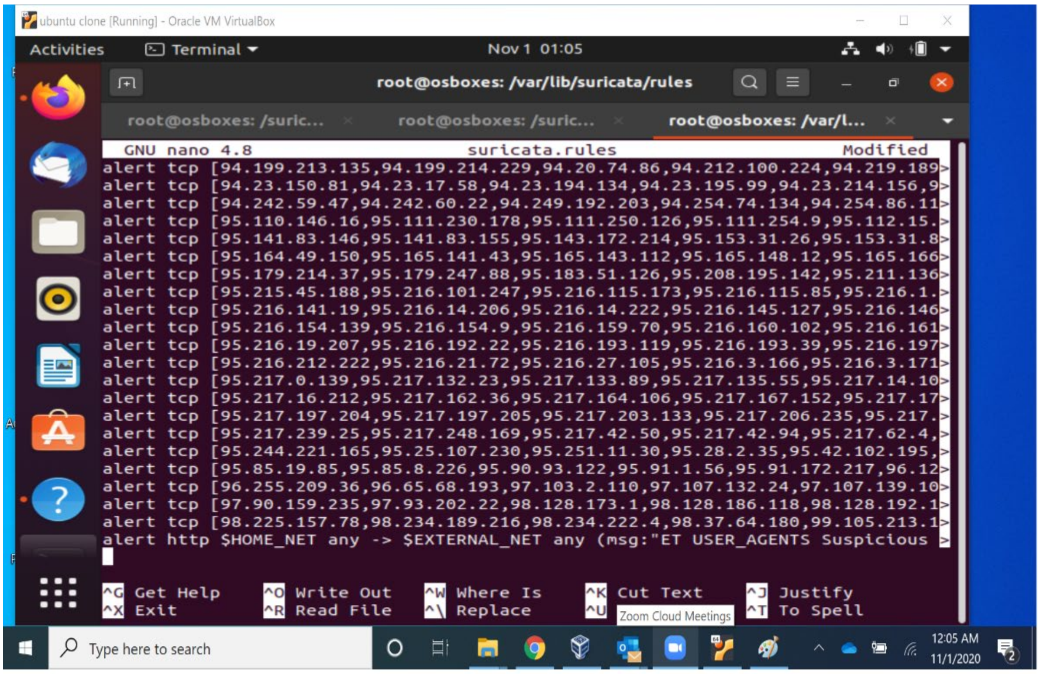
3. Below is the screenshot of suricata.log once the suricata service is started.



```
1/11/2020 -- 00:13:56 - <Info> - fast output device (regular) initialized: fast
.log
1/11/2020 -- 00:13:56 - <Info> - eve-log output device (regular) initialized: e
ve.json
1/11/2020 -- 00:13:56 - <Info> - http-log output device (regular) initialized:
http.log
1/11/2020 -- 00:13:56 - <Info> - tls-log output device (regular) initialized: t
ls.log
1/11/2020 -- 00:13:56 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)] - dns-
log is not longer available as of Suricata 5.0
1/11/2020 -- 00:13:56 - <Info> - stats output device (regular) initialized: sta
ts.log
1/11/2020 -- 00:13:56 - <Info> - Running in live mode, activating unix socket
1/11/2020 -- 00:13:57 - <Info> - 1 rule files processed. 21009 rules successful
ly loaded, 0 rules failed
1/11/2020 -- 00:13:57 - <Info> - Threshold config parsed: 0 rule(s) found
1/11/2020 -- 00:13:57 - <Info> - 21012 signatures processed. 1294 are IP-only r
ules, 4003 are inspecting packet payload, 15486 inspect application layer, 103
are decoder event only
1/11/2020 -- 00:14:08 - <Info> - Going to use 1 thread(s)
1/11/2020 -- 00:14:08 - <Info> - Running in live mode, activating unix socket
1/11/2020 -- 00:14:08 - <Info> - Using unix socket file '/var/run/suricata/suri
cata-command.socket'
1/11/2020 -- 00:14:08 - <Notice> - all 1 packet processing threads, 4 managemen
t threads initialized, engine started.
1/11/2020 -- 00:14:08 - <Info> - All AFP capture threads are running.
cowrie@osboxes:~/cowrie/etc$
```

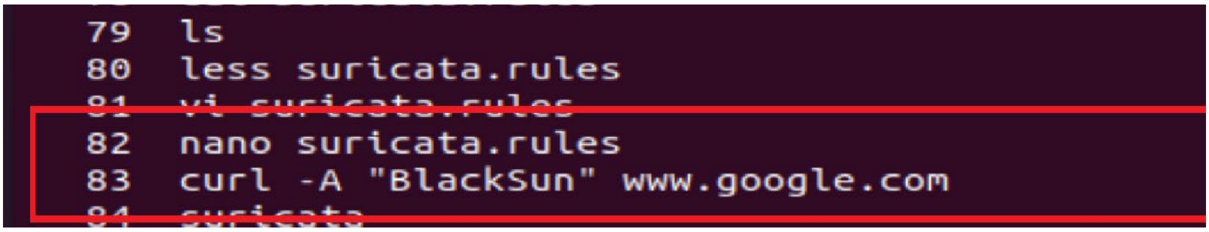
4. Below steps are performed to verify suricata whether it is saving log when a signature is matched.

a. The rules file is updated with a new rule which matches against known-bad user-agent. An alert is generated when a http request is received with user agent “BlackSun”



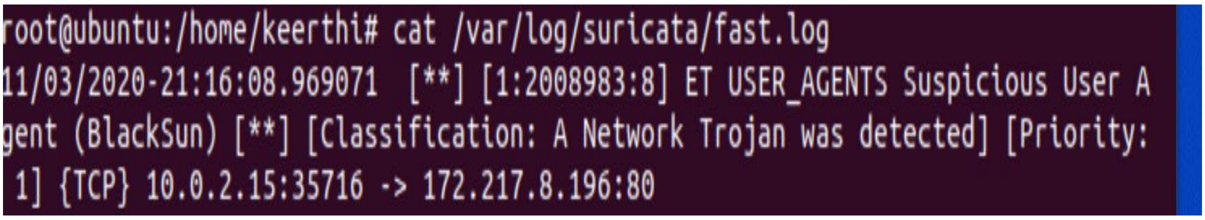
```
  GNU nano 4.8                     suricata.rules                     Modified
alert tcp [94.199.213.135,94.199.214.229,94.20.74.86,94.212.100.224,94.219.189>
alert tcp [94.23.150.81,94.23.17.58,94.23.194.134,94.23.195.99,94.23.214.156,9>
alert tcp [94.242.59.47,94.242.60.22,94.249.192.203,94.254.74.134,94.254.86.11>
alert tcp [95.110.146.16,95.111.230.178,95.111.250.126,95.111.254.9,95.112.15.>
alert tcp [95.141.83.146,95.141.83.155,95.143.172.214,95.153.31.26,95.153.31.8>
alert tcp [95.164.49.150,95.165.141.43,95.165.143.112,95.165.148.12,95.165.166>
alert tcp [95.179.214.37,95.179.247.88,95.183.51.126,95.208.195.142,95.211.136>
alert tcp [95.215.45.188,95.216.101.247,95.216.115.173,95.216.115.85,95.216.1.>
alert tcp [95.216.141.19,95.216.14.206,95.216.14.222,95.216.145.127,95.216.146>
alert tcp [95.216.154.139,95.216.154.9,95.216.159.70,95.216.160.102,95.216.161>
alert tcp [95.216.19.207,95.216.192.22,95.216.193.119,95.216.193.39,95.216.197>
alert tcp [95.216.212.222,95.216.21.72,95.216.27.105,95.216.3.166,95.216.3.171>
alert tcp [95.217.0.139,95.217.132.23,95.217.133.89,95.217.135.55,95.217.14.10>
alert tcp [95.217.16.212,95.217.162.36,95.217.164.106,95.217.167.152,95.217.17>
alert tcp [95.217.197.204,95.217.197.205,95.217.203.133,95.217.206.235,95.217.>
alert tcp [95.217.239.25,95.217.248.169,95.217.42.50,95.217.42.94,95.217.62.4,>
alert tcp [95.244.221.165,95.25.107.230,95.251.11.30,95.28.2.35,95.42.102.195,>
alert tcp [95.85.19.85,95.85.8.226,95.90.93.122,95.91.1.56,95.91.172.217,96.12>
alert tcp [96.255.209.36,96.65.68.193,97.103.2.110,97.107.132.24,97.107.139.10>
alert tcp [97.90.159.235,97.93.202.22,98.128.173.1,98.128.186.118,98.128.192.1>
alert tcp [98.225.157.78,98.234.189.216,98.234.222.4,98.37.64.180,99.105.213.1>
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET USER_AGENTS Suspicious >


^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit         ^R Read File    ^\ Replace      ^U              ^T To Spell
```

b. Using curl command , traffic is sent to google using user-agent “Blacksun”



```
  79  ls
  80  less suricata.rules
  81  vi suricata.rules
  82  nano suricata.rules
  83  curl -A "BlackSun" www.google.com
  84  suricata
```

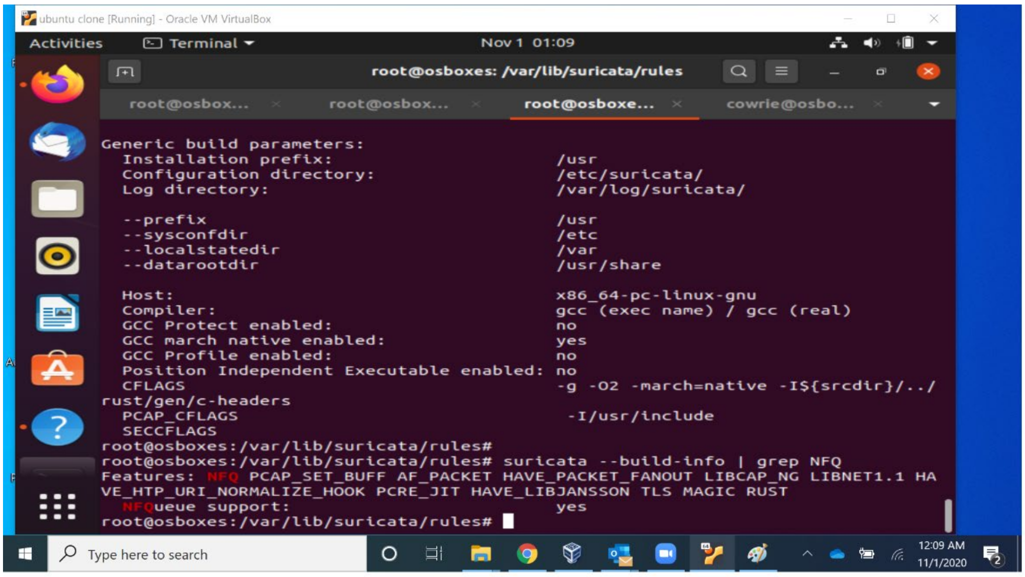
c. On verifying fast.log under /var/log/suricata , it is seen that an alert is triggered corresponding to the request made which matched with the rule added.



```
root@ubuntu:/home/keerthi# cat /var/log/suricata/fast.log
11/03/2020-21:16:08.969071  [**] [1:2008983:8] ET USER_AGENTS Suspicious User A
gent (BlackSun) [**] [Classification: A Network Trojan was detected] [Priority:
 1] {TCP} 10.0.2.15:35716 -> 172.217.8.196:80
```

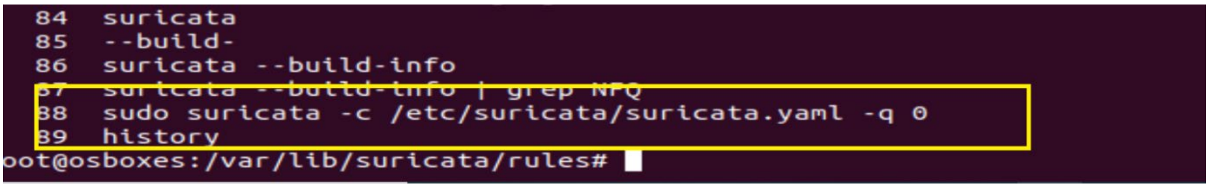
Section-03: Setting Suricata in layer-3 inline mode that is IPS

1. As shown in below screenshot, NFQ is supported in suricata.



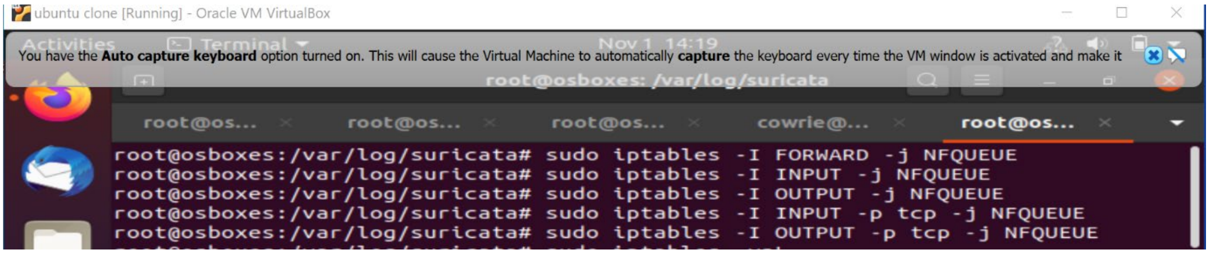
```
Generic build parameters:
  Installation prefix:                     /usr
  Configuration directory:                 /etc/suricata/
  Log directory:                           /var/log/suricata/

  --prefix                                 /usr
  --sysconfdir                             /etc
  --localstatedir                          /var
  --datarootdir                            /usr/share

  Host:                                    x86_64-pc-linux-gnu
  Compiler:                                gcc (exec name) / gcc (real)
  GCC Protect enabled:                     no
  GCC march native enabled:                yes
  GCC Profile enabled:                     no
  Position Independent Executable enabled: no
  CFLAGS                                   -g -O2 -march=native -I${srcdir}/../
rust/gen/c-headers
  PCAP_CFLAGS                               -I/usr/include
  SECCFLAGS
root@osboxes:/var/lib/suricata/rules#
root@osboxes:/var/lib/suricata/rules# suricata --build-info | grep NFQ
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HA
VE_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_LIBJANSSON TLS MAGIC RUST
  NFQueue support:                         yes
root@osboxes:/var/lib/suricata/rules#
```

2. Below command is issued to run suricata in NFQ mode.



```
 84  suricata
 85  --build-
 86  suricata --build-info
 87  suricata --build-info | grep NFQ
 88  sudo suricata -c /etc/suricata/suricata.yaml -q 0
 89  history
oot@osboxes:/var/lib/suricata/rules#
```

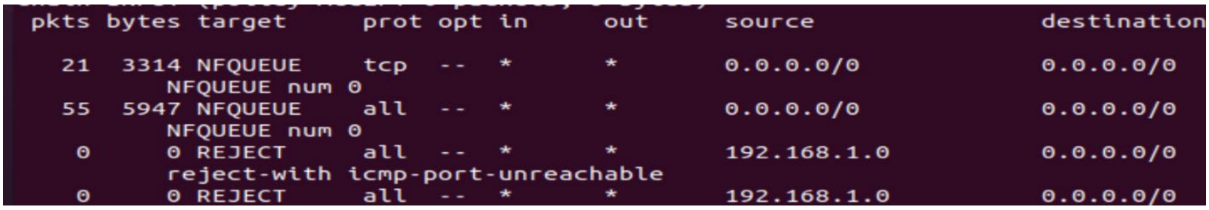
3. IP tables are configured to send traffic to Suricata. There are different ways to set rules for ip tables I.e make all traffic to go to Suricata I.e gateway scenario or configure as a host situation or check only tcp traffic .



You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it

```
root@osboxes:/var/log/suricata# sudo iptables -I FORWARD -j NFQUEUE
root@osboxes:/var/log/suricata# sudo iptables -I INPUT -j NFQUEUE
root@osboxes:/var/log/suricata# sudo iptables -I OUTPUT -j NFQUEUE
root@osboxes:/var/log/suricata# sudo iptables -I INPUT -p tcp -j NFQUEUE
root@osboxes:/var/log/suricata# sudo iptables -I OUTPUT -p tcp -j NFQUEUE
```

4. Verifying is suricata is running and logging packets. It is seen that packets and bytes are logged.



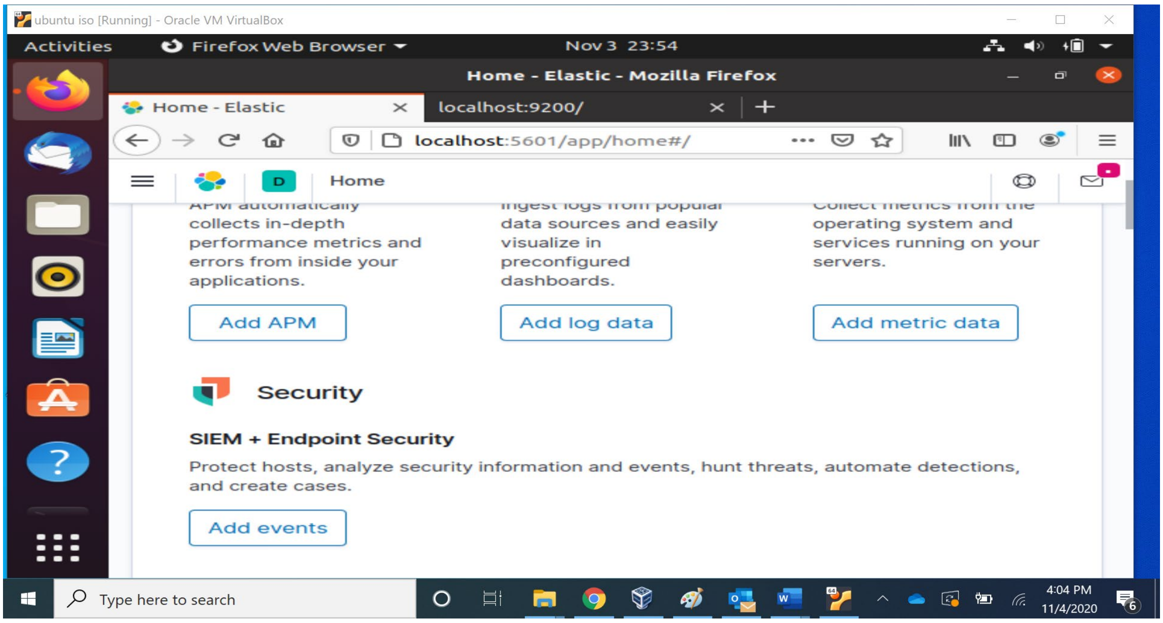
```
 pkts bytes target     prot opt in     out     source               destination

   21  3314 NFQUEUE    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
            NFQUEUE num 0
   55  5947 NFQUEUE    all  --  *      *       0.0.0.0/0            0.0.0.0/0
            NFQUEUE num 0
    0     0 REJECT     all  --  *      *       192.168.1.0          0.0.0.0/0
            reject-with icmp-port-unreachable
    0     0 REJECT     all  --  *      *       192.168.1.0          0.0.0.0/0
```

Section-04: Configuring ELK stack and viewing suricata logs:

After being Elasticsearch and kibana are installed. Their service is also started. Below steps needed to be executed to view Suricata logs in kibana.

Step 1:

Access kibana at http:localhost:5601. Click on add data and you will be navigated to the page shown in below screenshot .Using SIEM for viewing Suricata logs in Kibana. Selected “Add event” option under “SIEM+ Endpoint Security”



APM automatically collects in-depth performance metrics and errors from inside your applications.

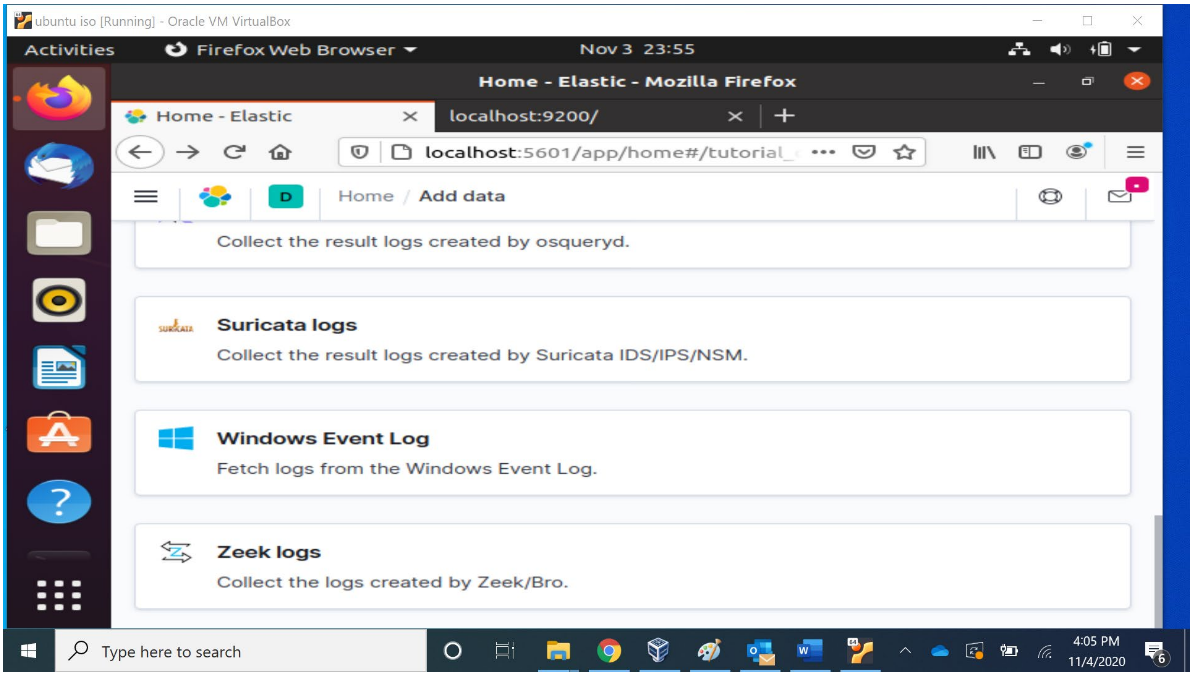
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Collect metrics from the operating system and services running on your servers.

SIEM + Endpoint Security

Protect hosts, analyze security information and events, hunt threats, automate detections, and create cases.

Step 2: Select Suricata logs among the different application logs



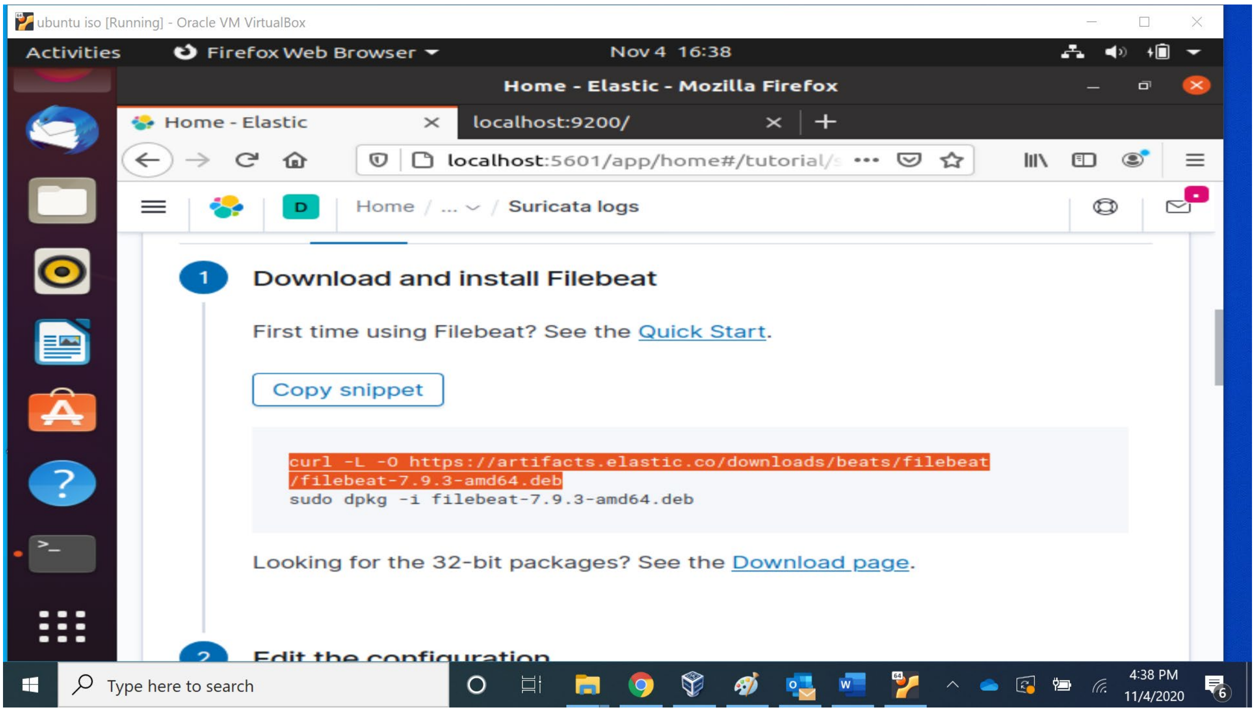
Collect the result logs created by osqueryd.

Suricata logs
Collect the result logs created by Suricata IDS/IPS/NSM.

Windows Event Log
Fetch logs from the Windows Event Log.

Zeek logs
Collect the logs created by Zeek/Bro.

Step 3: Page shown in below screenshot mentions all steps required to view Suricata logs in Kibana. The initial step is to download and install Filebeat.


ubuntu iso [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Nov 4 16:38
Home - Elastic - Mozilla Firefox
Home - Elastic
localhost:9200/
localhost:5601/app/home#/tutorial/
Home / ... / Suricata logs
Type here to search
4:38 PM
11/4/2020

1 Download and install Filebeat

First time using Filebeat? See the Quick Start.

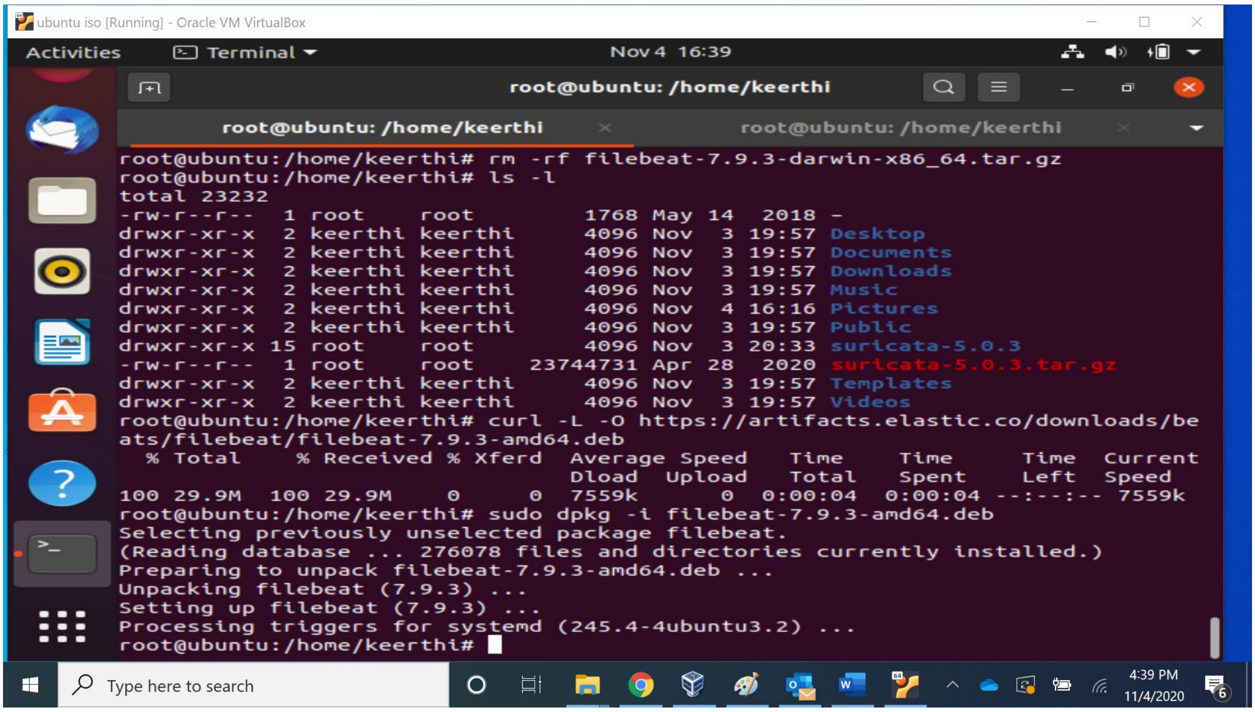
Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat
/filebeat-7.9.3-amd64.deb
sudo dpkg -i filebeat-7.9.3-amd64.deb
```

Looking for the 32-bit packages? See the Download page.

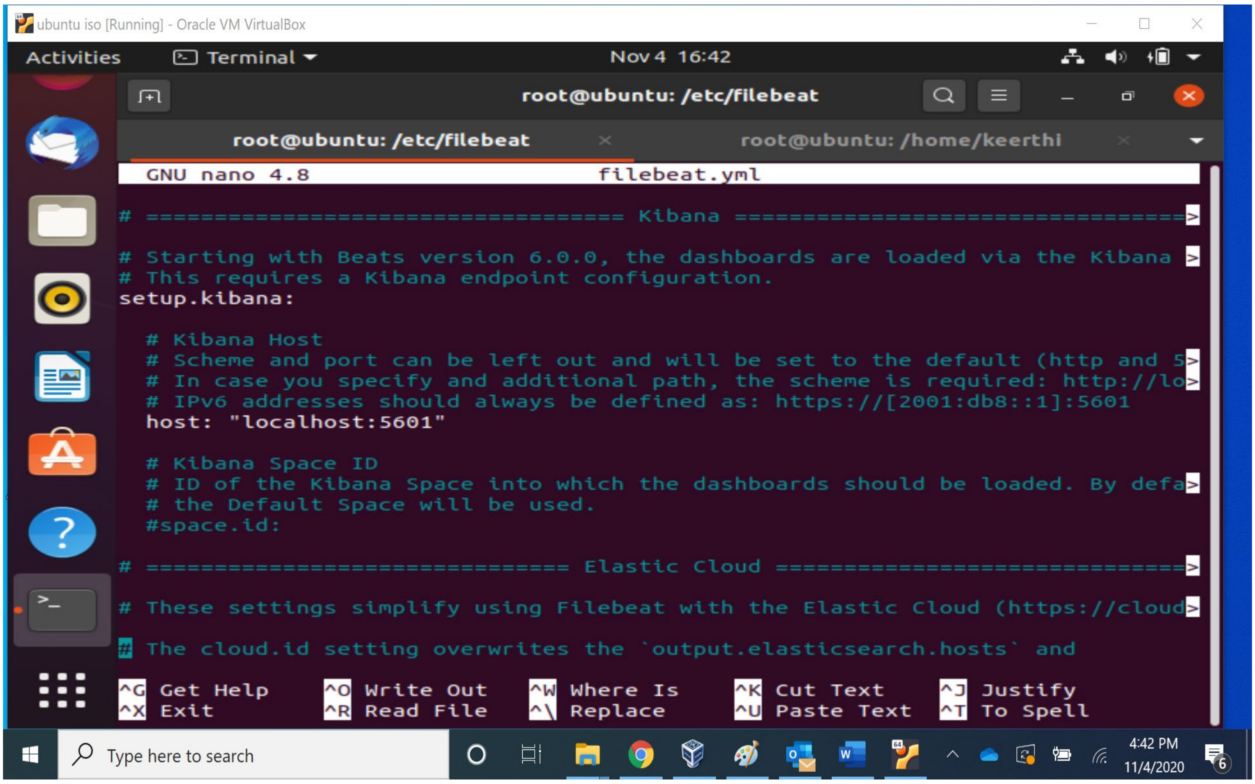
2 Edit the configuration

Step 4: Using curl filebeat.deb file is downloaded and installed as shown in below screenshot.


ubuntu iso [Running] - Oracle VM VirtualBox
Activities
Terminal
Nov 4 16:39
root@ubuntu: /home/keerthi
root@ubuntu: /home/keerthi
root@ubuntu: /home/keerthi
Type here to search
4:39 PM
11/4/2020

```
root@ubuntu:/home/keerthi# rm -rf filebeat-7.9.3-darwin-x86_64.tar.gz
root@ubuntu:/home/keerthi# ls -l
total 23232
-rw-r--r--  1 root    root        1768 May 14  2018 -
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Desktop
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Documents
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Downloads
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Music
drwxr-xr-x  2 keerthi keerthi     4096 Nov  4 16:16 Pictures
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Public
drwxr-xr-x 15 root    root        4096 Nov  3 20:33 suricata-5.0.3
-rw-r--r--  1 root    root    23744731 Apr 28  2020 suricata-5.0.3.tar.gz
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Templates
drwxr-xr-x  2 keerthi keerthi     4096 Nov  3 19:57 Videos
root@ubuntu:/home/keerthi# curl -L -O https://artifacts.elastic.co/downloads/be
ats/filebeat/filebeat-7.9.3-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 29.9M  100 29.9M    0     0  7559k      0  0:00:04  0:00:04 --:--:-- 7559k
root@ubuntu:/home/keerthi# sudo dpkg -i filebeat-7.9.3-amd64.deb
Selecting previously unselected package filebeat.
(Reading database ... 276078 files and directories currently installed.)
Preparing to unpack filebeat-7.9.3-amd64.deb ...
Unpacking filebeat (7.9.3) ...
Setting up filebeat (7.9.3) ...
Processing triggers for systemd (245.4-4ubuntu3.2) ...
root@ubuntu:/home/keerthi# 
```

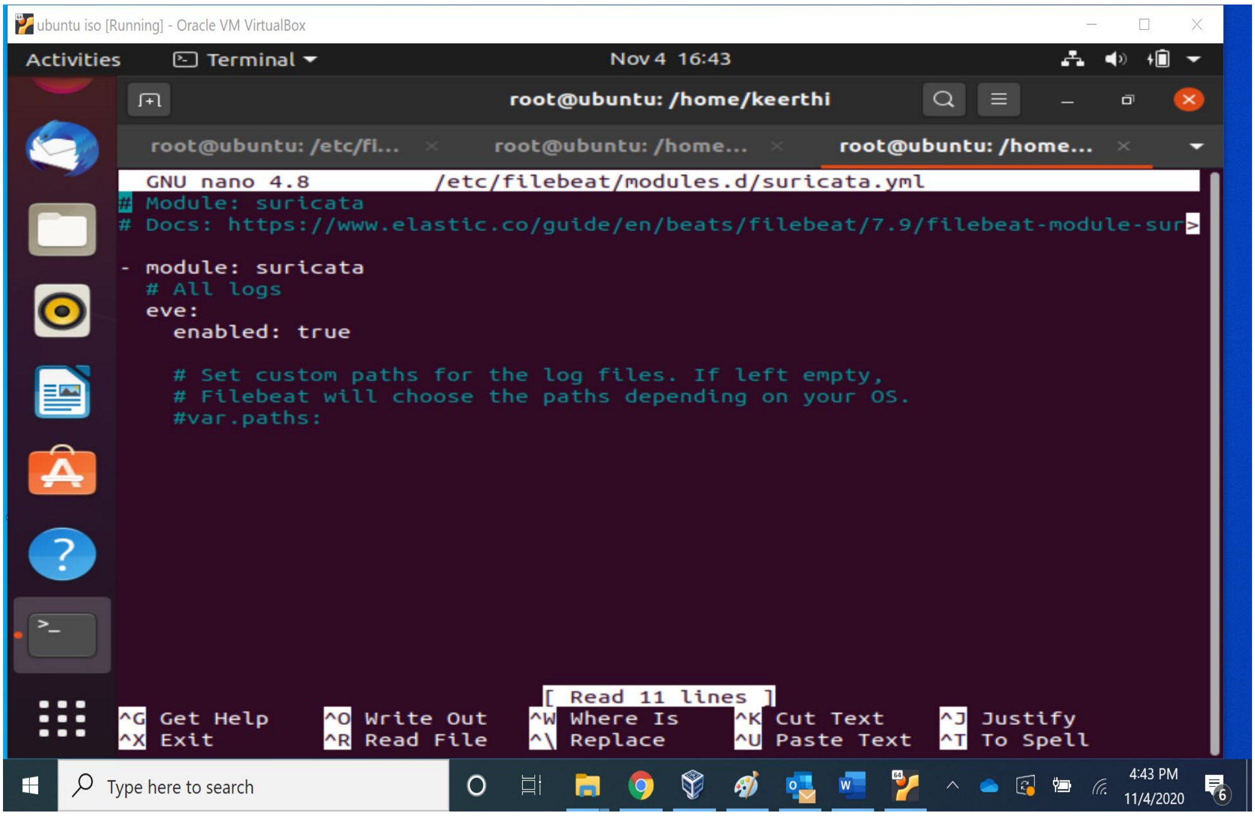
Step 5: Update filebeat.yml with kibana host value and elastic search host value.



```
GNU nano 4.8                    filebeat.yml

# ================================= Kibana =================================>

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana >
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5>
  # In case you specify and additional path, the scheme is required: http://lo>
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "localhost:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By defa>
  # the Default Space will be used.
  #space.id:

# =============================== Elastic Cloud ==============================>

# These settings simplify using Filebeat with the Elastic Cloud (https://cloud>

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit         ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell
```

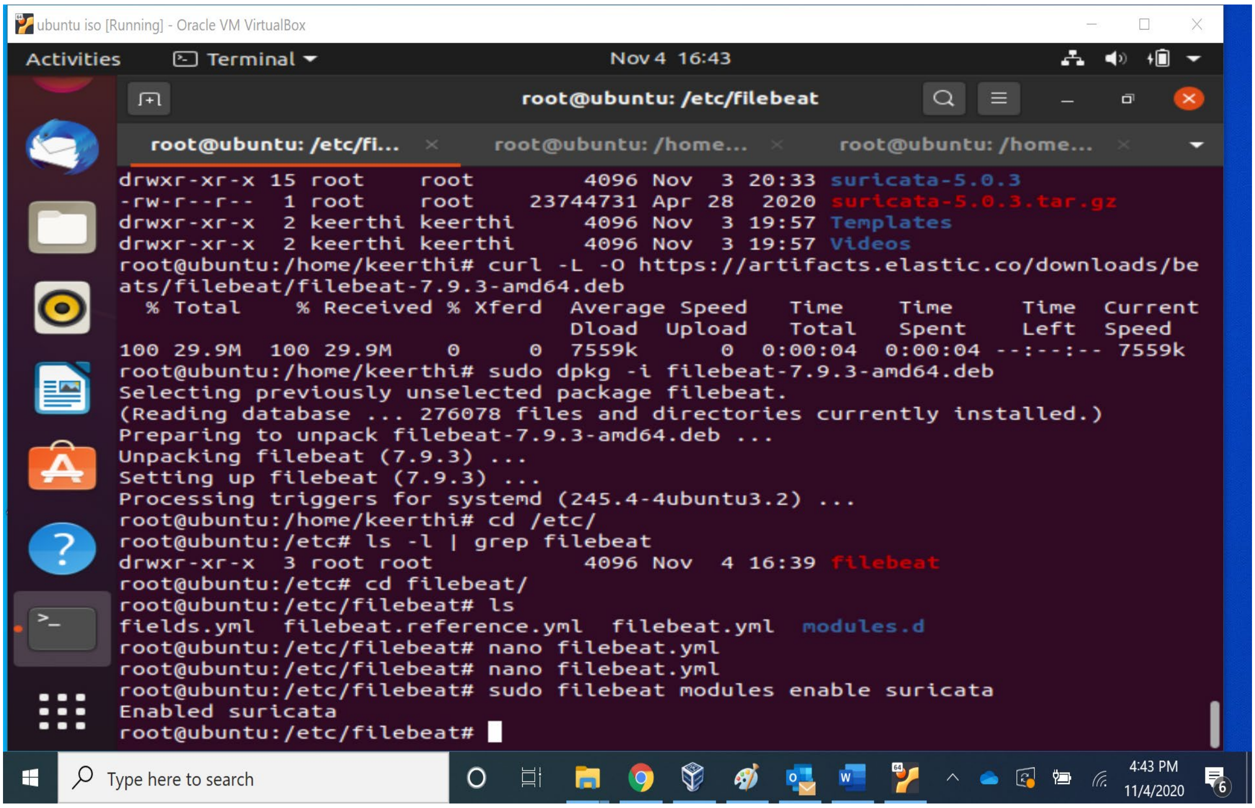
ubuntu iso [Running] - Oracle VM VirtualBox
Activities
Terminal
Nov 4 16:42
root@ubuntu: /etc/filebeat
root@ubuntu: /etc/filebeat
root@ubuntu: /home/keerthi
Type here to search
4:42 PM
11/4/2020

Step 6: Verify Suricata.yml file under modules.d folder of filebeat . As seen below Suricata is enabled.



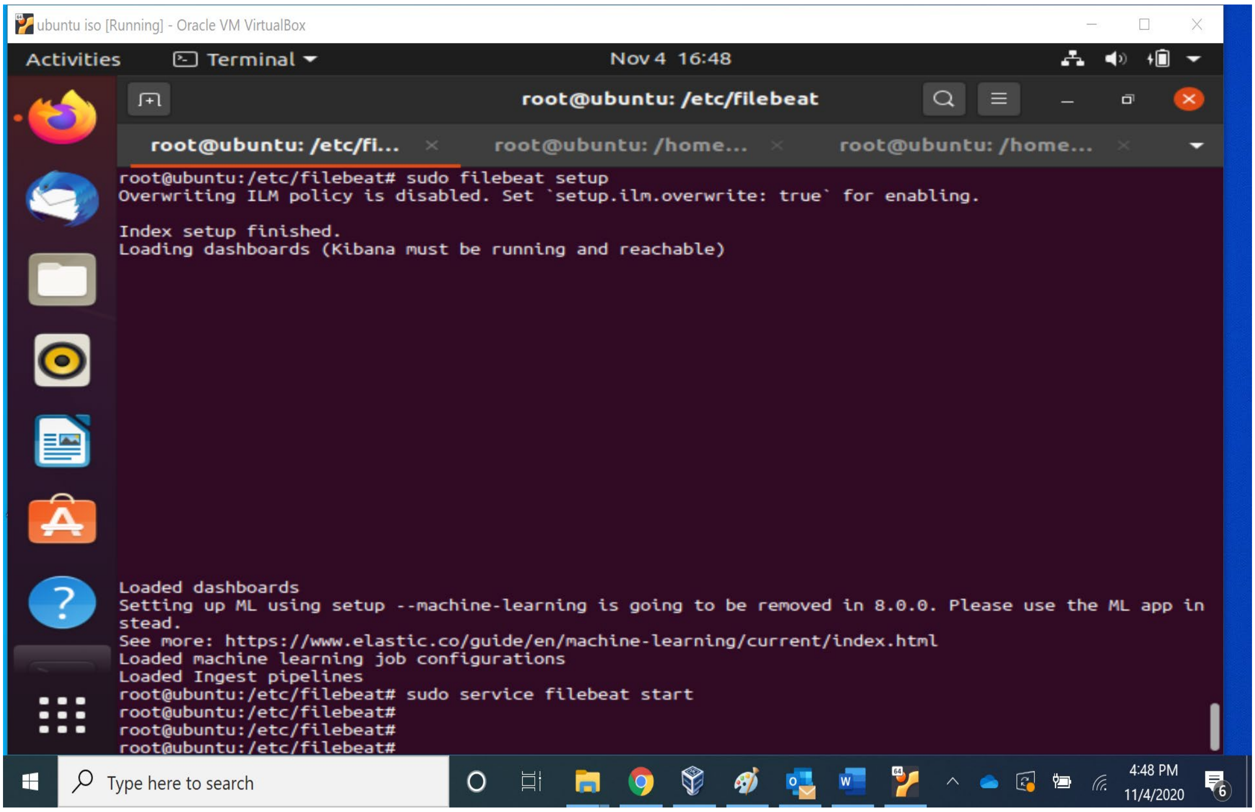
```
GNU nano 4.8          /etc/filebeat/modules.d/suricata.yml
# Module: suricata
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.9/filebeat-module-sur>

- module: suricata
  # All logs
  eve:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

                          [ Read 11 lines ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit         ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell
```

Step 7: Suricata module available among filebeat modules is enabled



```
drwxr-xr-x 15 root    root         4096 Nov  3 20:33 suricata-5.0.3
-rw-r--r--  1 root    root     23744731 Apr 28  2020 suricata-5.0.3.tar.gz
drwxr-xr-x  2 keerthi keerthi      4096 Nov  3 19:57 Templates
drwxr-xr-x  2 keerthi keerthi      4096 Nov  3 19:57 Videos
root@ubuntu:/home/keerthi# curl -L -O https://artifacts.elastic.co/downloads/be
ats/filebeat/filebeat-7.9.3-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 29.9M  100 29.9M    0     0  7559k      0  0:00:04  0:00:04 --:--:-- 7559k
root@ubuntu:/home/keerthi# sudo dpkg -i filebeat-7.9.3-amd64.deb
Selecting previously unselected package filebeat.
(Reading database ... 276078 files and directories currently installed.)
Preparing to unpack filebeat-7.9.3-amd64.deb ...
Unpacking filebeat (7.9.3) ...
Setting up filebeat (7.9.3) ...
Processing triggers for systemd (245.4-4ubuntu3.2) ...
root@ubuntu:/home/keerthi# cd /etc/
root@ubuntu:/etc# ls -l | grep filebeat
drwxr-xr-x  3 root root            4096 Nov  4 16:39 filebeat
root@ubuntu:/etc# cd filebeat/
root@ubuntu:/etc/filebeat# ls
fields.yml  filebeat.reference.yml  filebeat.yml  modules.d
root@ubuntu:/etc/filebeat# nano filebeat.yml
root@ubuntu:/etc/filebeat# nano filebeat.yml
root@ubuntu:/etc/filebeat# sudo filebeat modules enable suricata
Enabled suricata
root@ubuntu:/etc/filebeat# 
```

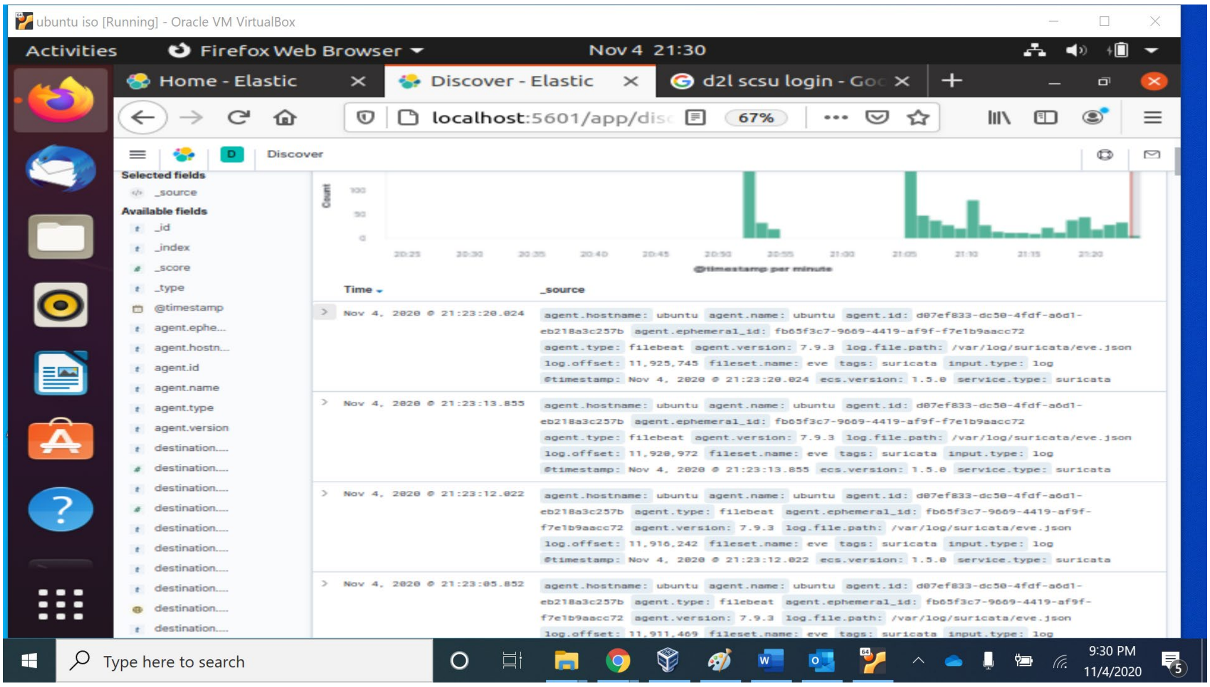
Step 8: Filebeat is setup and its service is started



```
root@ubuntu:/etc/filebeat# sudo filebeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app in
stead.
See more: https://www.elastic.co/guide/en/machine-learning/current/index.html
Loaded machine learning job configurations
Loaded Ingest pipelines
root@ubuntu:/etc/filebeat# sudo service filebeat start
root@ubuntu:/etc/filebeat#
root@ubuntu:/etc/filebeat#
root@ubuntu:/etc/filebeat#
```

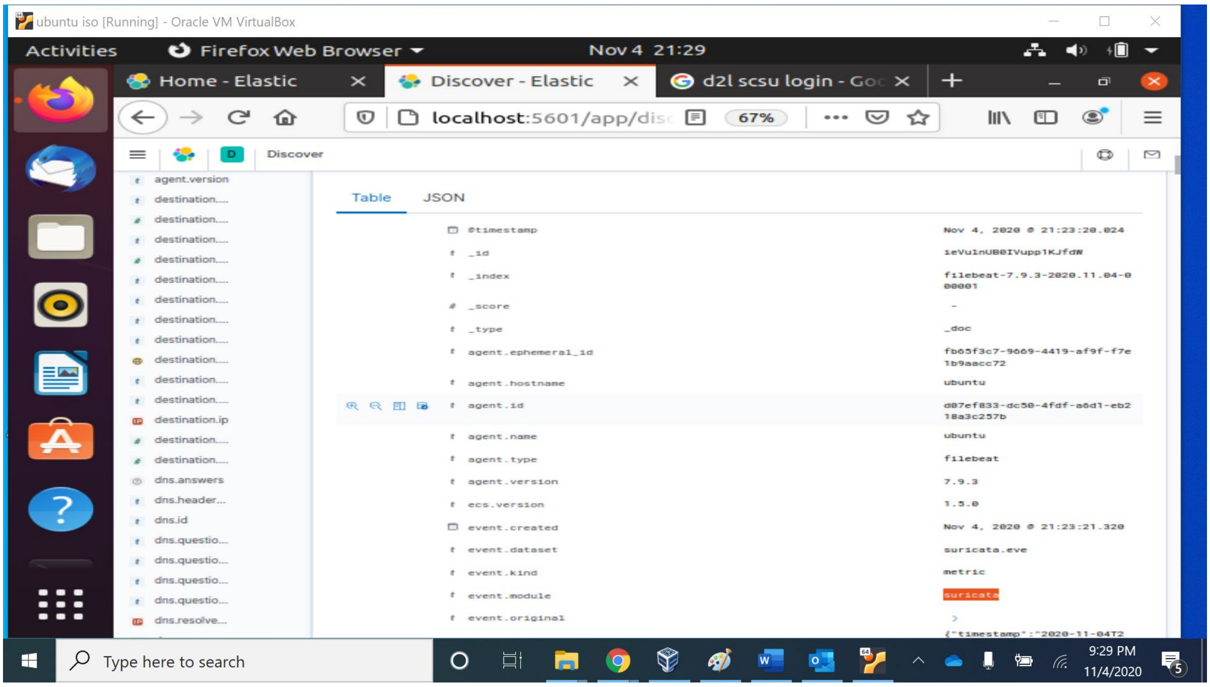
Step 9: Access Kibana and select discover tab in it . Create a new index pattern “filebeat*”.

We will now be able to see Suricata logs in ELK



```
> Nov 4, 2020 @ 21:23:20.024  agent.hostname: ubuntu agent.name: ubuntu agent.id: d07ef833-dc50-4fdf-a6d1-
                              eb218a3c257b agent.ephemeral_id: fb65f3c7-9669-4419-af9f-f7e1b9aacc72
                              agent.type: filebeat agent.version: 7.9.3 log.file.path: /var/log/suricata/eve.json
                              log.offset: 11,925,745 fileset.name: eve tags: suricata input.type: log
                              @timestamp: Nov 4, 2020 @ 21:23:20.024 ecs.version: 1.5.0 service.type: suricata
> Nov 4, 2020 @ 21:23:13.855  agent.hostname: ubuntu agent.name: ubuntu agent.id: d07ef833-dc50-4fdf-a6d1-
                              eb218a3c257b agent.ephemeral_id: fb65f3c7-9669-4419-af9f-f7e1b9aacc72
                              agent.type: filebeat agent.version: 7.9.3 log.file.path: /var/log/suricata/eve.json
                              log.offset: 11,920,972 fileset.name: eve tags: suricata input.type: log
                              @timestamp: Nov 4, 2020 @ 21:23:13.855 ecs.version: 1.5.0 service.type: suricata
> Nov 4, 2020 @ 21:23:12.022  agent.hostname: ubuntu agent.name: ubuntu agent.id: d07ef833-dc50-4fdf-a6d1-
                              eb218a3c257b agent.type: filebeat agent.ephemeral_id: fb65f3c7-9669-4419-af9f-
                              f7e1b9aacc72 agent.version: 7.9.3 log.file.path: /var/log/suricata/eve.json
                              log.offset: 11,916,242 fileset.name: eve tags: suricata input.type: log
                              @timestamp: Nov 4, 2020 @ 21:23:12.022 ecs.version: 1.5.0 service.type: suricata
> Nov 4, 2020 @ 21:23:05.852  agent.hostname: ubuntu agent.name: ubuntu agent.id: d07ef833-dc50-4fdf-a6d1-
                              eb218a3c257b agent.type: filebeat agent.ephemeral_id: fb65f3c7-9669-4419-af9f-
                              f7e1b9aacc72 agent.version: 7.9.3 log.file.path: /var/log/suricata/eve.json
                              log.offset: 11,911,469 fileset.name: eve tags: suricata input.type: log
```

Step 10: Below is the json format of a particular selected log .



@timestamp	Nov 4, 2020 @ 21:23:20.024
_id	1eVulnUB0IVupp1KJfdW
_index	filebeat-7.9.3-2020.11.04-000001
_score	-
_type	_doc
agent.ephemeral_id	fb65f3c7-9669-4419-af9f-f7e1b9aacc72
agent.hostname	ubuntu
agent.id	d07ef833-dc50-4fdf-a6d1-eb218a3c257b
agent.name	ubuntu
agent.type	filebeat
agent.version	7.9.3
ecs.version	1.5.0
event.created	Nov 4, 2020 @ 21:23:21.320
event.dataset	suricata.eve
event.kind	metric
event.module	suricata
event.original	{"timestamp":"2020-11-04T2

****

NOTE: You may add following sections into your LAB report to make a more comprehensive well written document based on your experiences during the LAB exercises.

****

Section-XX1: Conclusions/Discussion/Summary/Insights

Section-XX2: Limitations /Difficulties/Problems/Issues

Section-XX3: References

Appendixes: If available, For additional materials such as source codes and etc…!!!