



## 5. Network Defense with Open-Source Tools

### Activities:

- **Tools:** Suricata, Elastic SIEM, CrowdSec.
- **Task:** Configure Suricata to block malicious IPs and map alerts to MITRE ATT&CK.

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ ]
[ ]
File Actions Edit View Help
(blank@kali):~$
(blank@kali):~$ sudo apt update
[ ] sudo apt install suricata -y
[sudo] password for blank:
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
443 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
suricata

Installing dependencies:
isa-support libhyperscan5 librtte-bus-vdev25 librtte-hash25 librtte-log25 librtte-meter25 librtte-pci25 librtte-sched25 oinkmaster sse4.2-support
libfdt1 libnetfilter-log1 librtte-eal25 librtte-ip-frag25 librtte-mbuf25 librtte-net-bond25 librtte-rcu25 librtte-telemetry25 snort-rules-default suricata-update
libnft2 librtte-bus-pci25 librtte-ethdev25 librtte-kvargs25 librtte-mempool25 librtte-net25 librtte-ring25 libxdp1 sse3-support

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

Summary:
Upgrading: 0, Installing: 30, Removing: 0, Not Upgrading: 443
Download size: 6,992 kB
Space needed: 32.2 MB / 55.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 isa-support amd64 27 [34.9 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 sse4.2-support amd64 27 [3,692 B]
Get:3 http://kali.download/kali kali-rolling/main amd64 libhyperscan5 amd64 5.4.2-3 [72.9 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libnft2 amd64 1:0.5.50-1 [2.6 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libhyperscan5 amd64 5.4.2-3 [2,695 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libnetfilter-log1 amd64 1.0.2-4+b1 [13.3 kB]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 libfdt1 amd64 1.7.2-2+b1 [20.0 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 librtte-log25 amd64 24.11.2-2 [23.7 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 librtte-kvargs25 amd64 24.11.2-2 [17.8 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 librtte-telemetry25 amd64 24.11.2-2 [26.7 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 librtte-ring25 amd64 24.11.2-2 [20.2 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 librtte-mempool25 amd64 24.11.2-2 [30.3 kB]
Get:13 http://kali.download/kali kali-rolling/main amd64 librtte-meter25 amd64 24.11.2-2 [17.6 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 librtte-mbuf25 amd64 24.11.2-2 [36.2 kB]
Get:15 http://kali.download/kali kali-rolling/main amd64 librtte-net25 amd64 24.11.2-2 [17.6 kB]
Get:16 http://mirror.sg.gs/kali kali-rolling/main amd64 librtte-eal25 amd64 24.11.2-2 [159 kB]
Get:17 http://kali.download/kali kali-rolling/main amd64 librtte-net25 amd64 24.11.2-2 [23.7 kB]
Get:18 http://kali.download/kali kali-rolling/main amd64 librtte-ethdev25 amd64 24.11.2-2 [136 kB]
Get:19 http://kali.download/kali kali-rolling/main amd64 librtte-bus-pci25 amd64 24.11.2-2 [37.0 kB]
Get:20 http://kali.download/kali kali-rolling/main amd64 librtte-bus-vdev25 amd64 24.11.2-2 [21.5 kB]
Get:21 http://kali.download/kali kali-rolling/main amd64 librtte-rcu25 amd64 24.11.2-2 [22.1 kB]
Get:22 http://mirror.kku.ac.th/kali kali-rolling/main amd64 sse3-support amd64 27 [3,736 B]
Get:23 http://kali.download/kali kali-rolling/main amd64 librtte-nas25 amd64 24.11.2-2 [48.5 kB]
Get:24 http://kali.download/kali kali-rolling/main amd64 librtte-ip-frag25 amd64 24.11.2-2 [33.5 kB]
Get:25 http://kali.download/kali kali-rolling/main amd64 librtte-net-bond25 amd64 24.11.2-2 [61.3 kB]
Get:26 http://kali.download/kali kali-rolling/main amd64 librtte-net25 amd64 24.11.2-2 [17.6 kB]
Get:27 http://kali.download/kali kali-rolling/main amd64 suricata amd64 1:7.0.10-1 [2,979 kB]
Get:28 http://mirror.kku.ac.th/kali kali-rolling/main amd64 suricata-update amd64 1.3.6-1 [65.1 kB]
```

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ ]
[ ]
File Actions Edit View Help
(blank@kali):~$
(blank@kali):~$ nano /etc/suricata/suricata.yaml
GNU nano 2.9.4 /etc/suricata/suricata.yaml

filename: packet_stats.csv
# profiling of locking. Only available when Suricata was built with
# --enable-profiling-locks.
#
enabled: no
filename: lock_stats.log
append: yes

pcap-log:
enabled: no
filename: pcaplog_stats.log
append: yes

# Netfilter Integration
#
# When running in NFQ inline mode, it is possible to use a simulated
# non-terminal NQUEUE verdict.
# This permits sending all needed packet to Suricata via this rule:
# iptables -I FORWARD -m mark ! --mark $MARK/$MASK -j NQUEUE
# and below, you can have your standard filtering ruleset. To activate
# this mode, you need to set mode to 'repeat'
# If you want a packet to be sent to another queue after an ACCEPT decision
# set the mode to 'route' and set next-queue value.
# On linux >= 3.13, you can set batchcount to a value > 1 to improve performance
# by processing several packets before sending a verdict (worker runtime only).
# On linux >= 3.8, you can set the fail-open option to yes to have the kernel
# accept the packet if Suricata is not able to keep pace.
# Bypass mark and mask can be used to implement NQ bypass. If bypass mark is
# set then the NQ bypass is activated. Suricata will set the bypass mark/mask
# on packet of a flow that need to be bypassed. The Netfilter ruleset has to
# directly accept all packets of a flow once a packet has been marked.
nfq:
mode: accept
repeat-mask: 1
repeat-mask: 1
bypass-mark: 1
bypass-mask: 1
route-queue: 1
batchcount: 10
fail-open: yes

nfting support
nfting:
# netlink multicast group
# (the same as the iptables --nft-group param)
```

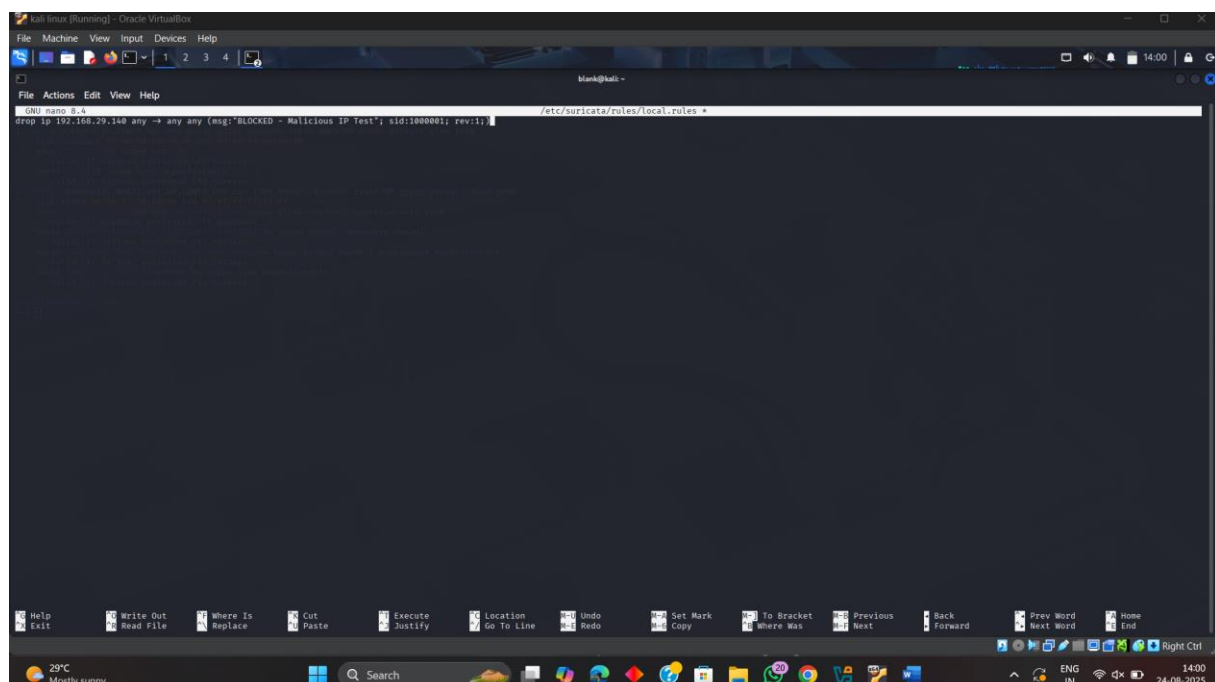


```
# Linux high speed capture support
af-packet:
- interface: eth0
  # Number of receive threads. "auto" uses the number of cores
  threads: 1
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
  # This is only supported for Linux kernel > 3.1
  # possible value are:
  # * cluster_flow: all packets of a given flow are sent to the same socket
  # * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
  # * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
  # socket. Requires at least Linux 3.14.
  # * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst for
  # more info.
  # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
  # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
  # cluster_rollover has been deprecated; if used, it'll be replaced with cluster_flow.
  cluster-type: cluster_flow
  # In some fragmentation cases, the hash can not be computed. If "defrag" is set
  # to yes, the kernel will do the needed defragmentation before sending the packets.
  defrag: yes
  # To use the ring feature of AF_PACKET, set 'use-mmap' to yes
  #use-mmap: yes
  # Lock memory map to avoid it being swapped. Be careful that over
  # subscribing could lock your system
  #mmap-locked: yes
  # Use tpacket_v3 capture mode, only active if use-mmap is true
  # Don't use it in IPS or TAP mode as it causes severe latency
  #tpacket-v3: yes
  # Ring size will be computed with respect to "max-pending-packets" and number
  # of threads. You can set manually the ring size in number of packets by setting
  # the following value. If you are using flow "cluster-type" and have really network
  # intensive single-flow you may want to set the "ring-size" independently of the number
  # of threads:
  #ring-size: 2048
  # Block size is used by tpacket_v3 only. It should set to a value high enough to contain
  # a decent number of packets. Size is in bytes so please consider your MTU. It should be
  # a power of 2 and it must be multiple of page size (usually 4096).
  #block-size: 32768
```

## Enhanced Tasks:

- **Suricata Rule:** Create a rule to block a malicious IP:

drop ip 192.168.1.100 any -> any any (msg:"Block Malicious IP"; sid:1000001;)



- Test by pinging from another VM.



- **ATT&CK Mapping:** Map a Suricata alert to a MITRE ATT&CK technique:

Alert	Tactic	Technique	Notes
-----	-----	-----	-----
Suspicious HTTP	Command and Control	T1071	Outbound traffic to C2

## MITRE ATTsCK Mapping Summary

Alert Name	Tactic	Technique ID	Technique Name	Notes
Suspicious HTTP	Command and control	T1071	Application Layer Protocol	Outbound traffic to C2