Assignment-8

Comprehensive Report on Suricata Intrusion Detection System (IDS)

---

1. Introduction

- **IDS Used**: Suricata.
- **Objective**: To install, configure, and study the functionality of Suricata as an Intrusion Detection System (IDS) for monitoring network traffic, detecting threats, and analyzing malicious activities.
- **Overview**: Suricata is a high-performance IDS/IPS capable of real-time traffic analysis, protocol detection, and intrusion detection based on custom rules or predefined rule sets.

---

2. Installation Process

System Requirements

- **Operating System**: Ubuntu 22.04 LTS.
- **Dependencies**: Python, libpcap, libnetfilter-queue, and gcc.

Steps to Install Suricata

1. **Update the System**:

```
sudo apt update && sudo apt upgrade -y
```

2. **Add Suricata Repository and Install**:

```
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata -y
```

3. **Verify Installation**:
   Check Suricata version:

   ```
   suricata --build-info
   ```

   Expected Output: Displays the installed version and build details.
4. **Download Rule Sets**:
   Suricata uses rules to detect malicious activities. Download rules from **Emerging Threats**:

   ```
   sudo apt install suricata-update
   sudo suricata-update
   ```

---

3. Configuration

1. Set Up the Configuration File

- The main configuration file is located at `/etc/suricata/suricata.yaml`.
- Key sections to configure:
  - **Network Interfaces**:
    Define the interface for monitoring traffic. Update the `af-packet` section:

    ```
    af-packet:
      - interface: eth0
    ```

  - **Rules Path**: Ensure Suricata uses the updated rule sets:

    ```
    default-rule-path: /var/lib/suricata/rules
    rule-files:
      - suricata.rules
    ```

2. Enable Logging

Suricata logs alerts and events for analysis.

- Configure log paths in `suricata.yaml`:

```
outputs:
  - eve-log:
      enabled: yes
      filetype: json
      filename: /var/log/suricata/eve.json
```

3. Start Suricata in IDS Mode

Run Suricata as an IDS on the specified interface:

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

- **Flags**:
  - `-c`: Specifies the configuration file.
  - `-i`: Specifies the monitoring interface.

---

4. Testing and Analysis

Test the IDS with Malicious Traffic

1. **Generate Malicious Traffic**:
   Use tools like **nmap** or **Metasploit** to simulate attacks:

   ```
   nmap -sS -p 80,443 192.168.1.1
   ```

   Suricata detects the port scan and logs the alert.
2. **Analyze Logs**:
   Suricata logs events in `/var/log/suricata/`.
   - Open `eve.json` to view detected alerts:

     ```
     cat /var/log/suricata/eve.json | jq
     ```

     Sample Log Entry:

     ```
     {
       "timestamp": "2024-12-02T14:32:20.123456",
       "event_type": "alert",
       "alert": {
     ```

```
    "severity": 3,
    "signature": "ET SCAN Nmap Scan",
    "category": "Attempted Information Leak",
    "action": "alert"
  },
  "src_ip": "192.168.1.100",
  "dest_ip": "192.168.1.1"
}
```

Test Custom Rules

1. Add a custom rule to `/var/lib/suricata/rules/custom.rules`:

   ```
   alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:100001; rev:1;)
   ```

2. Include the rule file in `suricata.yaml`:

   ```
   rule-files:
     - custom.rules
   ```

3. Reload Suricata:

   ```
   sudo systemctl restart suricata
   ```

4. Test by sending ICMP traffic (e.g., `ping`):

   ```
   ping -c 3 192.168.1.1
   ```

   Check `eve.json` for alerts related to ICMP traffic.

---

5. Observations

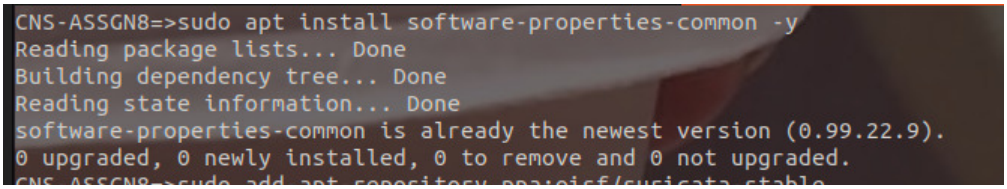
- **Strengths**:
  - Efficient detection of malicious activities in real-time.
  - Flexible and extensible rule management.
  - Comprehensive logging for analysis.
- **Challenges**:

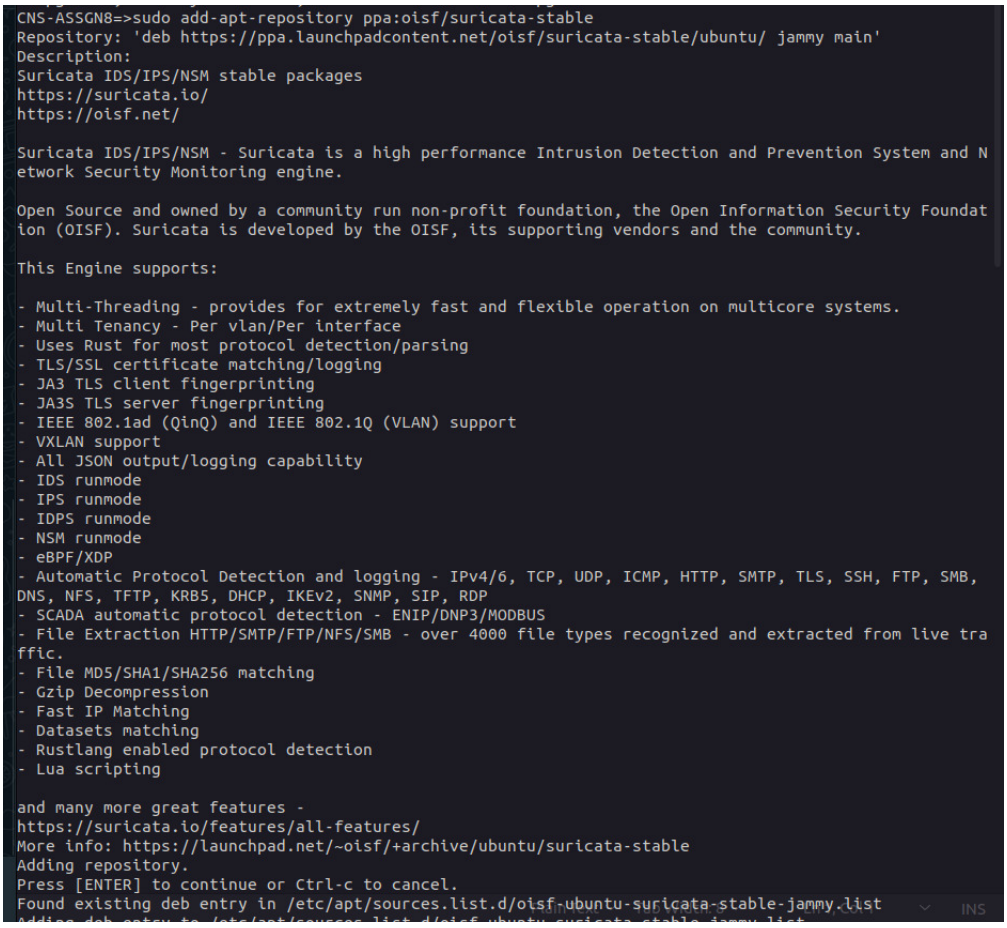
- Configuring rules for specific use cases requires a learning curve.
- High traffic can generate large logs, requiring proper log management.

---

6. Conclusion

Suricata is a powerful IDS that provides robust network monitoring and threat detection capabilities. During this study, it successfully detected simulated malicious traffic and custom rule-based alerts, demonstrating its flexibility and reliability. With proper configuration, it serves as an essential tool for securing network environments.





```
CNS-ASSGN8=>sudo apt install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:7.0.7-0ubuntu5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
CNS-ASSGN8=>
```

Plain Text

```
CNS-ASSGN8=>sudo apt install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:7.0.7-0ubuntu5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
CNS-ASSGN8=>suricata --build-info
This is Suricata version 7.0.7 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_H
OOK PCRE_JIT HAVE_NSS HTTP2_DECOMPRESSION HAVE_LUA HAVE_JA3 HAVE_JA4 HAVE_LUAJIT HAVE_LIBJANSSON TLS
TLS_C11 MAGIC RUST POPCNT64
SIMD support: SSE_2
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 11.4.0, C version 201112
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: _Thread_local
compiled with LibHTP v0.5.49, linked against LibHTP v0.5.49

Suricata Configuration:
  AF_PACKET support:                       yes
  AF_XDP support:                          no
  DPDK support:                            no
  eBPF support:                            no
  XDP support:                             no
  PF_RING support:                         no
  NFQueue support:                         yes
  NFLOG support:                           no
  IPFW support:                            no
  Netmap support:                          no
  DAG enabled:                             no
  Napatech enabled:                        no
  WinDivert enabled:                       no

  Unix socket enabled:                     yes
  Detection enabled:                       yes

  Libmagic support:                        yes
  libjansson support:                      yes
  hiredis support:                         yes
  hiredis async with libevent:             yes
  PCRE jit:                                yes
  LUA support:                             yes, through luajit
  libluajit:                               yes
  GeoIP2 support:                          yes
  JA3 support:                             yes
  JA4 support:                             yes
  Non-bundled htp:                         yes
  Hyperscan support:                       yes
  Libnet support:                          yes
  liblz4 support:                          yes
  Landlock support:                        yes
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
CNS-ASSGN8=>sudo apt install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:7.0.7-0ubuntu5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
CNS-ASSGN8=>suricata --build-info
This is Suricata version 7.0.7 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_H
OOK PCRE_JIT HAVE_NSS HTTP2_DECOMPRESSION HAVE_LUA HAVE_JA3 HAVE_JA4 HAVE_LUAJIT HAVE_LIBJANSSON TLS
TLS_C11 MAGIC RUST POPCNT64
SIMD support: SSE_2
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 11.4.0, C version 201112
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: _Thread_local
compiled with LibHTP v0.5.49, linked against LibHTP v0.5.49

Suricata Configuration:
  AF_PACKET support:                       yes
  AF_XDP support:                          no
  DPDK support:                            no
  eBPF support:                            no
  XDP support:                             no
  PF_RING support:                         no
  NFQueue support:                         yes
  NFLOG support:                           no
  IPFW support:                            no
  Netmap support:                          no
  DAG enabled:                             no
  Napatech enabled:                        no
  WinDivert enabled:                       no

  Unix socket enabled:                     yes
  Detection enabled:                       yes

  Libmagic support:                        yes
  libjansson support:                      yes
  hiredis support:                         yes
  hiredis async with libevent:             yes
  PCRE jit:                                yes
  LUA support:                             yes, through luajit
  libluajit:                               yes
  GeoIP2 support:                          yes
  JA3 support:                             yes
  JA4 support:                             yes
  Non-bundled htp:                         yes
  Hyperscan support:                       yes
  Libnet support:                          yes
  liblz4 support:                          yes
  Landlock support:                        yes
```



```
CNS-ASSGN8=>sudo apt install suricata-update -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata-update is already the newest version (1.2.3-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
CNS-ASSGN8=>
```

```
CNS-ASSGN8=>sudo suricata-update
2/12/2024 -- 12:35:19 - <Info> -- Using data-directory /var/lib/suricata.
2/12/2024 -- 12:35:19 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
2/12/2024 -- 12:35:19 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
2/12/2024 -- 12:35:19 - <Info> -- Found Suricata version 7.0.7 at /usr/bin/suricata.
2/12/2024 -- 12:35:19 - <Info> -- Loading /etc/suricata/suricata.yaml
2/12/2024 -- 12:35:19 - <Info> -- Disabling rules for protocol pgsql
2/12/2024 -- 12:35:19 - <Info> -- Disabling rules for protocol modbus
2/12/2024 -- 12:35:19 - <Info> -- Disabling rules for protocol dnp3
2/12/2024 -- 12:35:19 - <Info> -- Disabling rules for protocol enip
2/12/2024 -- 12:35:19 - <Info> -- No sources configured, will use Emerging Threats Open
2/12/2024 -- 12:35:19 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.7/emer
ging.rules.tar.gz.
 100% - 4610576/4610576
2/12/2024 -- 12:35:29 - <Info> -- Done.
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-
events.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-ev
ents.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dhcp-event
s.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dnp3-event
s.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/dns-events
.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/files.rule
s
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http2-even
ts.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/http-event
s.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ipsec-even
ts.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/kerberos-e
vents.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/modbus-eve
nts.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/mqtt-event
s.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/nfs-events
.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/ntp-events
.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/quic-event
s.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/rfb-events
.rules
2/12/2024 -- 12:35:29 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/smb-events
.rules
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
CNS-ASSGN8=>sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 12
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: 1 rule files processed. 40825 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 40828 signatures processed. 1203 are IP-only rules, 4263 are inspecting packet payload,
 35152 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
CNS-ASSGN8=>
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS


```
CNS-ASSGN8=>sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 12
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: 1 rule files processed. 40825 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 40828 signatures processed. 1203 are IP-only rules, 4263 are inspecting packet payload,
 35152 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
CNS-ASSGN8=>
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
CNS-ASSGN8=>ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f8:54:f6:06:13:8a brd ff:ff:ff:ff:ff:ff
    inet 192.168.220.229/24 brd 192.168.220.255 scope global dynamic noprefixroute wlp1s0
       valid_lft 3257sec preferred_lft 3257sec
    inet6 2402:3a80:42b1:d9d9:3f38:1dd5:43f6:8f4b/64 scope global temporary dynamic
       valid_lft 7156sec preferred_lft 7156sec
    inet6 2402:3a80:42b1:d9d9:1445:9ff9:ac24:a95/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 7156sec preferred_lft 7156sec
    inet6 fe80::405d:7ce2:b23:c63f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1
000
    link/ether 52:54:00:14:22:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
CNS-ASSGN8=>nano /etc/suricata/suricata.yaml
CNS-ASSGN8=>sudo suricata -i wlp1s0 -c /etc/suricata/suricata.yaml --af-packet
Info: suricata: Multiple af-packet option without interface on each is useless
i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 12 FM: 1 FR: 1   Engine started.
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

```
CNS-ASSN8=>sudo tail /var/log/suricata/suricata.log
[53191 - Suricata-Main] 2024-12-02 12:50:08 Perf: detect: Pkt MPM "ipv6.hdr": 1
[53191 - Suricata-Main] 2024-12-02 12:50:16 Config: af-packet: wlp1s0: using flow cluster mode for AF
_PACKET
[53191 - Suricata-Main] 2024-12-02 12:50:16 Config: af-packet: wlp1s0: using defrag kernel functional
ity for AF_PACKET
[53191 - Suricata-Main] 2024-12-02 12:50:16 Error: af-packet: fanout not supported by kernel: Kernel
too old or cluster-id 99 already in use.
[53191 - Suricata-Main] 2024-12-02 12:50:16 Info: runmodes: wlp1s0: creating 1 thread
[53191 - Suricata-Main] 2024-12-02 12:50:16 Config: flow-manager: using 1 flow manager threads
[53191 - Suricata-Main] 2024-12-02 12:50:16 Config: flow-manager: using 1 flow recycler threads
[53191 - Suricata-Main] 2024-12-02 12:50:16 Info: unix-manager: unix socket '/var/run/suricata/surica
ta-command.socket'
[53193 - W#01-wlp1s0] 2024-12-02 12:50:16 Perf: af-packet: wlp1s0: rx ring: block_size=32768 block_nr
=103 frame_size=1600 frame_nr=2060
[53191 - Suricata-Main] 2024-12-02 12:50:16 Notice: threads: Threads created -> W: 1 FM: 1 FR: 1   En
gine started.
```

```
CNS-ASSN8=>sudo tail -f /var/log/suricata/stats.log
flow.mgr.flows_timeout                    | Total                     | 13
flow.mgr.flows_evicted                    | Total                     | 13
memcap_pressure                           | Total                     | 10
memcap_pressure_max                       | Total                     | 10
flow.recycler.recycled                    | Total                     | 13
flow.recycler.queue_max                   | Total                     | 1
tcp.memuse                                | Total                     | 7274496
tcp.reassembly_memuse                     | Total                     | 1595392
http.memuse                               | Total                     | 224
flow.memuse                               | Total                     | 7479904
-------------------------------------------------------------------------------------
Date: 12/2/2024 -- 12:52:00 (uptime: 0d, 00h 01m 56s)
-------------------------------------------------------------------------------------
Counter                                   | TM Name                   | Value
-------------------------------------------------------------------------------------
capture.kernel_packets                    | Total                     | 515
capture.afpacket.polls                    | Total                     | 1188
capture.afpacket.poll_timeout             | Total                     | 961
capture.afpacket.poll_data                | Total                     | 227
decoder.pkts                              | Total                     | 515
decoder.bytes                             | Total                     | 270082
decoder.ipv4                              | Total                     | 150
decoder.ipv6                              | Total                     | 361
decoder.ethernet                          | Total                     | 515
decoder.arp                               | Total                     | 4
decoder.tcp                               | Total                     | 464
tcp.syn                                   | Total                     | 5
tcp.synack                                | Total                     | 5
tcp.rst                                   | Total                     | 5
decoder.udp                               | Total                     | 37
decoder.icmpv6                            | Total                     | 10
decoder.avg_pkt_size                      | Total                     | 524
decoder.max_pkt_size                      | Total                     | 1414
tcp.active_sessions                       | Total                     | 5
flow.total                                | Total                     | 22
flow.active                               | Total                     | 22
flow.tcp                                  | Total                     | 8
flow.udp                                  | Total                     | 10
flow.icmpv6                               | Total                     | 4
flow.wrk.spare_sync_avg                   | Total                     | 100
flow.wrk.spare_sync                       | Total                     | 1
tcp.sessions                              | Total                     | 5
tcp.ssn_from_pool                         | Total                     | 5
tcp.segment_from_cache                    | Total                     | 1
tcp.segment_from_pool                     | Total                     | 186
```