DIGITAL EMPOWERMENT NETWORK

INTERNSHIP REPORT

WEEK#04

PRESENTED BY ALIZA JAVED
CID DEN10161

CONTENTS

ABOUT THE COMPANY

At Digital Empowerment Network, we are dedicated to empowering Pakistan's university students through a wide range of initiatives that foster leadership, academic growth, and technical expertise. By bridging the digital divide with workshops, coding camps, and hackathons, we equip students with essential skills to thrive in the modern workforce. Our commitment to education extends beyond the classroom, as we reinvest proceeds from our revenue-generating partnerships into impactful programs and charitable initiatives, providing resources and support to underserved communities. We believe in the power of education to create well-rounded individuals who can drive innovation and make a positive impact on society.

CONFIGURING FIREWALLS AND INTRUSION DETECTION SYSTEMS

1.Objective:

Protect the network by setting up firewalls and IDS.

2.Description:

Implement firewalls and intrusion detection systems to monitor and control incoming and outgoing network traffic. Detect and prevent unauthorised access and attacks.

3.Key Steps:

- Selecting appropriate firewall and IDS solutions.
- Configuring firewall rules and policies.
- Setting up IDS to monitor network traffic.
- Analysing IDS alerts and responding to threats.
- Regularly updating and maintaining the configurations

INTRODUCTION TO FIREWALLS AND INTRUSION DETECTION SYSTEMS

In today's digital landscape, where cyber threats are increasingly sophisticated and prevalent, organisations must prioritise robust security measures to protect their networks. Two critical components of a comprehensive security strategy are Firewalls and Intrusion Detection Systems (IDS). These technologies work in tandem to create a secure environment for both data and users, ensuring that sensitive information remains protected against unauthorised access and cyber attacks.

Firewalls serve as the first line of defence in network security. They are designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. By acting as a barrier between a trusted internal network and untrusted external networks, firewalls filter out potentially harmful traffic. This filtering process can be based on various criteria, including IP addresses, protocols, and ports, effectively preventing unauthorised users from accessing the network. Firewalls can be implemented in hardware, software, or a combination of both, providing flexibility in deployment according to organisational needs. Their ability to enforce policies and control traffic helps mitigate risks associated with data breaches, malware infections, and other cyber threats.

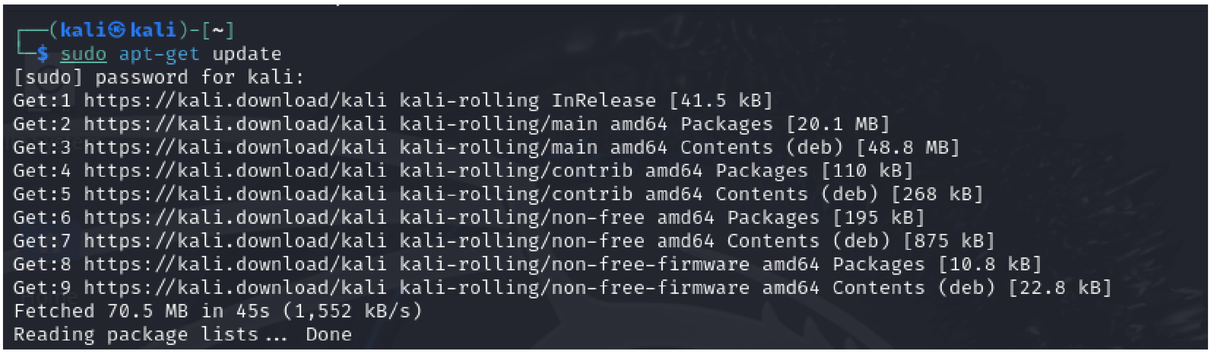
Intrusion Detection Systems (IDS) are crucial for monitoring network traffic and identifying suspicious activities that may indicate a security breach. IDS can analyse various data packets traversing the network and use signature-based detection to identify known threats or anomaly-based detection to flag unusual behaviour that deviates from established norms. Upon detecting a potential intrusion, an IDS generates alerts for system administrators, enabling them to respond swiftly to potential threats. While firewalls focus on preventing unauthorised access, IDS complements this by providing visibility into ongoing network activities, helping organisations detect and respond to incidents in real-time.

The necessity of implementing both firewalls and IDS cannot be overstated. Firewalls provide a proactive defence by controlling traffic at the perimeter, significantly reducing the attack surface. However, they are not infallible; sophisticated attackers can sometimes bypass firewalls through various techniques, such as social engineering or exploiting application vulnerabilities. This is where IDS becomes invaluable. By continuously monitoring network traffic and system behaviour, IDS can detect breaches that may have slipped past the firewall, offering an additional layer of protection.

Moreover, the integration of firewalls and IDS enhances an organisation's overall security posture. By working together, these technologies create a defence-in-depth strategy, which is essential in modern cybersecurity frameworks. Organisations can not only prevent unauthorised access but also have the capability to detect and respond to security incidents promptly. This is particularly important in today's regulatory environment, where organisations are required to comply with various data protection laws, such as GDPR and HIPAA, that mandate stringent security measures.

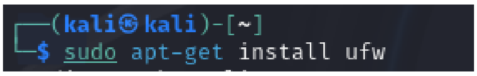
CONFIGURING FIREWALL RULES AND POLICIES

- Update the system to ensure that all packages and dependencies are current, enhancing security, stability, and compatibility with new software.



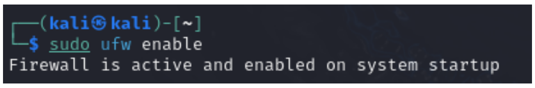
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Get:1 https://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 https://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:3 https://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Get:4 https://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
Get:5 https://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [268 kB]
Get:6 https://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 https://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [875 kB]
Get:8 https://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:9 https://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [22.8 kB]
Fetched 70.5 MB in 45s (1,552 kB/s)
Reading package lists ... Done
```

- Install ufw.



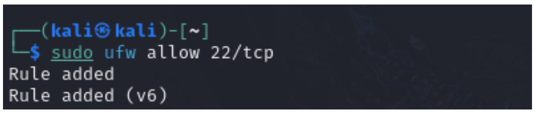
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install ufw
```

- Now Enable ufw.



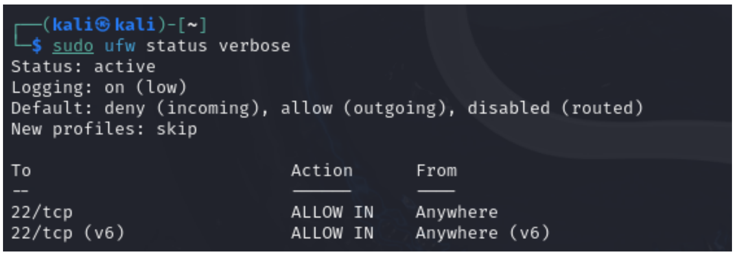
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup
```

- Setup basic rules.



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
```

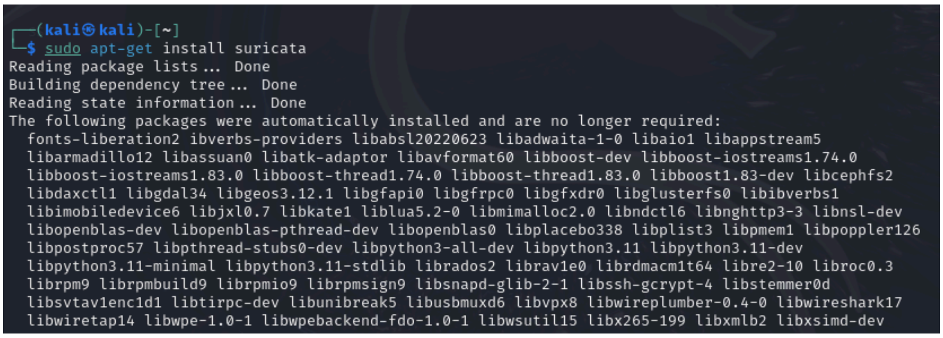
- Check the existing rules in the firewall.



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

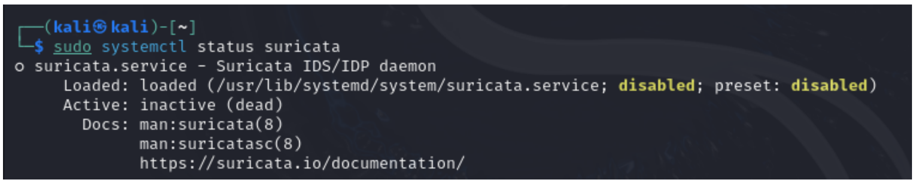
SETTING UP INTRUSION DETECTION SYSTEM TO MONITOR NETWORK TRAFFIC

- Install suricata.



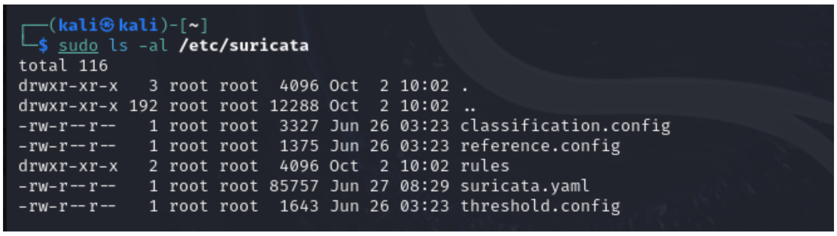
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 ibverbs-providers libabsl20220623 libadwaita-1-0 libaio1 libappstream5
  libarmadillo12 libassuan0 libatk-adaptor libavformat60 libboost-dev libboost-iostreams1.74.0
  libboost-iostreams1.83.0 libboost-thread1.74.0 libboost-thread1.83.0 libboost1.83-dev libcephfs2
  libdaxctl1 libgdal34 libgeos3.12.1 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libibverbs1
  libimobiledevice6 libjxl0.7 libkate1 liblua5.2-0 libmimalloc2.0 libndctl6 libnghttp3-3 libnsl-dev
  libopenblas-dev libopenblas-pthread-dev libopenblas0 libplacebo338 libplist3 libpmem1 libpoppler126
  libpostproc57 libpthread-stubs0-dev libpython3-all-dev libpython3.11 libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib librados2 librav1e0 librdmacm1t64 libre2-10 libroc0.3
  librpm9 librpmbuild9 librpmio9 librpmsign9 libsnapd-glib-2-1 libssh-gcrypt-4 libstemmer0d
  libsvtav1enc1d1 libtirpc-dev libunibreak5 libusbmuxd6 libvpx8 libwireplumber-0.4-0 libwireshark17
  libwiretap14 libwpe-1.0-1 libwpebackend-fdo-1.0-1 libwsutil15 libx265-199 libxmlb2 libxsimd-dev
```

- Check the status of suricata and make sure it is inactive.



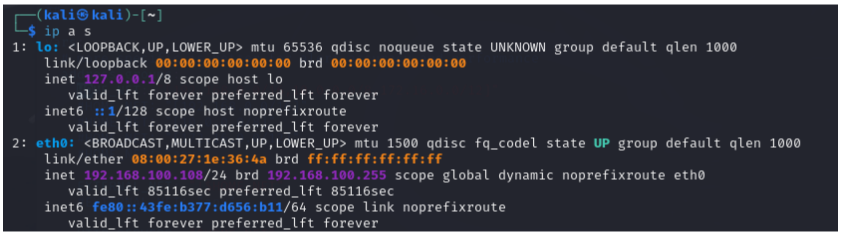
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata
○ suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
```

- List down the IDS configuration to check the files.



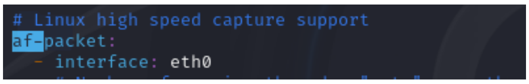
```
┌──(kali㉿kali)-[~]
└─$ sudo ls -al /etc/suricata
total 116
drwxr-xr-x   3 root root  4096 Oct  2 10:02 .
drwxr-xr-x 192 root root 12288 Oct  2 10:02 ..
-rw-r--r--   1 root root  3327 Jun 26 03:23 classification.config
-rw-r--r--   1 root root  1375 Jun 26 03:23 reference.config
drwxr-xr-x   2 root root  4096 Oct  2 10:02 rules
-rw-r--r--   1 root root 85757 Jun 27 08:29 suricata.yaml
-rw-r--r--   1 root root  1643 Jun 26 03:23 threshold.config
```

- Open the suricata.yaml file to set up the IDS configuration. Search HOMENET and change its ip to the systems ip as we are using the same system to ping the ip. To check the system ip, open another terminal and write ip a s to check the ip.



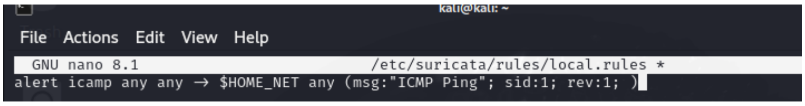
```
┌──(kali㉿kali)-[~]
└─$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1e:36:4a brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.108/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
       valid_lft 85116sec preferred_lft 85116sec
    inet6 fe80::43fe:b377:d656:b11/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Now search af-packet and make sure it has the same ethernet connection as of the ip address your are using.



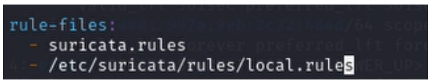
```
# Linux high speed capture support
af-packet:
  - interface: eth0
```

- Setup custom rules in the rules file.



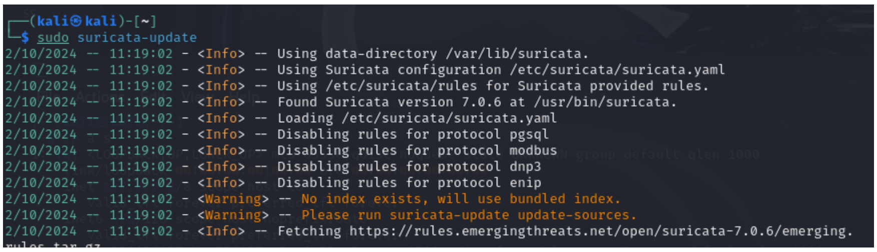
```
  GNU nano 8.1                          /etc/suricata/rules/local.rules *
alert icamp any any → $HOME_NET any (msg:"ICMP Ping"; sid:1; rev:1; )
```

- Add rules file path in the suricata.yaml file.



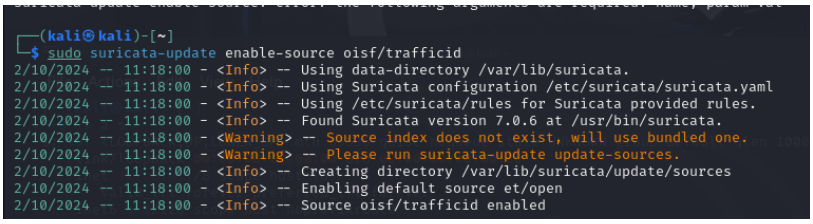
```
rule-files:
  - suricata.rules
  - /etc/suricata/rules/local.rules
```

- After setting up the configuration and rules, update suricata.

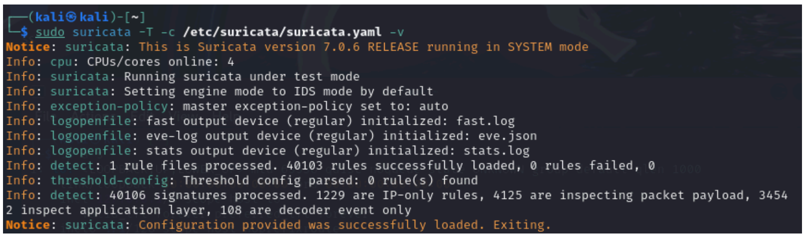


```
┌──(kali㉿kali)-[~]
└─$ sudo suricata-update
2/10/2024 -- 11:19:02 - <Info> -- Using data-directory /var/lib/suricata.
2/10/2024 -- 11:19:02 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
2/10/2024 -- 11:19:02 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
2/10/2024 -- 11:19:02 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
2/10/2024 -- 11:19:02 - <Info> -- Loading /etc/suricata/suricata.yaml
2/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol pgsql
2/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol modbus
2/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol dnp3
2/10/2024 -- 11:19:02 - <Info> -- Disabling rules for protocol enip
2/10/2024 -- 11:19:02 - <Warning> -- No index exists, will use bundled index.
2/10/2024 -- 11:19:02 - <Warning> -- Please run suricata-update update-sources.
2/10/2024 -- 11:19:02 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.6/emerging.
rules.tar.gz
```

- Now download suricata from the list sources and configure.

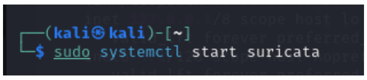


```
suricata-update enable-source: error: the following arguments are required: name, param-val

┌──(kali㉿kali)-[~]
└─$ sudo suricata-update enable-source oisf/trafficid
2/10/2024 -- 11:18:00 - <Info> -- Using data-directory /var/lib/suricata.
2/10/2024 -- 11:18:00 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
2/10/2024 -- 11:18:00 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
2/10/2024 -- 11:18:00 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
2/10/2024 -- 11:18:00 - <Warning> -- Source index does not exist, will use bundled one.
2/10/2024 -- 11:18:00 - <Warning> -- Please run suricata-update update-sources.
2/10/2024 -- 11:18:00 - <Info> -- Creating directory /var/lib/suricata/update/sources
2/10/2024 -- 11:18:00 - <Info> -- Enabling default source et/open
2/10/2024 -- 11:18:00 - <Info> -- Source oisf/trafficid enabled
```



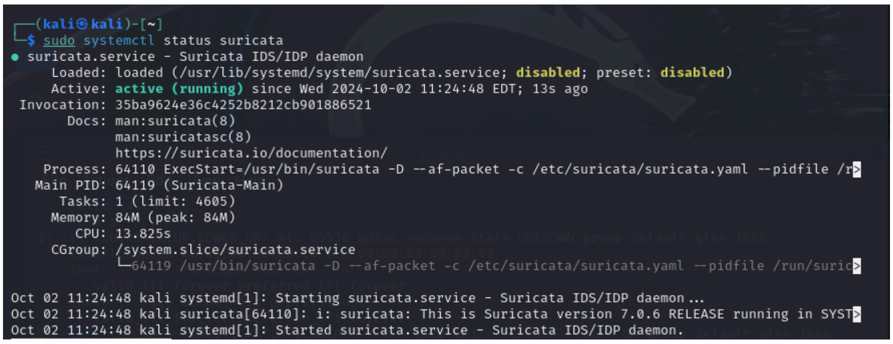
```
┌──(kali㉿kali)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: 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. 40103 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 40106 signatures processed. 1229 are IP-only rules, 4125 are inspecting packet payload, 3454
2 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

- Start suricata.



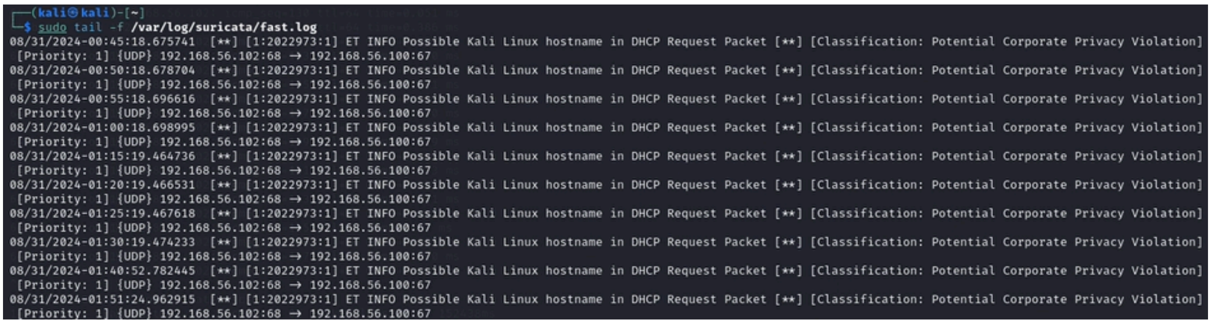
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start suricata
```

- Now check the status of suricata.



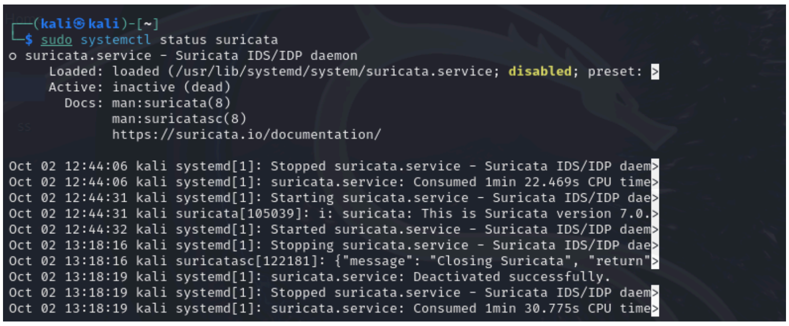
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
     Active: active (running) since Wed 2024-10-02 11:24:48 EDT; 13s ago
 Invocation: 35ba9624e36c4252b8212cb901886521
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 64110 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /r>
   Main PID: 64119 (Suricata-Main)
      Tasks: 1 (limit: 4605)
     Memory: 84M (peak: 84M)
        CPU: 13.825s
     CGroup: /system.slice/suricata.service
             └─64119 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suric>

Oct 02 11:24:48 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Oct 02 11:24:48 kali suricata[64110]: i: suricata: This is Suricata version 7.0.6 RELEASE running in SYST>
Oct 02 11:24:48 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
```

- Now ping your ip and check the logs in suricata.



```
┌──(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
```

- Monitor the logs and disable the suricata after monitoring.



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata
○ suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: >
     Active: inactive (dead)
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/

Oct 02 12:44:06 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daem>
Oct 02 12:44:06 kali systemd[1]: suricata.service: Consumed 1min 22.469s CPU time>
Oct 02 12:44:31 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP dae>
Oct 02 12:44:31 kali suricata[105039]: i: suricata: This is Suricata version 7.0.>
Oct 02 12:44:32 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daem>
Oct 02 13:18:16 kali systemd[1]: Stopping suricata.service - Suricata IDS/IDP dae>
Oct 02 13:18:16 kali suricatasc[122181]: {"message": "Closing Suricata", "return">
Oct 02 13:18:19 kali systemd[1]: suricata.service: Deactivated successfully.
Oct 02 13:18:19 kali systemd[1]: Stopped suricata.service - Suricata IDS/IDP daem>
Oct 02 13:18:19 kali systemd[1]: suricata.service: Consumed 1min 30.775s CPU time>
```

CONCLUSION

In conclusion, the configuration of firewalls and Intrusion Detection Systems (IDS) is crucial for bolstering the cybersecurity posture of organisations. Firewalls act as the first line of defence, meticulously controlling network traffic based on predefined security rules to prevent unauthorised access and mitigate threats. Meanwhile, IDS provides continuous monitoring, enabling the detection of suspicious behaviour and facilitating timely responses to potential breaches. This layered approach not only reduces the attack surface but also enhances the organisation’s ability to respond effectively to emerging threats. Throughout this internship, I have gained valuable hands-on experience in implementing and managing these essential security technologies, highlighting the importance of maintaining updated configurations and monitoring logs to ensure their ongoing effectiveness against evolving cyber threats.