Suricata

1. Environment Setup

- Install Suricata on a virtual machine. -Ensure the system has all necessary dependencies installed (e.g., libpcap, libnet, etc.).
- Update the system and Suricata to the latest stable versions.

```
┌──(kali㉿kali)-[~]
└─$ suricata -V
This is Suricata version 7.0.6 RELEASE
```

2. Initial Configuration

- Configure the Suricata YAML file (/etc/suricata/suricata.yaml).

  Command: **sudo nano /etc/suricata/suricata.yaml**

- Set up network interfaces for live traffic capture.
- Configure logging to output to both JSON and EVE (for later analysis).

```
# Linux high speed capture support
af-packet:
  - interface: eth0
```

```
  # Extensible Event Format (nicknamed EVE) event log in JSON format
  - eve-log:
      enabled: yes
      filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
      filename: eve.json
```

3. Basic Testing

- Start Suricata in live mode and ensure it is capturing traffic.

```
┌──(kali㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
W: detect: 1 rule files specified, but no rules were loaded!
i: threads: Threads created → W: 2 FM: 1 FR: 1   Engine started.
```

- Generate some network traffic and verify it is being logged by Suricata.
- Use tools like curl, ping, and nmap to generate various types of traffic.

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (142.251.5.100) 56(84) bytes of data.
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=1 ttl=57 time=44.5 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=2 ttl=57 time=36.7 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=3 ttl=57 time=35.4 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=4 ttl=57 time=25.8 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=5 ttl=57 time=55.0 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=6 ttl=57 time=35.4 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=7 ttl=57 time=33.8 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=8 ttl=57 time=31.2 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=9 ttl=57 time=25.9 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=10 ttl=57 time=30.0 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=11 ttl=57 time=30.2 ms
64 bytes from wg-in-f100.1e100.net (142.251.5.100): icmp_seq=12 ttl=57 time=121 ms
^C
── google.com ping statistics ──
12 packets transmitted, 12 received, 0% packet loss, time 11025ms
rtt min/avg/max/mdev = 25.755/42.097/121.242/25.100 ms

┌──(kali㉿kali)-[~]
└─$ cd /var/log/suricata/eve.json
bash: cd: /var/log/suricata/eve.json: Not a directory

┌──(kali㉿kali)-[~]
└─$ cd /var/log/suricata/

┌──(kali㉿kali)-[/var/log/suricata]
└─$ ls
eve.json  fast.log  stats.log  suricata.log

┌──(kali㉿kali)-[/var/log/suricata]
└─$ cat eve.json
{"timestamp":"2024-09-12T08:01:03.831211-0400","event_type":"stats","stats":{"uptime":8,"capture":{"kernel_packet
,"kernel_drops":0,"errors":0,"afpacket":{"busy_loop_avg":0,"polls":137,"poll_signal":0,"poll_timeout":113,"poll_
24,"poll_errors":0,"send_errors":0}},"decoder":{"pkts":31,"bytes":3884,"invalid":0,"ipv4":14,"ipv6":2,"ethernet"
rp":15,"unknown_ethertype":0,"chdlc":0,"raw":0,"null":0,"sll":0,"tcp":0,"udp":16,"sctp":0,"esp":0,"icmpv4":0,"ic
0,"ppp":0,"pppoe":0,"geneve":0,"gre":0,"vlan":0,"vlan_qinq":0,"vlan_qinqinq":0,"vxlan":0,"vntag":0,"ieee8021ah":
edo":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":125,"max_pkt_size":217,"max_mac_addrs_src":0,"m
```

4. Understanding Suricata Rules

- Study the existing Suricata rules and understand their structure.
- Read the Suricata documentation on writing custom rules.

  6.1. Rules Format — Suricata 6.0.0 documentation

5. Creating Custom Rules

- Create at least 5 custom Suricata rules that detect specific types of network behavior (e.g., detecting SSH login attempts, HTTP requests to a specific URI, suspicious DNS queries).

```
┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ cat /etc/suricata/rules/local.rules
alert tcp any any → any 22 (msg:"SSH Login Attempt"; sid:100001;)
alert http any any → any any (msg:"HTTP Request to /admin"; content:"/admin"; sid:100002;)
alert dns any any → any any (msg:"Suspicious DNS Query"; content:"malicious.com"; sid:100003;)
alert tcp any any → any any (msg:"Nmap Scan Detected"; flags:S; sid:100004;)
alert tcp any any → any 31337 (msg:"Unusual Port 31337 Access"; sid:100005;)
```

- Test these rules by generating the appropriate network traffic and ensure they trigger correctly.

  The ssh rule was tested as shown below.

```
C:\Users\betta>ssh kali@192.168.0.109
kali@192.168.0.109's password:
Permission denied, please try again.
kali@192.168.0.109's password:
Permission denied, please try again.
kali@192.168.0.109's password:
```

The command for live capturing:

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

And

Command to check the eve.json file:

cat /var/log/suricata/eve.json


```
{"timestamp":"2024-09-13T06:06:53.221666-0400","flow_id":1457486919172025,"in_iface":"eth0","e
vent_type":"ssh","src_ip":"192.168.0.119","src_port":53395,"dest_ip":"192.168.0.109","dest_por
t":22,"proto":"TCP","pkt_src":"wire/pcap","tx_id":0,"ssh":{"client":{"proto_version":"2.0","so
ftware_version":"OpenSSH_for_Windows_8.6"},"server":{"proto_version":"2.0","software_version":
"OpenSSH_9.7p1"}}}
```

Second trying with success

```
C:\Users\betta>ssh kali@192.168.0.109
kali@192.168.0.109's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2
 (2024-05-30) x86_64

The programs included with the Kali GNU/Linux system are free sof
tware;
the exact distribution terms for each program are described in th
e
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 13 05:18:04 2024 from 192.168.0.119
┌──(kali㉿kali)-[~]
└─$
```

Eve.json file showing the traffic


```
{"timestamp":"2024-09-13T05:20:31.706471-0400","flow_id":222722335237895,"in_iface":"eth0","
event_type":"flow","src_ip":"192.168.0.119","src_port":53079,"dest_ip":"192.168.0.109","dest
_port":22,"proto":"TCP","app_proto":"ssh","flow":{"pkts_toserver":14,"pkts_toclient":13,"byt
es_toserver":2673,"bytes_toclient":2558,"start":"2024-09-13T05:20:16.969360-0400","end":"202
4-09-13T05:20:27.380408-0400","age":11,"state":"established","reason":"shutdown","alerted":f
alse},"tcp":{"tcp_flags":"1a","tcp_flags_ts":"1a","tcp_flags_tc":"1a","syn":true,"psh":true,
"ack":true,"state":"established","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2024-09-13T05:20:31.709031-0400","flow_id":623707292454657,"in_iface":"eth0","
event_type":"flow","src_ip":"1.0.168.192","dest_ip":"224.0.0.1","proto":"ICMP","icmp_type":9
,"icmp_code":0,"flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":60,"bytes_toclie
nt":0,"start":"2024-09-13T05:20:18.210754-0400","end":"2024-09-13T05:20:18.210754-0400","age
":0,"state":"new","reason":"shutdown","alerted":false}}
```


6. Deliverables

- Zip file with Logs showing Suricata successfully capturing and logging traffic.

```
┌──(kali㉿kali)-[/var/log/suricata]
└─$ ls
eve.json  fast.log  stats.log  suricata.log  suricata_logs.zip

┌──(kali㉿kali)-[/var/log/suricata]
└─$ sudo mv suricata_logs.zip ~/suricata_logs.zip

┌──(kali㉿kali)-[/var/log/suricata]
└─$ ls
eve.json  fast.log  stats.log  suricata.log

┌──(kali㉿kali)-[/var/log/suricata]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    hydra.restore  packages-microsoft-prod.deb  rtl8812au          Videos
Documents  ipchang.sh     Pictures                     suricata_logs.zip  zeek-5.1.1
Downloads  Music          Public                       Templates          zeek-5.1.1.tar.gz
```