PRATICAL NUMBER 3 THREAT HUNTING

QUESTION

: How can you proactively detect malware using threat hunting techniques?

ANSWER

Threat hunting simply means proactively searching for cyber threats that are lurking undetected in a network. To proactively detect malware using threat hunting techniques;

<1>--Stay updated with the latest tactics and techniques used by threat actors. Sources like OSINT (open-source intelligence) , threat intelligence feeds and cybersecurity blogs helps to keep updated with malware trends used by threat actors

<2>--Network traffic should be monitored for unusual patterns. Implement SIEM(security information and event management) and use EDR tools that helps to give insight about endpoints and collect network activity .

<3>--The use of SOAR (security orchestration, automation and response) will help detect and respond to detected threats

QUESTION 2

Task: Use OSQuery or Sysmon to monitor system behavior and network traffic. Look for signs of malware, such as unusual process execution or outbound traffic to suspicious IP addresses. Create custom queries to detect potential indicators of compromise (IOCs). □ Tools: OSQuery, Sysmon, Wireshark.

ANSWER

--I installed osquery on my virtual machine and i also installed wireshark.

-I started a query by using the command **sudo osqueryi**

```
┌──(root㉿kali)-[~]
└─# sudo osqueryi
W0824 19:06:00.825416 53884 options.cpp:106] The CLI only flag --logger_plugi
n set via config file will be ignored, please use a flagfile or pass it to th
e process at startup
Using a virtual database. Need help, type '.help'
osquery> SELECT * FROM osquery_info;
+-------+------------------------------------------+----------------------------
-----------+---------+------------------------------------------+-------------
+------------+----------------+--------------+------------+---------+--------
------+
| pid   | uuid                                     | instance_id
          | version | config_hash                                | config_valid
| extensions | build_platform | build_distro | start_time | watcher | platfor
m_mask |
+-------+------------------------------------------+----------------------------
-----------+---------+------------------------------------------+-------------
+------------+----------------+--------------+------------+---------+--------
```

-I created a file **sudo nano /etc/osquery/osquery.conf**

```
+-------+-----+-------+-------+-------+---------------
--+------------+-----------+-------------
-------------+--------------+
osquery> sudo nano /etc/osquery/osquery.conf
    ...> {
```

**then i added a query to the file

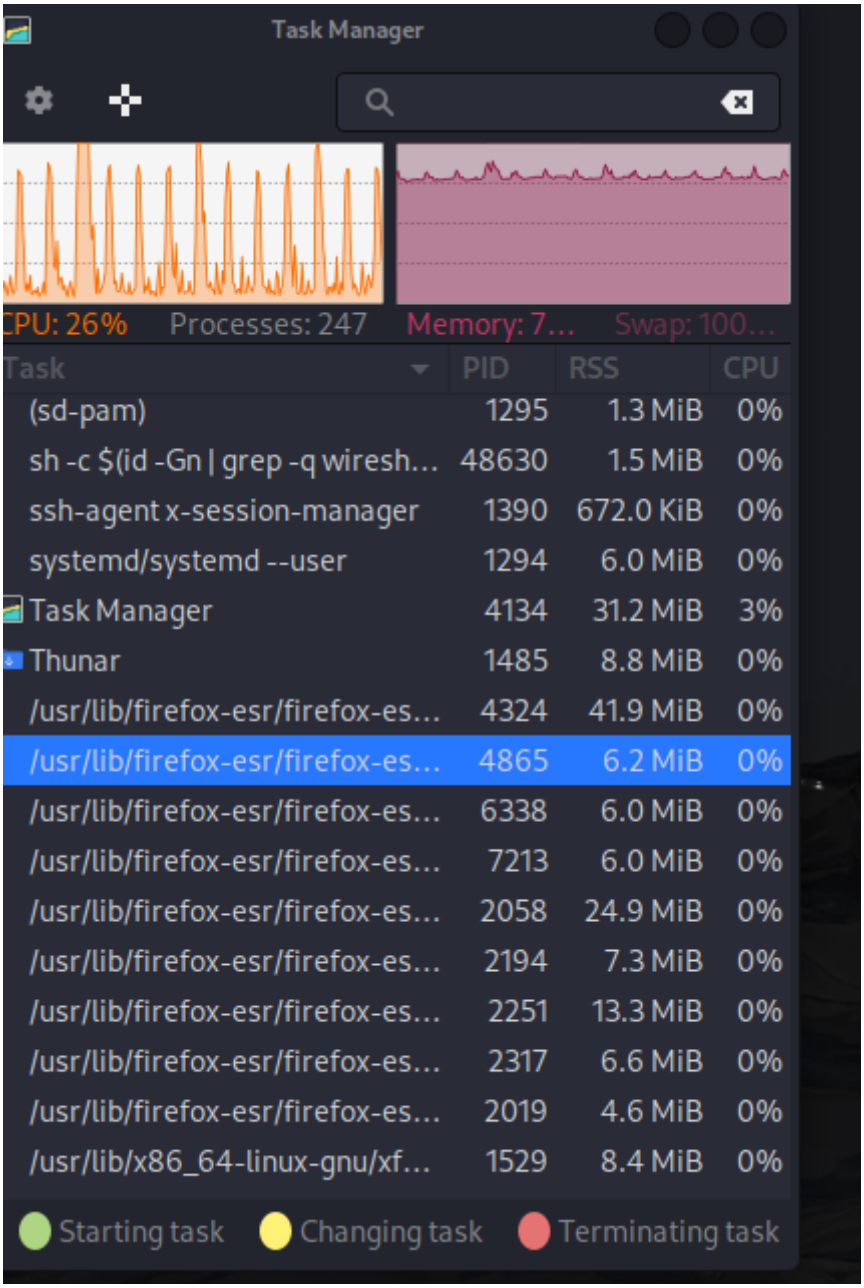
```
-------------+--------------+
osquery> sudo nano /etc/osquery/osquery.conf
    ...> {
    ...>   "schedule": {
    ...>     "network_interfaces": {
    ...>       "query": "SELECT * FROM interfaces;",
    ...>       "interval": 60
    ...>     },
    ...>     "listening_ports": {
    ...>       "query": "SELECT * FROM listening_ports;",
    ...>       "interval": 60
    ...>     },
    ...>     "open_sockets": {
    ...>       "query": "SELECT * FROM process_open_sockets;",
    ...>       "interval": 60
    ...>     }
    ...>   },
    ...>   "options": {
    ...>     "logger_plugin": "filesystem",
    ...>     "logger_path": "/var/log/osquery",
    ...>     "disable_distributed": true
    ...>   }
    ...> }
```

in which i stated where the logger_path should be and the logger_pluggin .

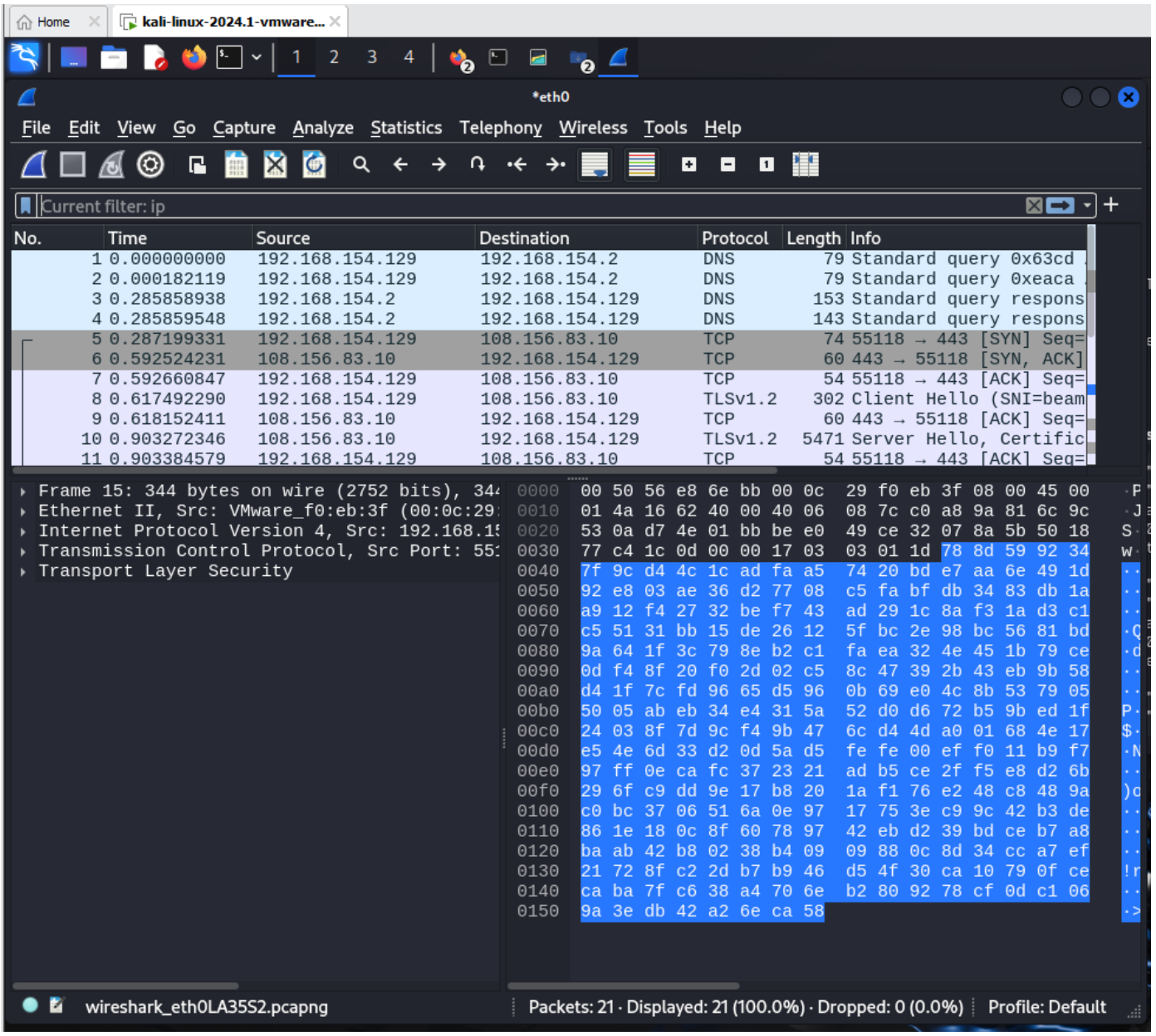
-I restart my osquery using the command

```
┌──(root㉿kali)-[~]
└─# sudo systemctl restart osqueryd
```

--Immediately I inputted this command , the task manager menu came up which allow users to monitor and manage the processes and applications running on my computer

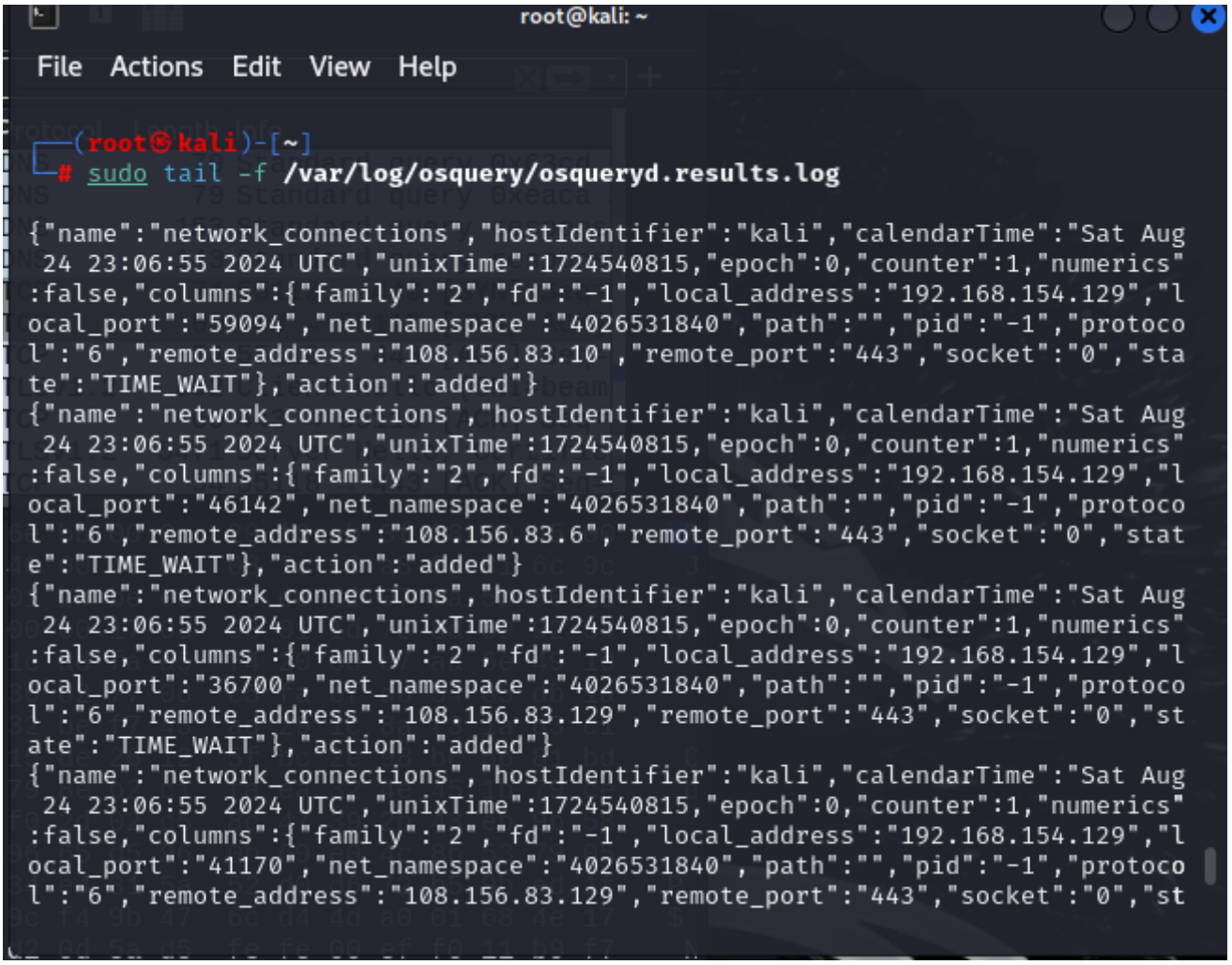


--I used my wireshark to capture traffic on eth0

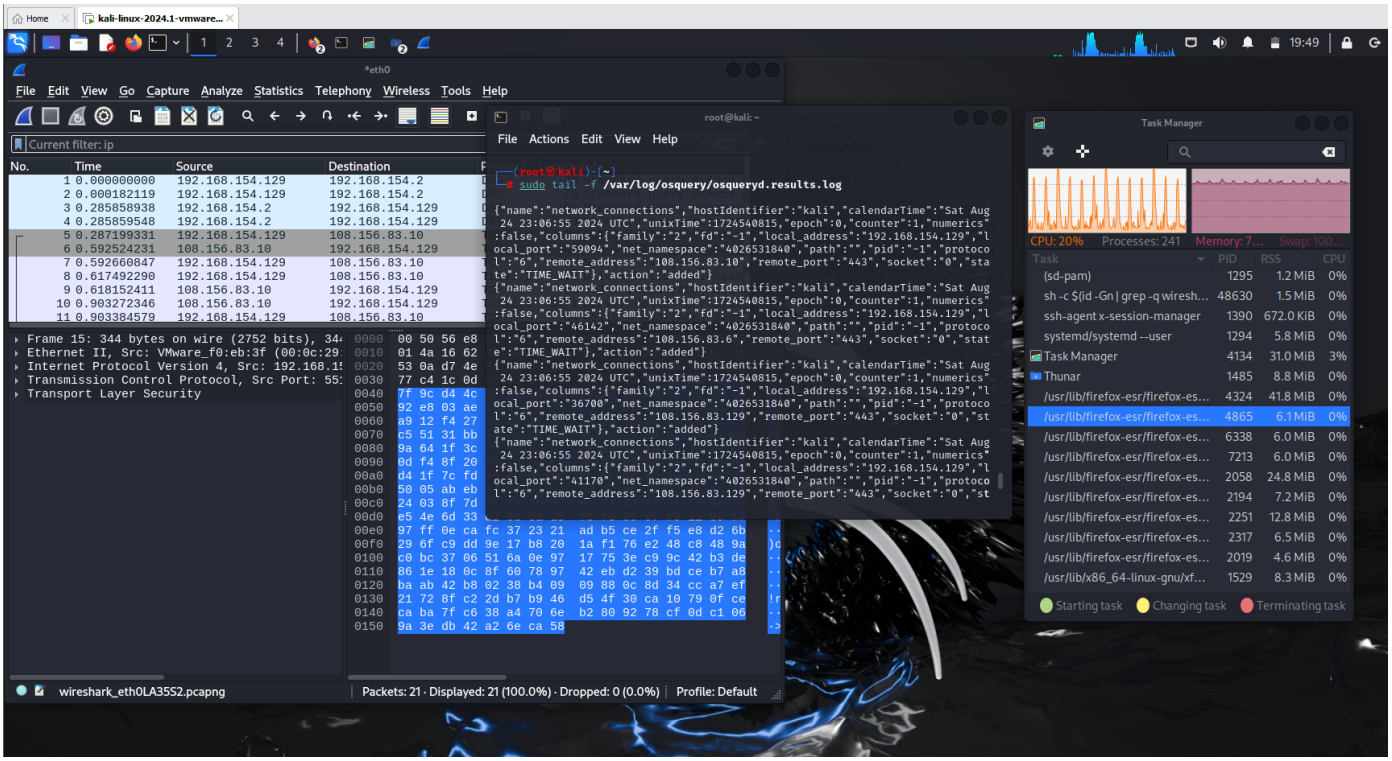


-After my analysis, I went back to my terminal and used the command to check for the logs being captured

sudo tail -f /var/log/osquery/osqueryd.results.log



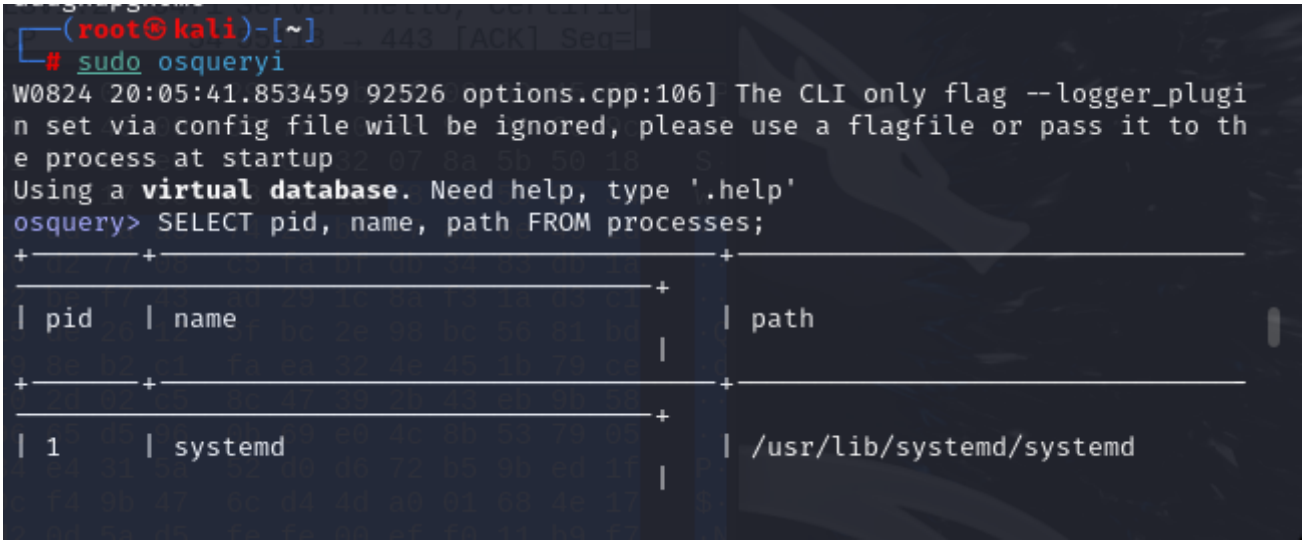
A combination of all screens showing the wireshark, task manager and linux terminal



TO create a custom query to detect potential indicator of compromise(IOCs) :

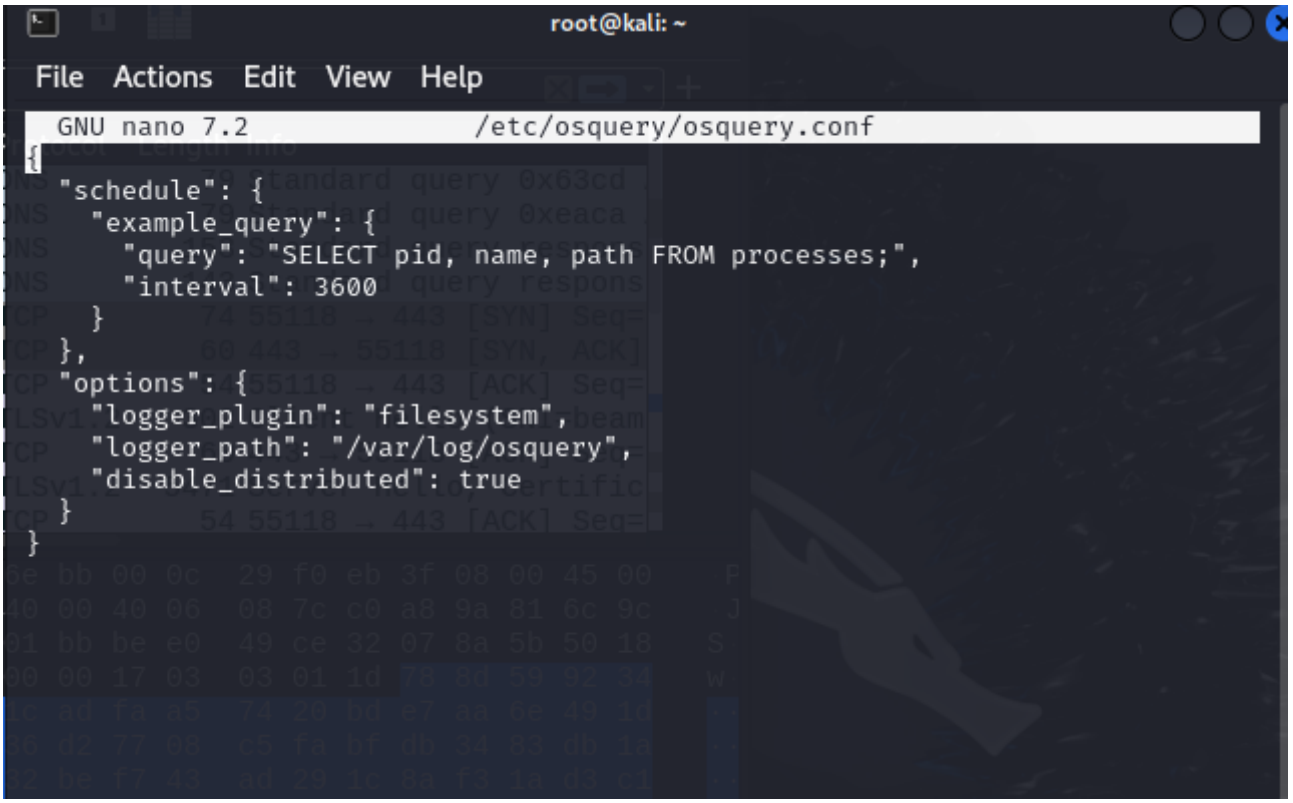
-TO detect for **suspicious process** which is also a sign of **indicator of compromise(loc)**

I use sudo osqueryi and then selected by PID, name and the path in which i want to be logged



I created a file and also created a query in the file

the query in the file is shown below



To detect for **unusual network connections** which is also an **indicator of compromise(IoC)**