



EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY



Network Protection for Energy Control Systems

These slides outline the essential offensive tools that will be used in this course.

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

IDS

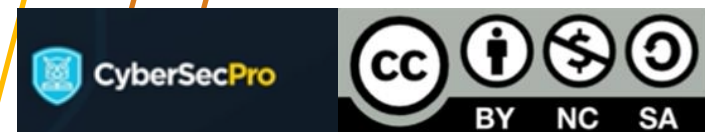
SURICATA

SURICATA

- Suricata is an **open-source-based intrusion detection** system and **intrusion prevention** system
- Suricata **analyzes** all **traffic** on the **interface**, searching for known **attacks** and **anomalies**
- When an **attack** or **anomaly** is **detected**, the system can **decide** whether to **block traffic** or **simply save** the **event** on a **log** ([/var/log/suricata/fast.log](#))
- **Suricata** can be **configured** using sets of **rules** organized in uniform categories.
- Each **category** can be set to:
 - **Enable**: traffic **matching rules** from these **categories** will be **reported**
 - **Block**: traffic **matching rules** from this **category** will be **dropped**
 - **Disable**: **rules** from this category are **ignored**

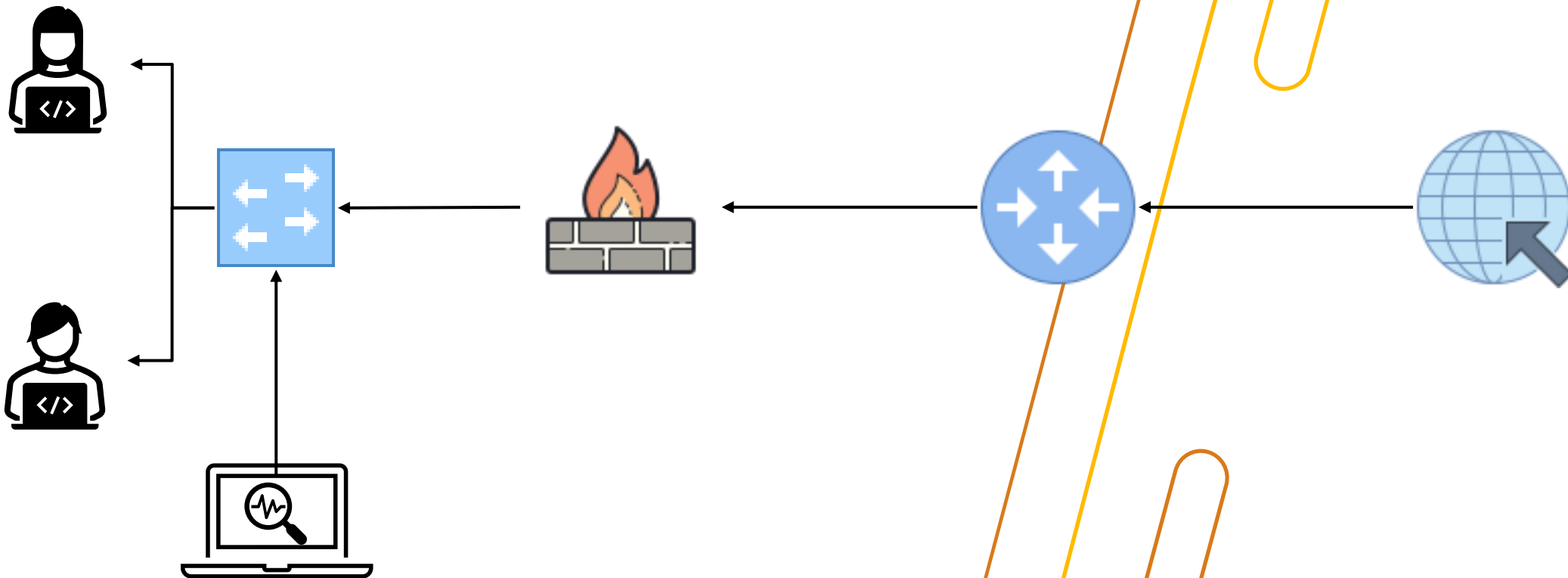


SURICATA



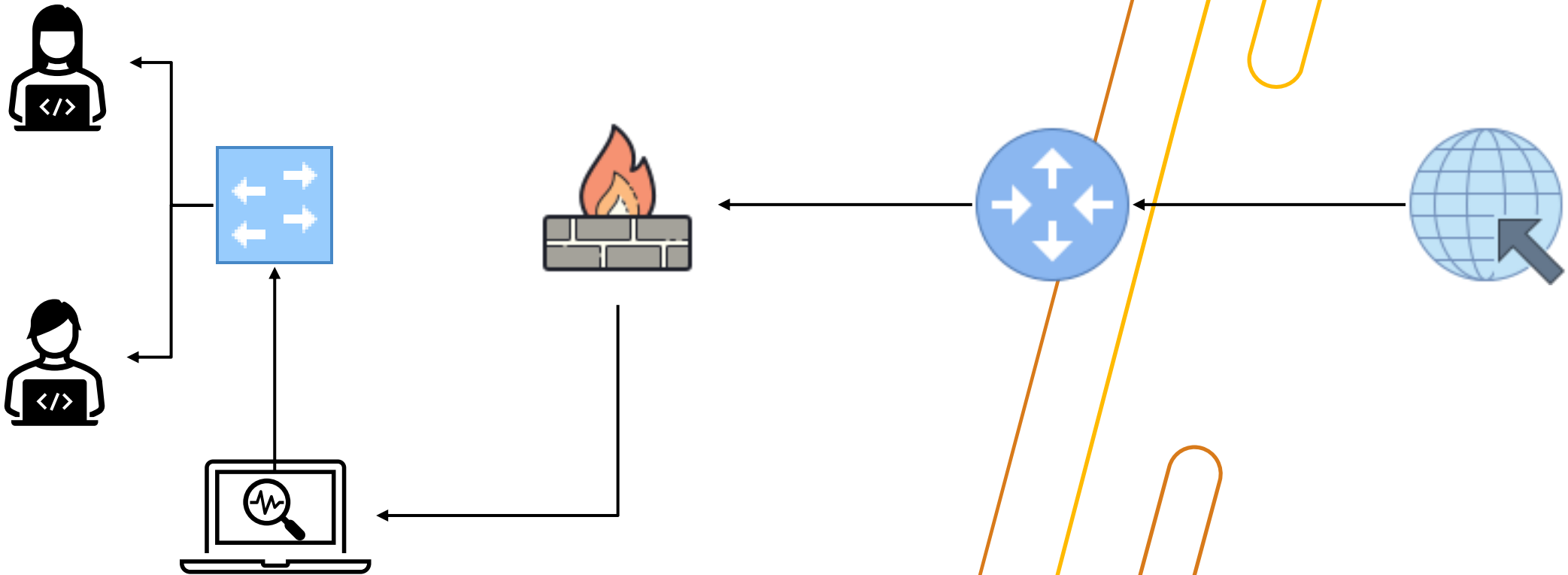
SURICTA Modes

IDS



SURICTA Modes

IPS



SURICATA Installation

- Sudo apt-get update
- Sudo apt-get install suricata

```
kali@kali: ~  
File Actions Edit View Help  
Setting up librt-net-bond24:amd64 (23.11-1) ...  
Setting up suricata (1:7.0.3-1) ...  
update-rc.d: We have no instructions for the suricata init script.  
update-rc.d: It looks like a network service, we disable it.  
suricata.service is a disabled or a static unit, not starting it.  
Processing triggers for libc-bin (2.37-12) ...  
Processing triggers for man-db (2.12.0-3) ...  
Processing triggers for kali-menu (2023.4.7) ...  
  
(kali@kali)-[~]  
└─$ suricata  
Suricata 7.0.3  
USAGE: suricata [OPTIONS] [BPF FILTER]  
  
-c <path>           : path to configuration file  
-T                 : test configuration file (use with -c)  
-i <dev or ip>     : run in pcap live mode  
-F <bpf filter file> : bpf filter file  
-r <path>         : run in pcap file/offline mode  
-q <qid[:qid]>    : run in inline nfqueue mode (use colon to specify a  
-s <path>         : path to signature file loaded in addition to suric  
(optional)  
-S <path>         : path to signature file loaded exclusively (optiona  
-l <dir>          : default log directory  
-D                : run as daemon  
-k [all|none]     : force checksum check (all) or disabled it (none)  
-V                : display Suricata version  
-v               : be more verbose (use multiple times to increase ve
```

Suricata Rules and Configurations

Suricata list of Rules

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls -al /etc/suricata
total 116
drwxr-xr-x  3 root root  4096 Apr  8 17:44 .
drwxr-xr-x 182 root root 12288 Apr  8 17:44 ..
-rw-r--r--  1 root root  3327 Feb  8 04:35 classification.config
-rw-r--r--  1 root root  1375 Feb  8 04:35 reference.config
drwxr-xr-x  2 root root  4096 Apr  8 17:44 rules
-rw-r--r--  1 root root 85175 Feb  8 17:22 suricata.yaml
-rw-r--r--  1 root root  1643 Feb  8 04:35 threshold.config

(kali@kali)-[~]
└─$
  
```

Suricata Configurations and Rules

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls -al /etc/suricata/rules
total 152
drwxr-xr-x  2 root root  4096 Apr  8 17:44 .
drwxr-xr-x  3 root root  4096 Apr  8 17:44 ..
-rw-r--r--  1 root root  1858 Feb  8 04:35 app-layer-events.rules
-rw-r--r--  1 root root 20880 Feb  8 04:35 decoder-events.rules
-rw-r--r--  1 root root   468 Feb  8 04:35 dhcp-events.rules
-rw-r--r--  1 root root  1221 Feb  8 04:35 dnp3-events.rules
-rw-r--r--  1 root root  1198 Feb  8 04:35 dns-events.rules
-rw-r--r--  1 root root  4005 Feb  8 04:35 files.rules
-rw-r--r--  1 root root   446 Feb  8 04:35 ftp-events.rules
-rw-r--r--  1 root root 14256 Feb  8 04:35 http-events.rules
-rw-r--r--  1 root root  3311 Feb  8 04:35 http2-events.rules
-rw-r--r--  1 root root  2832 Feb  8 04:35 ipsec-events.rules
-rw-r--r--  1 root root   585 Feb  8 04:35 kerberos-events.rules
-rw-r--r--  1 root root  2077 Feb  8 04:35 modbus-events.rules
-rw-r--r--  1 root root  2187 Feb  8 04:35 mqtt-events.rules
-rw-r--r--  1 root root   729 Feb  8 04:35 nfs-events.rules
-rw-r--r--  1 root root   558 Feb  8 04:35 ntp-events.rules
-rw-r--r--  1 root root   544 Feb  8 04:35 quic-events.rules
-rw-r--r--  1 root root   926 Feb  8 04:35 rfb-events.rules
-rw-r--r--  1 root root  4607 Feb  8 04:35 smb-events.rules
-rw-r--r--  1 root root  5393 Feb  8 04:35 smtp-events.rules
-rw-r--r--  1 root root   719 Feb  8 04:35 ssh-events.rules
-rw-r--r--  1 root root 14311 Feb  8 04:35 stream-events.rules
-rw-r--r--  1 root root  6861 Feb  8 04:35 tls-events.rules

(kali@kali)-[~]
└─$
  
```

Suricata Rules and Configurations

Some **configurations** in the ``suricata.yaml`` file need to be **updated**.

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls -al /etc/suricata
total 116
drwxr-xr-x  3 root root  4096 Apr  8 17:44 .
drwxr-xr-x 182 root root 12288 Apr  8 17:44 ..
-rw-r--r--  1 root root  3327 Feb  8 04:35 classification.config
-rw-r--r--  1 root root  1375 Feb  8 04:35 reference.config
drwxr-xr-x  2 root root  4096 Apr  8 17:44 rules
-rw-r--r--  1 root root 85175 Feb  8 17:22 suricata.yaml
-rw-r--r--  1 root root  1643 Feb  8 04:35 threshold.config

(kali@kali)-[~]
└─$
```

Suricata Configurations and Rules

You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

Update the configuration file
Sudo vim /etc/suricata/suricata.yaml

```
~/Desktop/suricata.yaml - Mousepad
File Edit Search View Document Help

1 %YAML 1.1
2 ---
3
4 # Suricata configuration file. In addition to the comments describing all
5 # options in this file, full documentation can be found at:
6 # https://docs.suricata.io/en/latest/configuration/suricata-yaml.html
7
8 # This configuration file generated by Suricata 7.0.3.
9 suricata-version: "7.0"
10
11 ##
12 ## Step 1: Inform Suricata about your network
13 ##
14
15 vars:
16 # more specific is better for alert accuracy and performance
17 address-groups:
18   HOME_NET: "[192.168.122.0/24]"
19   #HOME_NET: "[192.168.0.0/16]"
20   #HOME_NET: "[10.0.0.0/8]"
21   #HOME_NET: "[172.16.0.0/12]"
22   #HOME_NET: "any"
23
24   EXTERNAL_NET: "!$HOME_NET"
25   #EXTERNAL_NET: "any"
26
27   HTTP_SERVERS: "$HOME_NET"
28   SMTP_SERVERS: "$HOME_NET"
29   SQL_SERVERS: "$HOME_NET"
30   DNS_SERVERS: "$HOME_NET"
31   TELNET_SERVERS: "$HOME_NET"
32   AIM_SERVERS: "$EXTERNAL_NET"
33   DC_SERVERS: "$HOME_NET"
34   DNP3_SERVER: "$HOME_NET"
35   DNP3_CLIENT: "$HOME_NET"
36   MODBUS_CLIENT: "$HOME_NET"
37   MODBUS_SERVER: "$HOME_NET"
38   ENIP_CLIENT: "$HOME_NET"
39   ENIP_SERVER: "$HOME_NET"
40
41 port-groups:
42   HTTP_PORTS: "80"
43   SHELLCODE_PORTS: "!80"
44   ORACLE_PORTS: 1521
45   SSH_PORTS: 22
46   DNP3_PORTS: 20000
47   MODBUS_PORTS: 502
```

Suricata Rules and Configurations

We need to configure the **HOME_NET** that we want to **monitor** and **ensure** the correct **interface** name is defined.

So we need to know the **subnet**

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.122.203 netmask 255.255.255.0 broadcast 192.168.122.255
    inet6 fe80::1a9:e34d:3f1b:b318 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:fa:75:14 txqueuelen 1000 (Ethernet)
    RX packets 53707 bytes 77874681 (74.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22955 bytes 1632538 (1.5 MiB)
    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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
└─$
```

You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

Update the configuration file
Sudo vim /etc/suricata/suricata.yaml

```
root@kali: ~
File Actions Edit View Help
%YAML 1.1
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html
# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"
##
## Step 1: Inform Suricata about your network
##
vars:
# more specific is better for alert accuracy and performance
address-groups:
  HOME_NET: "[192.168.122.0/24]"
  #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:
24,5
Top
CyberSecPro
BY NC SA
```

Suricata Rules and Configurations

We need to configure the **HOME_NET** that we want to **monitor** and **ensure** the correct **interface** name is defined.

So we need to know the **interface**

```
kali@kali: ~
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.122.203 netmask 255.255.255.0 broadcast 192.168.122.255
    inet6 fe80::1af9:e34d:3f15:b318 prefixlen 64 scopeid 0<link>
    ether 08:00:27:fa:75:14 txqueuelen 1000 (Ethernet)
    RX packets 53707 bytes 77874681 (74.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22955 bytes 1632538 (1.5 MiB)
    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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
└─$
```

Interface
name

You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

Update the configuration file
Sudo vim /etc/suricata/suricata.yaml

```
~/Desktop/suricata.yaml - Mousepad
File Edit Search View Document Help
┌─$
607 ## Step 3: Configure common capture settings
608 ##
609 ## See "Advanced Capture Options" below for more options, including Netmap
610 ## and PF_RING.
611 ##
612 ##
613 # Linux high speed capture support
614 # if-packet:
615 #   - interface: eth0
616 #     # Number of receive threads. "auto" uses the number of cores
617 #     #threads: auto
618 #   # Default cluster-id. AF_PACKET will load balance packets based on flow.
619 #   cluster-id: 99
620 #   # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
621 #   # This is only supported for Linux kernel > 3.1
622 #   possible value are:
623 #   * cluster_flow: all packets of a given flow are sent to the same socket
624 #   * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
625 #   * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
626 #   # socket. Requires at least Linux 3.14.
627 #   * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst
628 #   for
629 #   # more info.
630 #   # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
631 #   # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
632 #   # cluster_rollover has been deprecated; if used, it'll be replaced with cluster_flow.
633 #   cluster-type: cluster_flow
634 #   # In some fragmentation cases, the hash can not be computed. If "defrag" is set
635 #   # to yes, the kernel will do the needed defragmentation before sending the packets.
636 #   defrag: yes
637 #   # To use the ring feature of AF_PACKET, set 'use-mmap' to yes
638 #   #use-mmap: yes
639 #   # Lock memory map to avoid it being swapped. Be careful that over
640 #   # subscribing could lock your system
641 #   #mmap-locked: yes
642 #   # Use tpacket_v3 capture mode, only active if use-mmap is true
643 #   # Don't use it in IPS or TAP mode as it causes severe latency
644 #   #tpacket-v3: yes
645 #   # Ring size will be computed with respect to "max-pending-packets" and number
646 #   # of threads. You can set manually the ring size in number of packets by setting
647 #   # the following value. If you are using flow "cluster-type" and have really network
648 #   # intensive single-flow you may want to set the "ring-size" independently of the number
649 #   # of threads:
650 #   #ring-size: 2048
651 #   # Block size is used by tpacket_v3 only. It should set to a value high enough to contain
652 #   # a decent number of packets. Size is in bytes so please consider your MTU. It should be
653 #   # a power of 2 and it must be multiple of page size (usually 4096).
```

Interface name

Unique number

Suricata Rules and Configurations

We need to configure the **HOME_NET** that we want to **monitor** and **ensure** the correct **interface** name is defined.

So we need to know the **interface**

```
kali@kali: ~
┌───(kali㉿kali)-[~]
│   └─$ ifconfig
│ eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
│         inet 192.168.122.203  netmask 255.255.255.0  broadcast 192.168.122.255
│         inet6 fe80::1af9:e34d:5f15:b218  prefixlen 64  scopeid 0x20<link>
│         ether 08:00:27:fa:75:14  txqueuelen 1000  (Ethernet)
│         RX packets 53707  bytes 77874681 (74.2 MiB)
│         RX errors 0  dropped 0  overruns 0  frame 0
│         TX packets 22955  bytes 1632538 (1.5 MiB)
│         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 4  bytes 240 (240.0 B)
│        RX errors 0  dropped 0  overruns 0  frame 0
│        TX packets 4  bytes 240 (240.0 B)
│        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
│
└─(kali㉿kali)-[~]
└─$
```

Interface
name

```
~/Desktop/suricata.yaml - Mousepad
File Edit Search View Document Help
┌───(kali㉿kali)-[~/Desktop]
│   └─$ sudo vim /etc/suricata/suricata.yaml
│
│ 788
│ 789 - interface: default
│ 790   threads: auto
│ 791   promisc: true
│ 792   multicast: true
│ 793   checksum-checks: true
│ 794   checksum-checks-offload: true
│ 795   mtu: 1500
│ 796   rss-hash-functions: auto
│ 797   mempool-size: 65535
│ 798   mempool-cache-size: 257
│ 799   rx-descriptors: 1024
│ 800   tx-descriptors: 1024
│ 801   copy-mode: none
│ 802   copy-iface: none
│ 803
│ 804
│ 805 # Cross platform libpcap capture support
│ 806 pcap:
│ 807   - interface: eth0
│ 808   # On Linux, pcap will try to use mmap'd capture and will use "buffer-size"
│ 809   # as total memory used by the ring. So set this to something bigger
│ 810   # than 1% of your bandwidth.
│ 811   #buffer-size: 16777216
│ 812   #bpf-filter: "tcp and port 25"
│ 813   # Choose checksum verification mode for the interface. At the moment
│ 814   # of the capture, some packets may have an invalid checksum due to
│ 815   # the checksum computation being offloaded to the network card.
│ 816   # Possible values are:
│ 817   # - yes: checksum validation is forced
│ 818   # - no: checksum validation is disabled
│ 819   # - auto: Suricata uses a statistical approach to detect when
│ 820   # checksum off-loading is used. (default)
│ 821   # Warning: 'capture.checksum-validation' must be set to yes to have any validation
│ 822   #checksum-checks: auto
│ 823   # With some accelerator cards using a modified libpcap (like Myricom), you
│ 824   # may want to have the same number of capture threads as the number of capture
│ 825   # rings. In this case, set up the threads variable to N to start N threads
│ 826   # listening on the same interface.
│ 827   #threads: 16
│ 828   # set to no to disable promiscuous mode:
│ 829   #promisc: no
│ 830   # set snaplen, if not set it defaults to MTU if MTU can be known
│ 831   # via ioctl call and to full capture if not.
│ 832   #snaplen: 1518
│ 833   # Put default values here
│ 834   - interface: default
```

Interface
name

You can also copy the **suricata.yaml** file, paste a version on the **desktop**, make your changes, and then save it to the original path.

Sudo cp Source_file Destination_directory

Suricata Rules and Configurations

```

125 # include the name of the input pcap file in pcap file processing mode
126 pcap-file: false
127
128 # Community Flow ID
129 # Adds a 'community_id' field to EVE records. These are meant to give
130 # records a predictable flow ID that can be used to match records to
131 # output of other tools such as Zeek (Bro).
132 #
133 # Takes a 'seed' that needs to be same across sensors and tools
134 # to make the id less predictable.
135 # enable/disable the community id feature.
136 community-id: true
137 # Seed value for the ID output. Valid values are 0-65535.
138 community-id-seed: 0
139
140 # HTTP X-Forwarded-For support by adding an extra field or overwriting
141 # the source or destination IP address (depending on flow direction)
142 # with the one reported in the X-Forwarded-For HTTP header. This is
143 # helpful when reviewing alerts for traffic that is being reverse
144 # or forward proxied.
145 xff:
146   enabled: no
147   # Two operation modes are available: "extra-data" and "overwrite".
148   mode: extra-data
149   # Two proxy deployments are supported: "reverse" and "forward". In
150   # a "reverse" deployment the IP address used is the last one, in a
151   # "forward" deployment the first IP address is used.
152   deployment: reverse
153   # Header name where the actual IP address will be reported. If more
154   # than one IP address is present, the last IP address will be the
155   # one taken into consideration.
156   header: X-Forwarded-For
157
158 types:
159 - alert:
160   # payload: yes # enable dumping payload in Base64
161   # payload-buffer-size: 4kb # max size of payload buffer to output in eve-log
162   # payload-printable: yes # enable dumping payload in printable (lossy) format
163   # packet: yes # enable dumping of packet (without stream segments)
164   # metadata: no # enable inclusion of app layer metadata with alert.
165
166 Default yes
167 # http-body: yes # Requires metadata; enable dumping of HTTP body in Base64
168 # http-body-printable: yes # Requires metadata; enable dumping of HTTP body in
169 # printable format
170 # Enable the logging of tagged packets for rules using the

```

You could directly open the **.yaml** configuration file, make any **updates** you want, and then **store** the **file again**.

If you are using **VIM**:

To **Exit VIM**, press **Esc** with **q**:

Type **q** for **quite**

Type **q!** for **quiet without saving**

Type **wq** to **write and quite**

If you copied the **suricata.yaml** file, then use the **cp** command

Sudo cp Source_file Destination_directory

Destination Directory: /etc/suricata/suricata.yaml

Suricata Rules and Configurations

Update suricata using: **sudo suricata-update**

No errors detected 😊

```

root@kali: ~
└─(root@kali)-[~]
   └─# suricata-update
1/10/2024 -- 08:34:18 - <Info> -- Using data-directory /var/lib/suricata.
1/10/2024 -- 08:34:18 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
1/10/2024 -- 08:34:18 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
1/10/2024 -- 08:34:18 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
1/10/2024 -- 08:34:18 - <Info> -- Loading /etc/suricata/suricata.yaml
1/10/2024 -- 08:34:18 - <Info> -- Disabling rules for protocol pgsq
1/10/2024 -- 08:34:18 - <Info> -- Disabling rules for protocol modbus
1/10/2024 -- 08:34:18 - <Info> -- Disabling rules for protocol dnp3
1/10/2024 -- 08:34:18 - <Info> -- Disabling rules for protocol enip
1/10/2024 -- 08:34:18 - <Info> -- No sources configured, will use Emerging Threats Open
1/10/2024 -- 08:34:18 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-7.0.3
/emerging.rules.tar.gz.md5.
1/10/2024 -- 08:34:18 - <Info> -- Remote checksum has not changed. Not fetching.
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-e
vents.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-eve
nts.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events
.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events
.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.
rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events
.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-event
s.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-ev
ents.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-even
ts.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.
rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.
rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.
rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events
.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-even
ts.rules
1/10/2024 -- 08:34:18 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.
rules
1/10/2024 -- 08:34:18 - <Info> -- Ignoring file 4e6a132a847628f220180159c03f96d3/rules/emerging-
deleted.rules
1/10/2024 -- 08:34:20 - <Info> -- Loaded 53066 rules.
1/10/2024 -- 08:34:20 - <Info> -- Disabled 14 rules.
1/10/2024 -- 08:34:20 - <Info> -- Enabled 0 rules.
1/10/2024 -- 08:34:20 - <Info> -- Modified 0 rules.
1/10/2024 -- 08:34:20 - <Info> -- Dropped 0 rules.
1/10/2024 -- 08:34:20 - <Info> -- Enabled 136 rules for flowbit dependencies.
1/10/2024 -- 08:34:20 - <Info> -- Backing up current rules.
1/10/2024 -- 08:34:22 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total
: 53066; enabled: 40033; added: 0; removed 0; modified: 0
1/10/2024 -- 08:34:22 - <Info> -- Writing /var/lib/suricata/rules/classification.config

```



BY NC SA

Suricata Rules and Configurations

To **test** the **configuration** file of **Suricata**; **sudo suricata -T -c /etc/suricata/suricata.yaml -v**

All intrusion activities are in the **.log** file; the **.json** contains the same **collected/detected** intrusions but in **JSON** format.

```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
└─# suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: this is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast_output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats_output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 40034 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 4003/ signatures processed. 1221 are IP-only rules, 4125 are inspecting packet pay
load, 34481 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
(root@kali)-[~]
└─#
  
```

Running on the **IDS** mode

There are **40034** rules **successfully** loaded, and **0** failed

Running Suricata

- Run as a **daemon**
 - **sudo systemctl start suricata.service**
- Check the **status** of the **Suricata** tool
 - **sudo systemctl status suricata.service**

```

root@kali: ~
File Actions Edit View Help
Info: detect: 40037 signatures processed. 1221 are IP-only rules, 4125 are inspecting packet pay
load, 34481 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.

(root@kali)-[~]
└─$ systemctl start suricata.service Start the Suricata tool

(root@kali)-[~]
└─$ systemctl status suricata.service Check the status of Suricata
● Suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
   Active: active (running) since Tue 2024-10-01 07:59:53 EDT; 30s ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata.io/documentation/
   Process: 63345 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml -->
   Main PID: 63346 (Suricata-Main)
     Tasks: 10 (limit: 4611)
    Memory: 438.8M (peak: 439.3M)
       CPU: 26.808s
    CGroup: /system.slice/suricata.service
           └─63346 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile >

Oct 01 07:59:53 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon ...
Oct 01 07:59:53 kali suricata[63345]: i: suricata: This is Suricata version 7.0.3 RELEASE runni>
Oct 01 07:59:53 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-17/17 (END)

```

Now it means that the **tool** is **running** on the background

Suricata log Files

Check all log files generated by Suricata for network traffic analysis.

`ls -al /var/log/suricata`

```

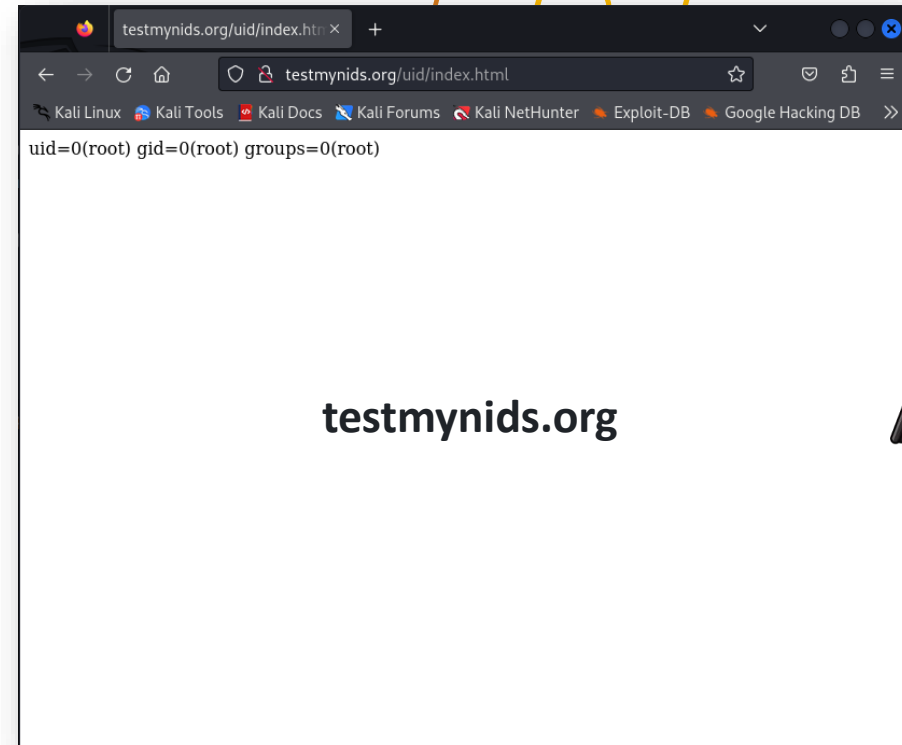
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# ls -al /var/log/suricata
total 100844
drwxr-xr-x  2 root root   4096 Sep 29 11:04 .
drwxr-xr-x 23 root root   4096 Oct  1 07:14 ..
-rw-r--r--  1 root root 978490 Oct  1 08:44 eve.json
-rw-r--r--  1 root root     0 Sep 29 11:04 eve.json.1
-rw-r--r--  1 root root 5382144 Apr 22 15:27 eve.json.1-2024052102.backup
-rw-r--r--  1 root root 14114816 May 21 02:55 eve.json.1-2024052805.backup
-rw-r--r--  1 root root     0 May 28 05:54 eve.json.1-2024080605.backup
-rw-r--r--  1 root root     0 Aug  6 05:25 eve.json.1-2024081305.backup
-rw-r--r--  1 root root 43995136 Aug 13 05:22 eve.json.1-2024082705.backup
-rw-r--r--  1 root root     0 Aug 27 05:03 eve.json.1-2024092314.backup
-rw-r--r--  1 root root     0 Sep 23 14:18 eve.json.1-2024092911.backup
-rw-r--r--  1 root root    227 Oct  1 08:40 fast.log
-rw-r--r--  1 root root     0 Sep 29 11:04 fast.log.1
-rw-r--r--  1 root root   2093 Apr 22 15:27 fast.log.1-2024052102.backup
-rw-r--r--  1 root root   2024 May 21 02:55 fast.log.1-2024052805.backup
-rw-r--r--  1 root root     0 May 28 05:54 fast.log.1-2024080605.backup
-rw-r--r--  1 root root     0 Aug  6 05:25 fast.log.1-2024081305.backup
-rw-r--r--  1 root root 46655 Aug 13 05:22 fast.log.1-2024082705.backup
-rw-r--r--  1 root root     0 Aug 27 05:03 fast.log.1-2024092314.backup
-rw-r--r--  1 root root     0 Sep 23 14:18 fast.log.1-2024092911.backup
-rw-r--r--  1 root root 330697 Oct  1 08:44 stats.log
-rw-r--r--  1 root root     0 Sep 29 11:04 stats.log.1
-rw-r--r--  1 root root 2850816 Apr 22 15:27 stats.log.1-2024052102.backup
-rw-r--r--  1 root root 7102464 May 21 02:55 stats.log.1-2024052805.backup
-rw-r--r--  1 root root     0 May 28 05:54 stats.log.1-2024080605.backup
-rw-r--r--  1 root root     0 Aug  6 05:25 stats.log.1-2024081305.backup
-rw-r--r--  1 root root 28381184 Aug 13 05:22 stats.log.1-2024082705.backup
-rw-r--r--  1 root root     0 Aug 27 05:03 stats.log.1-2024092314.backup
-rw-r--r--  1 root root     0 Sep 23 14:18 stats.log.1-2024092911.backup
-rw-r--r--  1 root root   4952 Oct  1 08:37 suricata.log
-rw-r--r--  1 root root     0 Sep 29 11:04 suricata.log.1
-rw-r--r--  1 root root   25641 Apr 22 15:27 suricata.log.1-2024052102.backup
-rw-r--r--  1 root root   7365 May 21 02:55 suricata.log.1-2024052805.backup
-rw-r--r--  1 root root     0 May 28 05:54 suricata.log.1-2024080605.backup
-rw-r--r--  1 root root     0 Aug  6 05:25 suricata.log.1-2024081305.backup
-rw-r--r--  1 root root   1586 Aug 13 05:22 suricata.log.1-2024082705.backup
-rw-r--r--  1 root root     0 Aug 27 05:03 suricata.log.1-2024092314.backup
-rw-r--r--  1 root root     0 Sep 23 14:18 suricata.log.1-2024092911.backup

```

Intrusion Detection using Suricata

- **Test Suricata**
 - **Visit:** <http://testmynids.org/uid/index.html>
- **Check the log:**
 - **sudo cat /var/log/suricata/fast.log**

```
kali@kali: ~  
File Actions Edit View Help  
drwxr-xr-x 4 root root 4096 Apr 8 18:39 ..  
-rw-r--r-- 1 root root 3228 Apr 8 18:39 classification.config  
-rw-r--r-- 1 root root 28320075 Apr 8 18:39 suricata.rules  
  
(kali@kali)~  
$ sudo cat /var/log/suricata/fast.log  
04/10/2024-06:55:53.676710 [++] [1:2100,98:7] GPL ATTACK_RESPONSE id c  
heck returned root [**] [Classification: Potentially Bad Traffic] [Prio  
rity: 2] {TCP} 13.32.110.51:80 → 192.168.122.203:37862  
  
(kali@kali)~  
$
```



GitHub - 3CORESec/testmynids.org: A website and framework for testing NIDS detection

Intrusion Detection using Suricata

- Execute the **ping command** from the **Kali admin device** to any **device/server**, such as **Google**.
- Visit **the testmynids.org/uid/index.html** on the **server device** (IP end with **.109**) in your network.

All **traffic** communication in **Suricata** will be **collected** and **stored** in the **fast.log**.

- Check the log:
 - **sudo cat /var/log/suricata/fast.log**

```

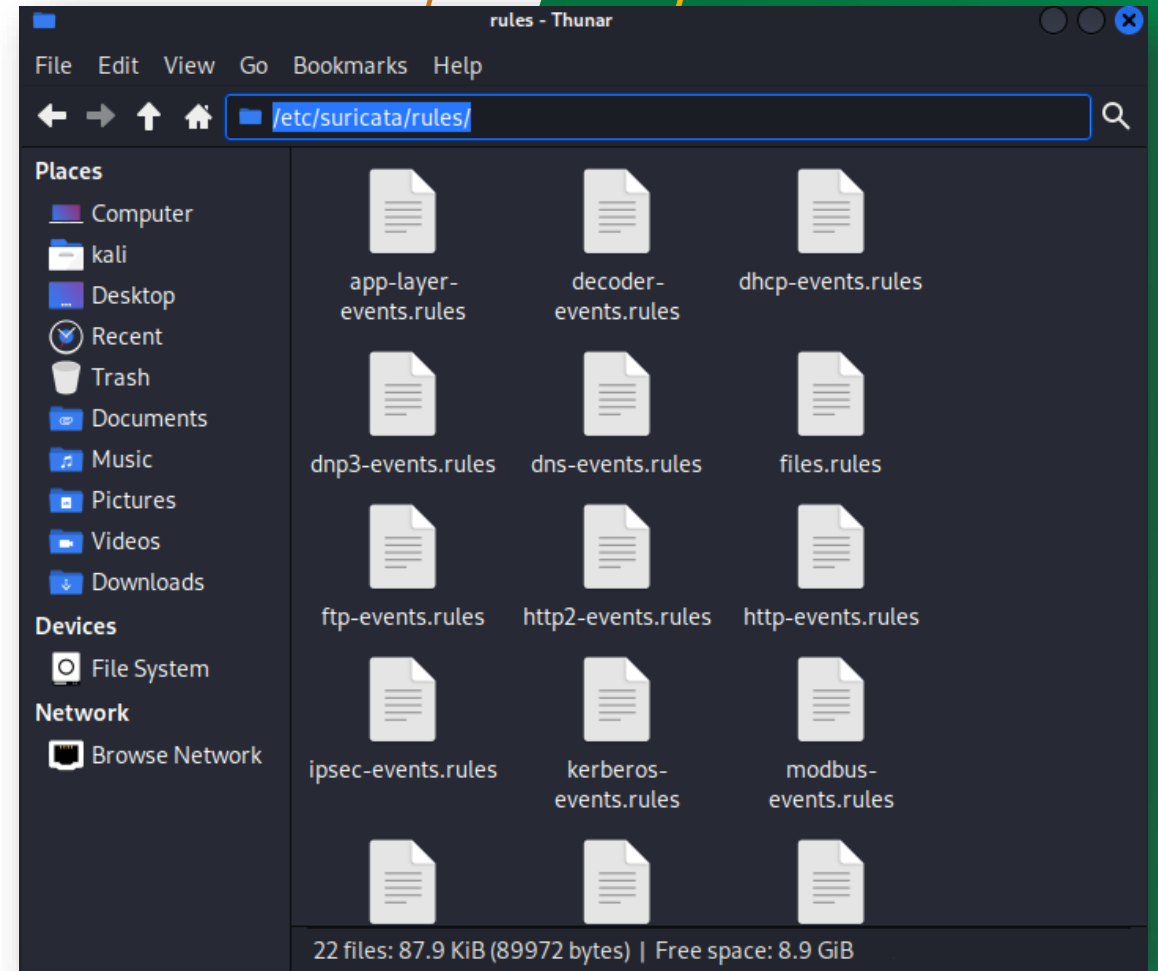
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
└─# cat /var/log/suricata/fast.log
10/01/2024-08:40:33.615027  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.122.203:68 → 192.168.122.1:67
10/01/2024-08:51:12.555139  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 3.165.206.84:80 → 192.168.122.203:42920
10/01/2024-08:52:57.124540  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Priority: 3] {ICMP} 3.165.206.97:0 → 192.168.122.203:0
10/01/2024-08:54:25.695249  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67
10/01/2024-08:56:56.233802  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 3.165.206.97:80 → 192.168.122.109:42924

(root@kali)-[~]
└─#
  
```

Customize Rules for Suricata

All rules are store on: `/etc/suricata/rules`



Customize Rules for Suricata

Check the configuration file

Suricata -T -c /etc/suricata/suricata.yaml -v

It seems that everything running well 😊

- **Run Suricata**
 - **Sudo systemctl start suricata.service**

```
kali@kali: ~/Desktop
File Actions Edit View Help
riority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67

(kali@kali)-[~/Desktop]
└─$ sudo cp -f suricata.yaml /etc/suricata

(kali@kali)-[~/Desktop]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 37121 rules successfully loaded, 0 rules failed,
0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 37124 signatures processed. 1183 are IP-only rules, 4910 are inspecting
packet payload, 30819 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.

(kali@kali)-[~/Desktop]
└─$
```

Run Customize Rules

- Check the log:
 - `sudo cat /var/log/suricata/fast.log`

```

root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# cat /var/log/suricata/fast.log
10/01/2024-08:40:33.615027  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.122.203:68 → 192.168.122.1:67
10/01/2024-08:51:12.555139  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 3.165.206.84:80 → 192.168.122.203:42920
10/01/2024-08:52:57.124540  [**] [1:1:1] Ping ICMP [**] [Classification: (null)] [Priority: 3] {ICMP} 3.165.206.97:0 → 192.168.122.203:0
10/01/2024-08:54:25.695249  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.122.27:68 → 192.168.122.1:67
10/01/2024-08:56:56.233802  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 3.165.206.97:80 → 192.168.122.109:49294

(root@kali)-[~]
#

```

- Ping
 - Ping command from the admin Kai device to testmynids website

The **results** may not **appear immediately**. Please wait for a while until the **newly added rule** detects the ping **activities** across your **network**.

Admin Kali pings the testmynids website

Stop Suricata

- Stop Suricata
 - **Sudo systemctl stop suricata.service**

```

root@kali: ~
File Actions Edit View Help

(root@kali) [~]
# systemctl stop suricata.service

(root@kali) [~]
#

```

- Status Suricata
 - **Sudo systemctl status suricata.service**

```

root@kali: ~
File Actions Edit View Help

(root@kali) [~]
# systemctl status suricata.service
o suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:suricata(8)
        man:suricatasc(8)
        https://suricata.io/documentation/

Oct 01 08:53:43 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.
Oct 01 08:53:43 kali systemd[1]: suricata.service: Consumed 42.727s CPU time, 110.7M memory peak.
Oct 01 08:53:52 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon ...
Oct 01 08:53:52 kali suricata[90286]: i: suricata: This is Suricata version 7.0.3 RELEASE running.
Oct 01 08:53:52 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
Oct 01 09:26:35 kali systemd[1]: Stopping suricata.service - Suricata IDS/IDP daemon ...
Oct 01 09:26:35 kali suricatasc[106278]: {"message": "Closing Suricata", "return": "OK"}
Oct 01 09:26:37 kali systemd[1]: suricata.service: Deactivated successfully.
Oct 01 09:26:37 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.
lines 1-16 ... skipping ...
o suricata.service - Suricata IDS/IDP daemon
  Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:suricata(8)
        man:suricatasc(8)
        https://suricata.io/documentation/

Oct 01 08:53:43 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.
Oct 01 08:53:43 kali systemd[1]: suricata.service: Consumed 42.727s CPU time, 110.7M memory peak.
Oct 01 08:53:52 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon ...
Oct 01 08:53:52 kali suricata[90286]: i: suricata: This is Suricata version 7.0.3 RELEASE running.
Oct 01 08:53:52 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
Oct 01 09:26:35 kali systemd[1]: Stopping suricata.service - Suricata IDS/IDP daemon ...
Oct 01 09:26:35 kali suricatasc[106278]: {"message": "Closing Suricata", "return": "OK"}
Oct 01 09:26:37 kali systemd[1]: suricata.service: Deactivated successfully.
Oct 01 09:26:37 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.
Oct 01 09:26:37 kali systemd[1]: suricata.service: Consumed 1min 1.793s CPU time.
~
~
~
~
~
~
lines 1-17/17 (END) ... skipping ...
o suricata.service - Suricata IDS/IDP daemon

```

Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at