

Suricata NIDS Tools Project Report

Prepared By: Olatunji Lawal

5th July, 2025

Outline

1.0	Summary	3
2.0	Objective	3
3.0	Environment Setup	3
4.0	Execution Step	4
4.1	Install Suricata	4
4.2	Update Suricata	5
4.3	Set a New Rule in Rule Destination	6
4.4	Add a New Rule	6
4.5	Start Suricata	7
4.6	Run Suricata	7
4.7	Trigger the Alert	7
4.8	Investigate	9
5.0	Key learning	10
6.0	Conclusion	10

1. Summary

Suricata is an advanced, open-source network intrusion detection and prevention system (NIDS/NIPS) created by the Open Information Security Foundation. It does real-time packet analysis, protocol identification, and generates alerts for questionable network activities. This project explains how to install, configure, and utilize the Suricata Intrusion Detection System (IDS) to monitor and warn network traffic. It takes a step-by-step approach, from installation to alarm investigation, which includes custom rule generation.

2. Objectives

- Install and configure Suricata.
 - Update Suricata and its rule sets
 - Add a custom detection rule
 - Run and test Suricata to trigger and analyze alerts
 - Document findings for analysis and reporting
-

3. Environment Setup

- **Operating System:** Kali Linux - Debian
- **Suricata Version:** [7.1.10]
- **Tools Used:** Terminal

4. Execution Steps

4.1: Install Suricata

Suricata must be installed on the target host system using the appropriate package for the operating system. The interface needs to be established first by using **ifconfig** command.

Commands used to install Suricata (for Kali/Debian):

sudo apt update

sudo apt install suricata

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.72 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2a0d:3344:832:5510:69af:9dca:4fd9:d87 prefixlen 64 scopeid 0<global>
    inet6 fdb3:b698:5a2f:10:a00:27ff:fe6c:6eb8 prefixlen 64 scopeid 0<global>
    inet6 2a0d:3344:832:5510:a00:27ff:fe6c:6eb8 prefixlen 64 scopeid 0<global>
    inet6 fdb3:b698:5a2f:10:4f6f:ad9c:776c:5803 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe6c:6eb8 prefixlen 64 scopeid 0<link>
    ether 08:00:27:6c:6e:b8 txqueuelen 1000 (Ethernet)
    RX packets 260 bytes 36092 (35.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 49 bytes 12394 (12.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali㉿kali)-[~]
$ sudo apt install suricata
[sudo] password for kali:
Installing:
  suricata

Installing dependencies:
  isa-support      librtt-bus-vdev25  librtt-log25      librtt-pci25      oinkmaster
  libfdt1          librtt-eal25      librtt-mbuf25     librtt-rcu25      snort-rules-default
  libhttp2         librtt-ethdev25   librtt-mempool25  librtt-ring25     sse3-support
  libhyperscan5    librtt-hash25     librtt-meter25    librtt-sched25    sse4.2-support
  libnetfilter-log1 librtt-ip-frag25   librtt-net-bond25 librtt-telemetry25 suricata-update
  librtt-bus-pci25 librtt-kvargs25    librtt-net25      libxdp1

Suggested packages:
  snort | snort-pgsql | snort-mysql libtcmalloc-minimal4

Summary:
  Upgrading: 0, Installing: 30, Removing: 0, Not Upgrading: 0
  Download size: 6,991 kB
  Space needed: 32.1 MB / 17.9 GB available
```

4.2: Update Suricata

To ensure the latest threat detection capabilities, updated rule sets with the latest version:

sudo suricata-update

```
(kali@kali)-[/etc/suricata]
$ sudo suricata-update
2/7/2025 -- 13:27:40 - <Info> -- Using data-directory /var/lib/suricata.
2/7/2025 -- 13:27:40 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
2/7/2025 -- 13:27:40 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
2/7/2025 -- 13:27:40 - <Info> -- Found Suricata version 7.0.10 at /usr/bin/suricata.
2/7/2025 -- 13:27:40 - <Info> -- Loading /etc/suricata/suricata.yaml
2/7/2025 -- 13:27:40 - <Info> -- Disabling rules for protocol postgres
2/7/2025 -- 13:27:40 - <Info> -- Disabling rules for protocol modbus
2/7/2025 -- 13:27:40 - <Info> -- Disabling rules for protocol dnp3
2/7/2025 -- 13:27:40 - <Info> -- Disabling rules for protocol enip
2/7/2025 -- 13:27:40 - <Info> -- No sources configured, will use Emerging Threats Open
2/7/2025 -- 13:27:40 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.10/emerg
ing.rules.tar.gz.
100% - 4957270/4957270
2/7/2025 -- 13:27:53 - <Info> -- Done.
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.r
ules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rul
es
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/http2-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rule
s
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/mqtt-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/quic-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/rfb-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/ssh-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rule
s
2/7/2025 -- 13:27:53 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
2/7/2025 -- 13:27:53 - <Info> -- Ignoring file f625293e2432dbf07497d06349de6f0b/rules/emerging-deleted
.rules
2/7/2025 -- 13:27:57 - <Info> -- Loaded 59677 rules.
2/7/2025 -- 13:27:58 - <Info> -- Disabled 13 rules.
2/7/2025 -- 13:27:58 - <Info> -- Enabled 0 rules.
2/7/2025 -- 13:27:58 - <Info> -- Modified 0 rules.
2/7/2025 -- 13:27:58 - <Info> -- Dropped 0 rules.
2/7/2025 -- 13:27:58 - <Info> -- Enabled 136 rules for flowbit dependencies.
2/7/2025 -- 13:27:58 - <Info> -- Backing up current rules.
2/7/2025 -- 13:27:58 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 59677
; enabled: 44083; added: 59677; removed 0; modified: 0
2/7/2025 -- 13:27:58 - <Info> -- Writing /var/lib/suricata/rules/classification.config
2/7/2025 -- 13:27:59 - <Info> -- Testing with suricata -T.
```

4.3: Set a New Rule in Rule Destination

A custom rule was added to detect specific network activity.

Custom rules are typically stored in `/etc/suricata/rules/`

```
(kali@kali)-[/etc/suricata]
$ cd rules

(kali@kali)-[/etc/suricata/rules]
$ ls
app-layer-events.rules  dhcp-events.rules  ftp-events.rules  kerberos-events.rules  ntp-events.rules  smtp-events.rules
cybersec.rules          dnp3-events.rules  http2-events.rules  modbus-events.rules    quic-events.rules  ssh-events.rules
cybersec.rules.save     dns-events.rules   http-events.rules  mqtt-events.rules       rfb-events.rules   stream-events.rules
decoder-events.rules    files.rules        ipsec-events.rules  nfs-events.rules        smb-events.rules    tls-events.rules
```

```
(olatumji@Desktop)-[/var/lib/suricata/rules]
$ sudo rm -r cybersec.rules

(kolatumji@Desktop)-[/var/lib/suricata/rules]
$ ls
classification.config  suricata.rules

(kolatumji@Desktop)-[/var/lib/suricata/rules]
$
```

Ensure this is referenced in the main configuration file:

`/etc/suricata/suricata.yaml`

```
(olatumji@Desktop)-[/etc/suricata]
$ sudo nano suricata.yaml
```

4.4: Add a New Rule

Add a basic ICMP alert rule to detect ping traffic:

- `alert icmp any any → any any (msg: "I detected an ICMP request"; itype:8; sid:1000001; rev:1)`

```
GNU nano 8.4 suricata.yaml
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hash5tuplesorted

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

default-rule-path: /var/lib/suricata/rules

rule-files:
- suricata.rules
- cybersec.rules
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line  M-E Redo
```

```
(kali@kali)-[/etc/suricata]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -v
Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
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
```

4.5: Start Suricata

Checked status:

```
sudo systemctl status suricata
```

```
sudo systemctl start suricata
```

```
File Actions Edit View Help
$ sudo nano suricata.yaml

(olatumji@Desktop)-[/etc/suricata]
$ sudo nano suricata.yaml

(olatumji@Desktop)-[/etc/suricata]
$ cd

(olatumji@Desktop)-[~]
$ sudo systemctl start suricata

(olatumji@Desktop)-[~]
$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-07-05 10:49:35 BST; 20s ago
     Invocation: cac47dd30c494566bde42c488982484a
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
   Process: 30313 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=0)
   Main PID: 30314 (Suricata-Main)
     Tasks: 1 (limit: 4546)
    Memory: 306.7M (peak: 306.7M)
       CPU: 21.043s
    CGroup: /system.slice/suricata.service
```

4.6: Run Suricata

Suricata was run in test mode and in live monitoring mode using:

```
sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -V
```

```
(kali@kali)-[~]
$ sudo suricata -c/etc/suricata/suricata.yaml -i eth0 -v

Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
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
```

4.7: Trigger the Alert

Used ping command to generate ICMP traffic and trigger the rule:


```
(olatumji@Desktop)-[~]  
$ ping -c 4 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=67.1 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=44.8 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=32.3 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=70.3 ms  
  
— 8.8.8.8 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3012ms  
rtt min/avg/max/mdev = 32.277/53.608/70.276/15.740 ms
```

4.8: Investigate

Suricata logs were checked at:

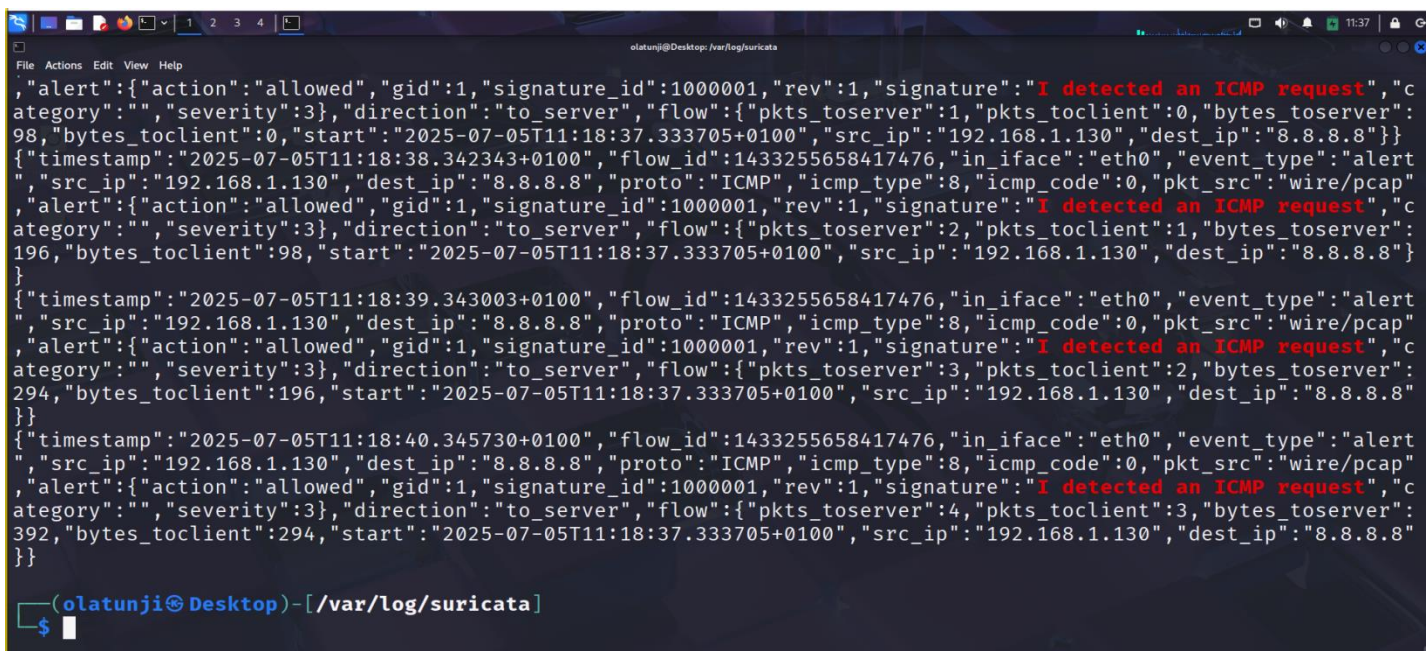
/var/log/suricata/eve.json

Used the following tools:

- `cat /var/log/suricata/fast.log`

Summary of findings:

- The custom ICMP rule was triggered successfully.
- Source and destination IPs were identified.
- Timestamp and payload were analyzed for confirmation.



```
olatumji@Desktop: /var/log/suricata
File Actions Edit View Help
{"alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected an ICMP request","category":"","severity":3},"direction":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":98,"bytes_toclient":0,"start":"2025-07-05T11:18:37.333705+0100","src_ip":"192.168.1.130","dest_ip":"8.8.8.8"}}
{"timestamp":"2025-07-05T11:18:38.342343+0100","flow_id":1433255658417476,"in_iface":"eth0","event_type":"alert","src_ip":"192.168.1.130","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected an ICMP request","category":"","severity":3},"direction":"to_server","flow":{"pkts_toserver":2,"pkts_toclient":1,"bytes_toserver":196,"bytes_toclient":98,"start":"2025-07-05T11:18:37.333705+0100","src_ip":"192.168.1.130","dest_ip":"8.8.8.8"}}
{"timestamp":"2025-07-05T11:18:39.343003+0100","flow_id":1433255658417476,"in_iface":"eth0","event_type":"alert","src_ip":"192.168.1.130","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected an ICMP request","category":"","severity":3},"direction":"to_server","flow":{"pkts_toserver":3,"pkts_toclient":2,"bytes_toserver":294,"bytes_toclient":196,"start":"2025-07-05T11:18:37.333705+0100","src_ip":"192.168.1.130","dest_ip":"8.8.8.8"}}
{"timestamp":"2025-07-05T11:18:40.345730+0100","flow_id":1433255658417476,"in_iface":"eth0","event_type":"alert","src_ip":"192.168.1.130","dest_ip":"8.8.8.8","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":1,"signature":"I detected an ICMP request","category":"","severity":3},"direction":"to_server","flow":{"pkts_toserver":4,"pkts_toclient":3,"bytes_toserver":392,"bytes_toclient":294,"start":"2025-07-05T11:18:37.333705+0100","src_ip":"192.168.1.130","dest_ip":"8.8.8.8"}}
(olatumji@Desktop)-[/var/log/suricata]
$
```

5. Key Learnings

- Writing and testing custom IDS rules
- Interpreting Suricata alert logs
- Understanding packet behaviour triggering alerts
- Real-time IDS monitoring

6. Conclusion

Using a custom rule, the Suricata IDS was successfully configured, tested, and validated. This process shows how to successfully setup Suricata for simple threat detection. I've laid the groundwork for future network defense. This real-world application improved comprehension of log analysis and NIDS operation. Now, Suricata may be extended to include threat hunting, complete intrusion detection, and integration with programs like Splunk, SIEM, or ELK Slack.

Report prepared by:

Olatunji Lawal

Cybersecurity Analyst