DEN

DIGITAL EMPOWERMENT NETWORK

FINAL TASK REPORT

Name	**Syed Sheeraz Ali Shah**
Department	**Cybersecurity**
Instructor	**Mrs. Noor us Sama**
Task	**4**

Dated: 3/10/2024

Configuring Firewalls and Intrusion Detection Systems

Objective:
The primary goal of this project was to protect the network by implementing firewalls and an Intrusion Detection System (IDS). The focus was on selecting and configuring appropriate solutions to monitor and control network traffic, detect unauthorized access, and respond to potential threats effectively.

Description of Implementation:
I chose Suricata as the IDS solution to implement on my virtual machine running Kali Linux. Suricata is a well-regarded open-source IDS/IPS (Intrusion Prevention System) that offers powerful real-time intrusion detection and analysis capabilities. Below are the steps I followed during the implementation process:

1. Selecting Appropriate Firewall and IDS Solutions

After reviewing various options, I selected Suricata for its robust detection capabilities, ease of configuration, and strong community support. Suricata offers deep packet inspection, network security monitoring, and signature-based threat detection, making it ideal for this task.

2. Configuring Firewall Rules and Policies

While setting up the firewall, I ensured that the system was protected by implementing restrictive rules. This included:

- Blocking all incoming traffic by default.
- Allowing only specific ports necessary for legitimate traffic.
- Creating logging rules to track dropped and accepted packets.

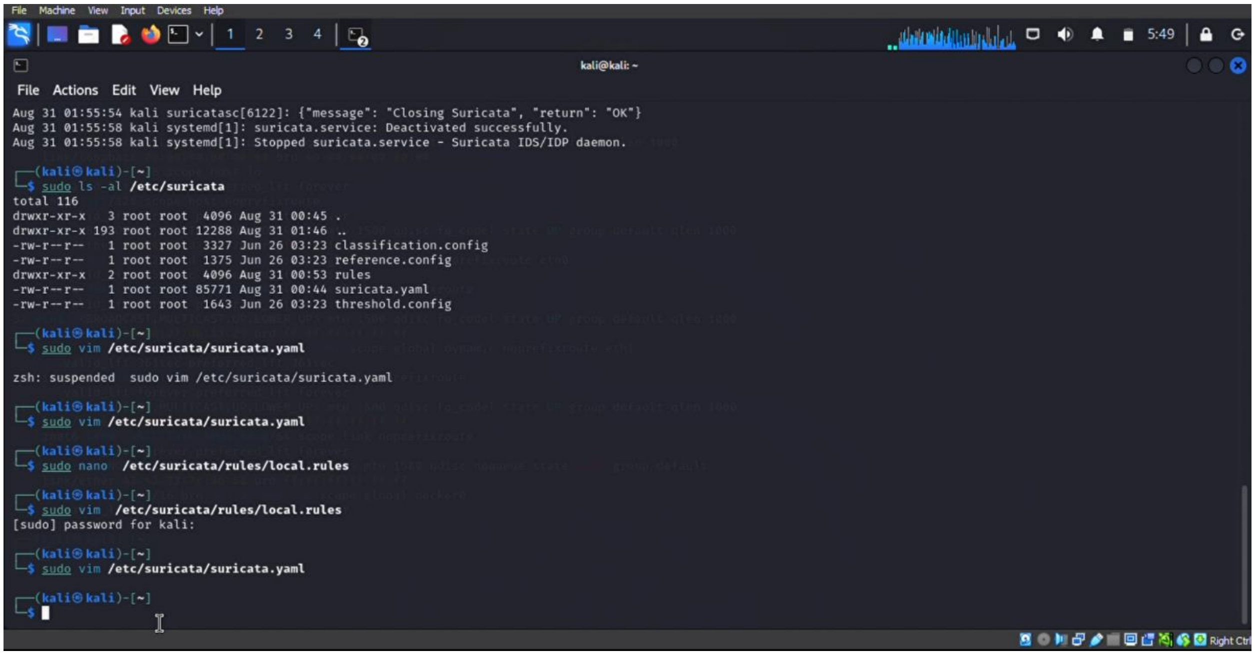
These rules were tested and fine-tuned to ensure no disruption to legitimate network traffic while preventing unauthorized access.

3. Setting Up Suricata IDS

To install and configure Suricata on Kali Linux, I performed the following steps:

- **Installation:** I installed Suricata using the official Kali Linux repositories. sudo apt-get install suricata

- **Configuration:** I configured Suricata to monitor network interfaces and capture network traffic in real time. I also set up Suricata to use its default rule set to identify common attack patterns.
    - Modified the **suricata.yaml** configuration file to enable the correct network interface monitoring.


File Machine View Input Devices Help
1 2 3 4
5:49
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
Aug 31 01:55:54 kali suricatasc[6122]: {"message": "Closing Suricata", "return": "OK"}
Aug 31 01:55:58 kali systemd[1]: suricata.service: Deactivated successfully.
Aug 31 01:55:58 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.

┌──(kali㉿kali)-[~]
└─$ sudo ls -al /etc/suricata
total 116
drwxr-xr-x   3 root root  4096 Aug 31 00:45 .
drwxr-xr-x 193 root root 12288 Aug 31 01:46 ..
-rw-r--r--   1 root root  3327 Jun 26 03:23 classification.config
-rw-r--r--   1 root root  1375 Jun 26 03:23 reference.config
drwxr-xr-x   2 root root  4096 Aug 31 00:53 rules
-rw-r--r--   1 root root 85771 Aug 31 00:44 suricata.yaml
-rw-r--r--   1 root root  1643 Jun 26 03:23 threshold.config

┌──(kali㉿kali)-[~]
└─$ sudo vim /etc/suricata/suricata.yaml

zsh: suspended  sudo vim /etc/suricata/suricata.yaml

┌──(kali㉿kali)-[~]
└─$ sudo vim /etc/suricata/suricata.yaml

┌──(kali㉿kali)-[~]
└─$ sudo nano  /etc/suricata/rules/local.rules

┌──(kali㉿kali)-[~]
└─$ sudo vim  /etc/suricata/rules/local.rules
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo vim /etc/suricata/suricata.yaml

┌──(kali㉿kali)-[~]
└─$ 
```

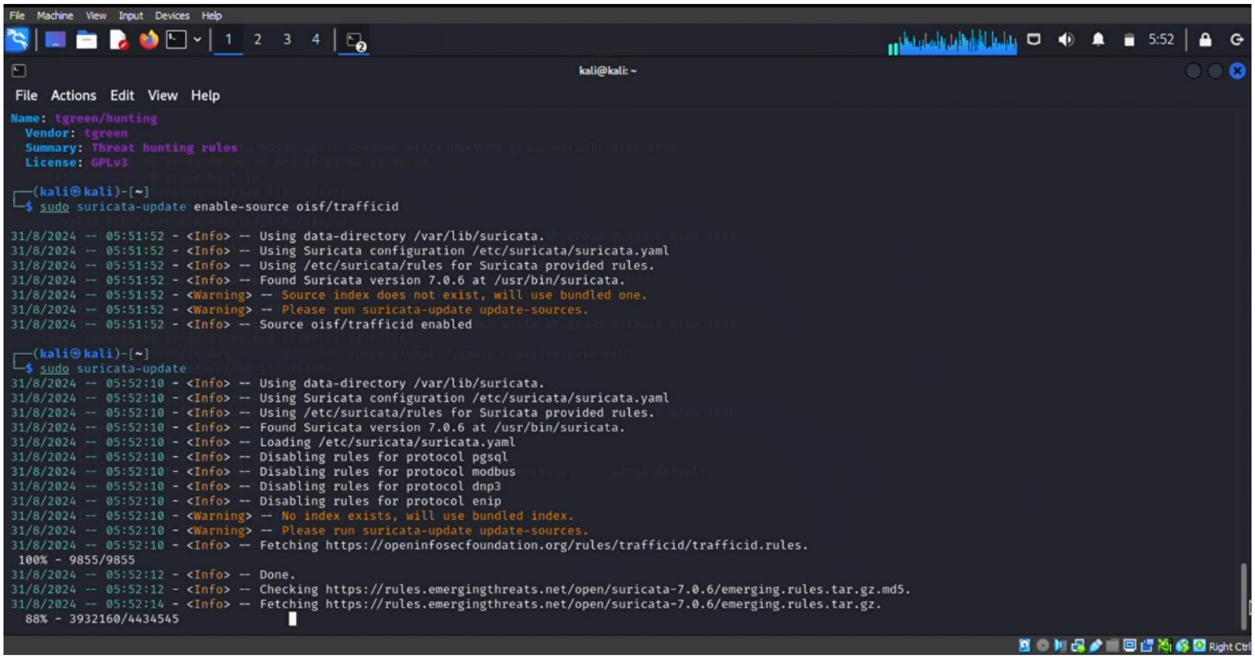
-
    - Integrated additional rules from the Emerging Threats Open rule set for improved detection.

- **Testing:** After the initial setup, I performed various penetration tests using Kali's built-in tools (such as Nmap) to validate Suricata's detection capabilities. The system successfully detected suspicious activities and flagged them accordingly.

4. Analyzing IDS Alerts and Responding to Threats

Once Suricata was operational, I monitored the alert logs generated by the system. Alerts were analyzed using Suricata's logs, stored in /var/log/suricata/. These alerts helped me identify potential threats and anomalies in the network traffic.

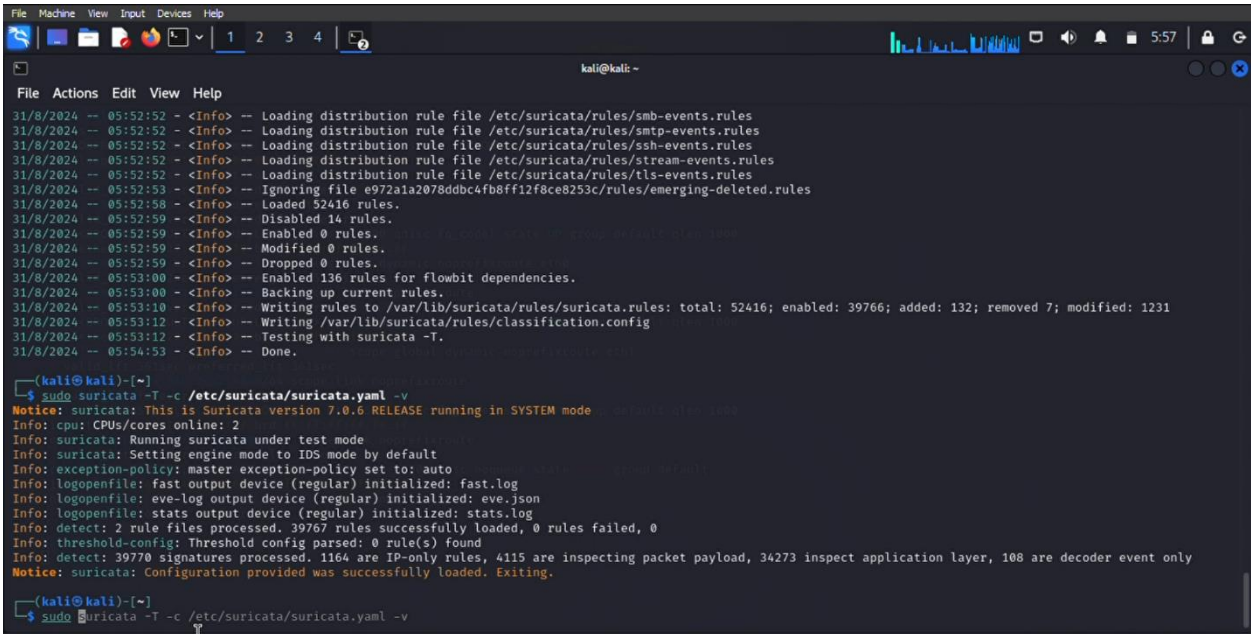
- Suricata provided detailed logs for each incident, including the time, source IP, destination IP, and type of attack detected.


File Machine View Input Devices Help
1 2 3 4
5:52
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
Name: tgreen/hunting
  Vendor: tgreen
  Summary: Threat hunting rules
  License: GPLv3

┌──(kali㉿kali)-[~]
└─$ sudo suricata-update enable-source oisf/trafficid

31/8/2024 -- 05:51:52 - <Info> -- Using data-directory /var/lib/suricata.
31/8/2024 -- 05:51:52 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
31/8/2024 -- 05:51:52 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
31/8/2024 -- 05:51:52 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
31/8/2024 -- 05:51:52 - <Warning> -- Source index does not exist, will use bundled one.
31/8/2024 -- 05:51:52 - <Warning> -- Please run suricata-update update-sources.
31/8/2024 -- 05:51:52 - <Info> -- Source oisf/trafficid enabled

┌──(kali㉿kali)-[~]
└─$ sudo suricata-update
31/8/2024 -- 05:52:10 - <Info> -- Using data-directory /var/lib/suricata.
31/8/2024 -- 05:52:10 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
31/8/2024 -- 05:52:10 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
31/8/2024 -- 05:52:10 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
31/8/2024 -- 05:52:10 - <Info> -- Loading /etc/suricata/suricata.yaml
31/8/2024 -- 05:52:10 - <Info> -- Disabling rules for protocol pgsql
31/8/2024 -- 05:52:10 - <Info> -- Disabling rules for protocol modbus
31/8/2024 -- 05:52:10 - <Info> -- Disabling rules for protocol dnp3
31/8/2024 -- 05:52:10 - <Info> -- Disabling rules for protocol enip
31/8/2024 -- 05:52:10 - <Warning> -- No index exists, will use bundled index.
31/8/2024 -- 05:52:10 - <Warning> -- Please run suricata-update update-sources.
31/8/2024 -- 05:52:10 - <Info> -- Fetching https://openinfosecfoundation.org/rules/trafficid/trafficid.rules.
 100% - 9855/9855
31/8/2024 -- 05:52:12 - <Info> -- Done.
31/8/2024 -- 05:52:12 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-7.0.6/emerging.rules.tar.gz.md5.
31/8/2024 -- 05:52:14 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.6/emerging.rules.tar.gz.
  88% - 3932160/4434545
```

- I performed a manual analysis of these logs to ensure proper understanding of the threat landscape.

- Based on the alerts, I updated the firewall rules and IDS policies to respond to any detected threats.



File Machine View Input Devices Help
1 2 3 4
5:57
kali@kali: ~
File Actions Edit View Help

```
31/8/2024 -- 05:52:52 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
31/8/2024 -- 05:52:52 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
31/8/2024 -- 05:52:52 - <Info> -- Loading distribution rule file /etc/suricata/rules/ssh-events.rules
31/8/2024 -- 05:52:52 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
31/8/2024 -- 05:52:52 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
31/8/2024 -- 05:52:53 - <Info> -- Ignoring file e972a1a2078ddbc4fb8ff12f8ce8253c/rules/emerging-deleted.rules
31/8/2024 -- 05:52:58 - <Info> -- Loaded 52416 rules.
31/8/2024 -- 05:52:59 - <Info> -- Disabled 14 rules.
31/8/2024 -- 05:52:59 - <Info> -- Enabled 0 rules.
31/8/2024 -- 05:52:59 - <Info> -- Modified 0 rules.
31/8/2024 -- 05:52:59 - <Info> -- Dropped 0 rules.
31/8/2024 -- 05:53:00 - <Info> -- Enabled 136 rules for flowbit dependencies.
31/8/2024 -- 05:53:00 - <Info> -- Backing up current rules.
31/8/2024 -- 05:53:10 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 52416; enabled: 39766; added: 132; removed 7; modified: 1231
31/8/2024 -- 05:53:12 - <Info> -- Writing /var/lib/suricata/rules/classification.config
31/8/2024 -- 05:53:12 - <Info> -- Testing with suricata -T.
31/8/2024 -- 05:54:53 - <Info> -- Done.

┌──(kali㉿kali)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
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. 39767 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 39770 signatures processed. 1164 are IP-only rules, 4115 are inspecting packet payload, 34273 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.

┌──(kali㉿kali)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

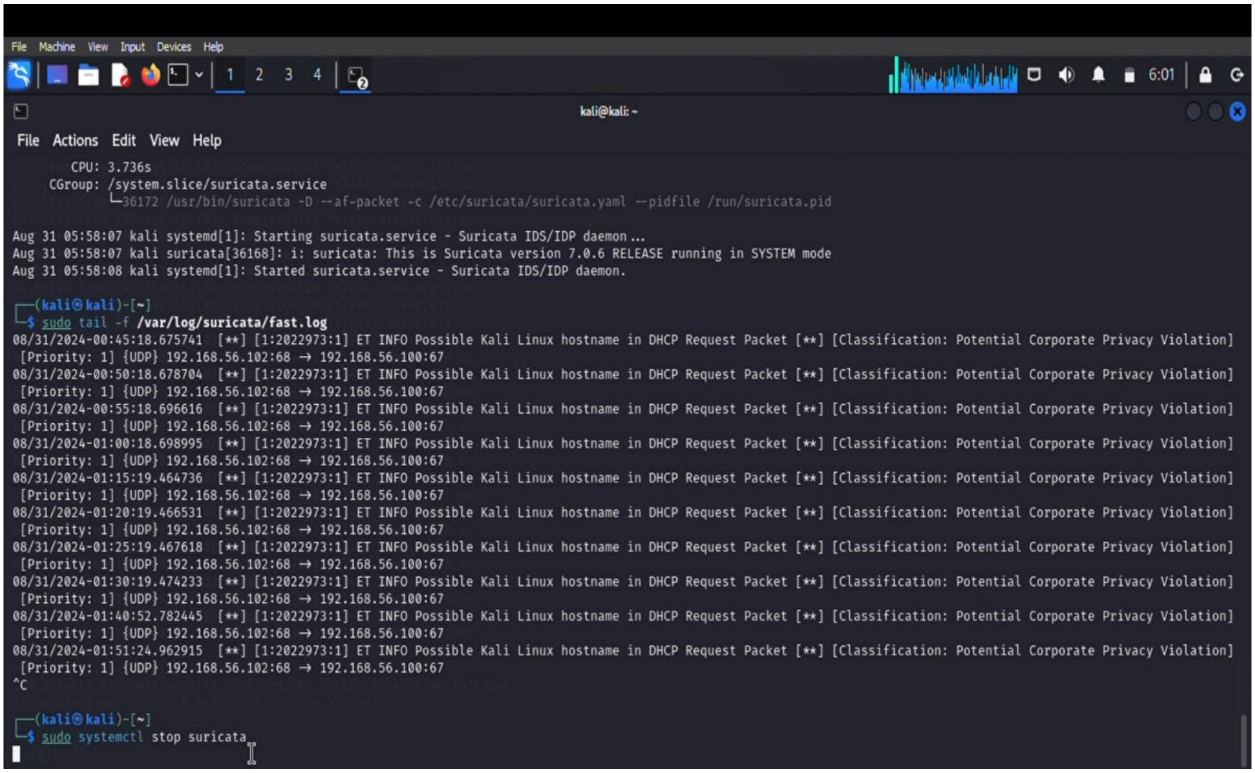
5. Regular Maintenance and Updates

I made it a point to regularly update the IDS rules and configurations to stay current with emerging threats. This involved:

- Periodically downloading new rule sets from Emerging Threats.
- Reviewing logs and making necessary adjustments to the firewall and IDS settings.
- Ensuring system patches and updates were applied to both the firewall and Suricata.

Outcome:

By implementing Suricata IDS on Kali Linux, I have established a robust layer of network security. Suricata efficiently monitors incoming and outgoing traffic, detects potential intrusions, and alerts me to threats in real time. With continuous monitoring, rule updates, and response protocols in place, the network is significantly more secure against unauthorized access and attacks.

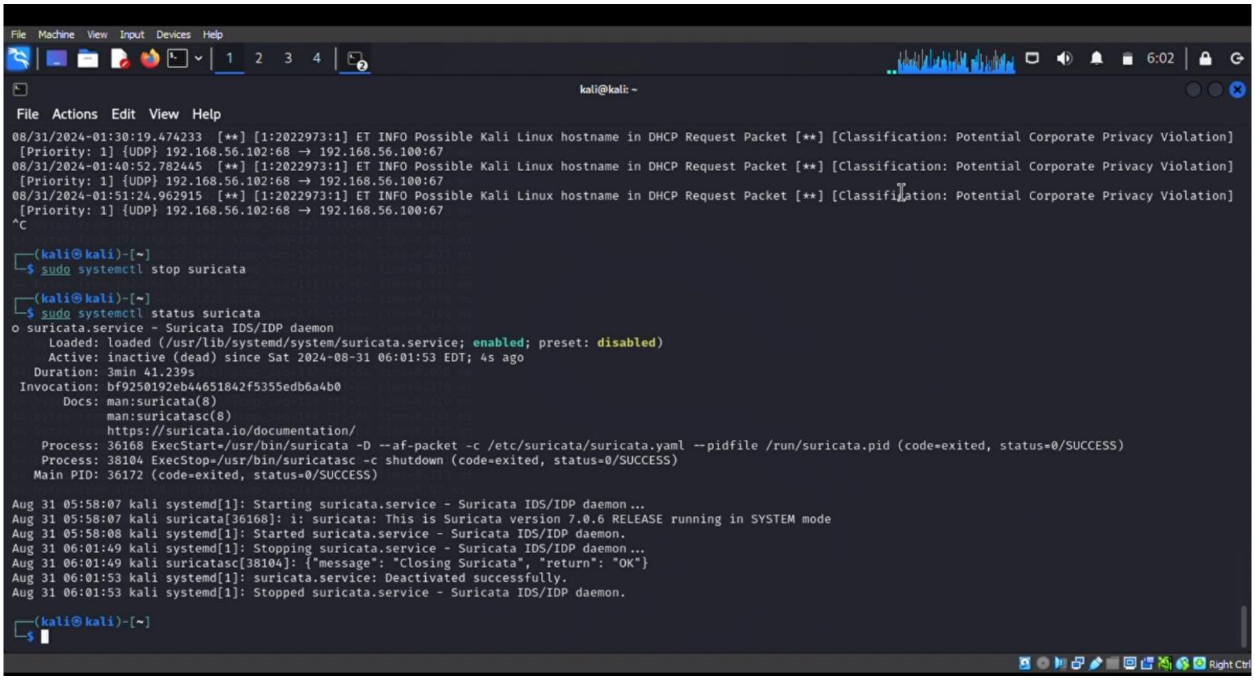

File Machine View Input Devices Help
1 2 3 4
6:01
kali@kali: ~
File Actions Edit View Help

```
       CPU: 3.736s
    CGroup: /system.slice/suricata.service
            └─36172 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Aug 31 05:58:07 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Aug 31 05:58:07 kali suricata[36168]: i: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Aug 31 05:58:08 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.

┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/suricata/fast.log
08/31/2024-00:45:18.675741  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-00:50:18.678704  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-00:55:18.696616  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:00:18.698995  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:15:19.464736  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:20:19.466531  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:25:19.467618  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:30:19.474233  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:40:52.782445  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:51:24.962915  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
^C

┌──(kali㉿kali)-[~]
└─$ sudo systemctl stop suricata
```

Conclusion:

In conclusion, implementing Suricata IDS on my Kali Linux virtual machine allowed me to significantly enhance network security by monitoring traffic, detecting potential intrusions, and responding to threats in real time. However, I observed that Suricata consumes considerable system resources while running, which can impact the performance of other applications on the virtual machine.

To address this, I decided to stop the Suricata service after ensuring the system was properly secured and all configurations were optimized. This approach allows me to conserve resources when IDS monitoring is not required, while still retaining the ability to quickly re-enable Suricata for active monitoring during periods of heightened network activity or security assessment. This balance ensures system performance without compromising security readiness.


File Machine View Input Devices Help
1 2 3 4
6:02
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
08/31/2024-01:30:19.474233  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:40:52.782445  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
08/31/2024-01:51:24.962915  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation]
 [Priority: 1] {UDP} 192.168.56.102:68 → 192.168.56.100:67
^C

┌──(kali㉿kali)-[~]
└─$ sudo systemctl stop suricata

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata
o suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: disabled)
     Active: inactive (dead) since Sat 2024-08-31 06:01:53 EDT; 4s ago
   Duration: 3min 41.239s
 Invocation: bf9250192eb44651842f5355edb6a4b0
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 36168 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid (code=exited, status=0/SUCCESS)
    Process: 38104 ExecStop=/usr/bin/suricatasc -c shutdown (code=exited, status=0/SUCCESS)
   Main PID: 36172 (code=exited, status=0/SUCCESS)

Aug 31 05:58:07 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Aug 31 05:58:07 kali suricata[36168]: i: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Aug 31 05:58:08 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
Aug 31 06:01:49 kali systemd[1]: Stopping suricata.service - Suricata IDS/IDP daemon...
Aug 31 06:01:49 kali suricatasc[38104]: {"message": "Closing Suricata", "return": "OK"}
Aug 31 06:01:53 kali systemd[1]: suricata.service: Deactivated successfully.
Aug 31 06:01:53 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daemon.

┌──(kali㉿kali)-[~]
└─$ 
```