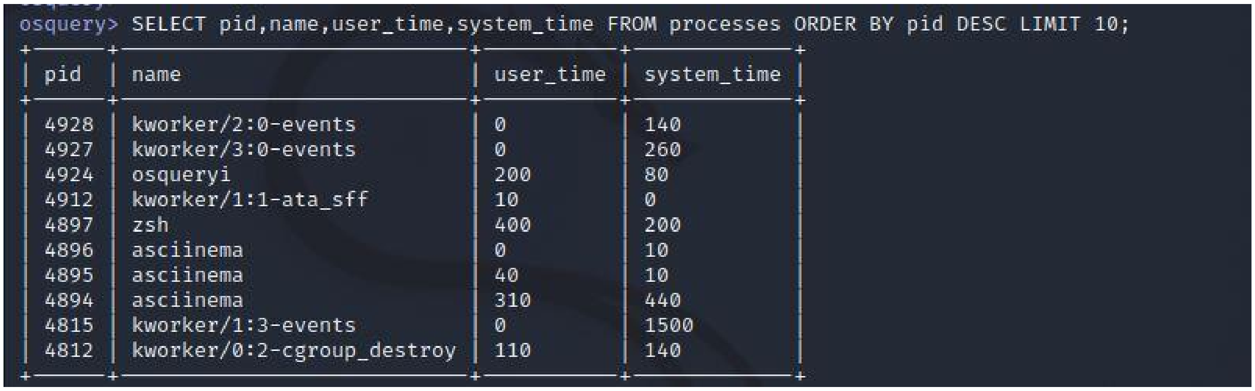
Project 4 - Auditing with OSquery and YARA

OSquery is an multi-platform operating system instrumentation framework. It is supported for Windows, OSX, Linux and FreeBSD. [1]

OSQuery exposes the operating system’s data in the form of a relational database that is tuned for high-performance.It can be used for various kinds of instrumentation of the OS. Running processes, kernel modules, installed packages and more for basic monitoring of the system. It can also be used for network monitoring to get open ports, firewall rules and more. It can even be connected with syslog to read syslog events. Some of the examples queries and their outputs are shown below.

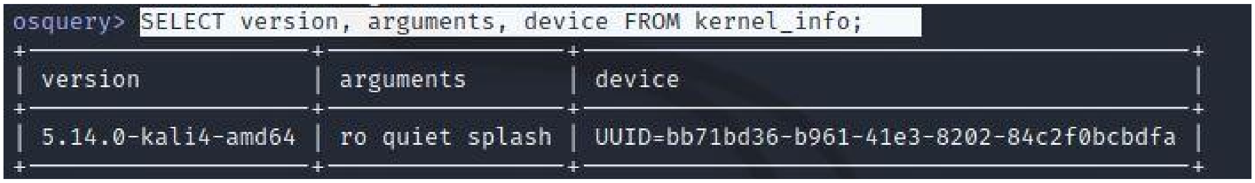
PART 1: BASIC MONITORING OF A SYSTEM

P1.1a - SELECT pid,name,user_time,system_time FROM processes ORDER BY pid DESC LIMIT 10;



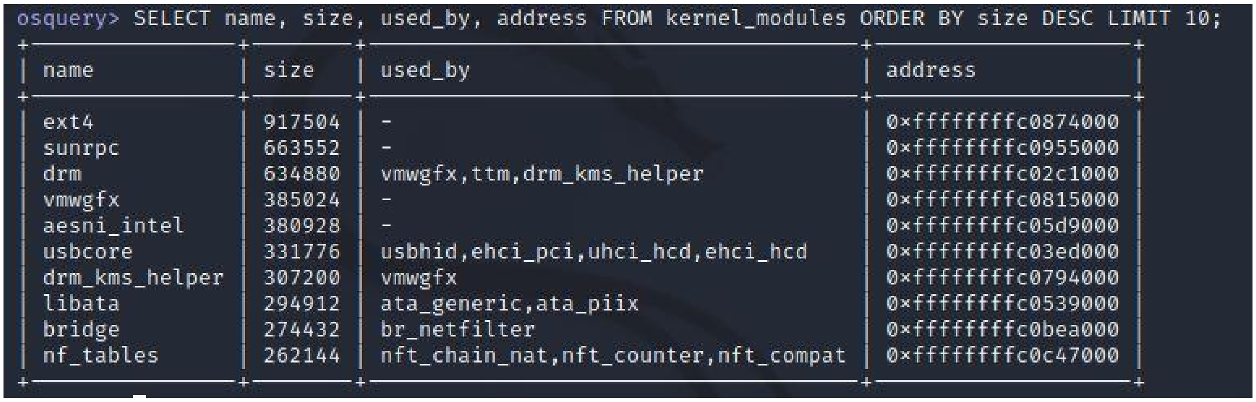
```
osquery> SELECT pid,name,user_time,system_time FROM processes ORDER BY pid DESC LIMIT 10;
+------+---------------------------+-----------+-------------+
| pid  | name                      | user_time | system_time |
+------+---------------------------+-----------+-------------+
| 4928 | kworker/2:0-events        | 0         | 140         |
| 4927 | kworker/3:0-events        | 0         | 260         |
| 4924 | osqueryi                  | 200       | 80          |
| 4912 | kworker/1:1-ata_sff       | 10        | 0           |
| 4897 | zsh                       | 400       | 200         |
| 4896 | asciinema                 | 0         | 10          |
| 4895 | asciinema                 | 40        | 10          |
| 4894 | asciinema                 | 310       | 440         |
| 4815 | kworker/1:3-events        | 0         | 1500        |
| 4812 | kworker/0:2-cgroup_destroy | 110      | 140         |
+------+---------------------------+-----------+-------------+
```

P1.2a - SELECT version, arguments, device FROM kernel_info;



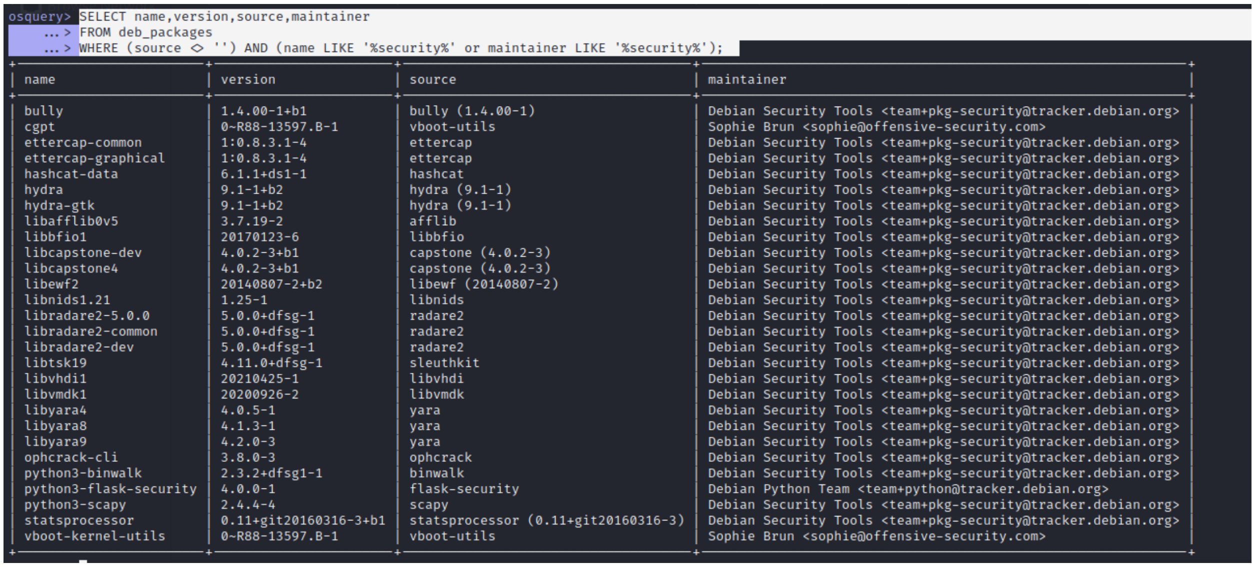
```
osquery> SELECT version, arguments, device FROM kernel_info;
+--------------------+-------------------+-------------------------------------------+
| version            | arguments         | device                                    |
+--------------------+-------------------+-------------------------------------------+
| 5.14.0-kali4-amd64 | ro quiet splash   | UUID=bb71bd36-b961-41e3-8202-84c2f0bcbdfa |
+--------------------+-------------------+-------------------------------------------+
```

P1.2b - SELECT name, size, used_by, address FROM kernel_modules ORDER BY name ASC LIMIT 10;



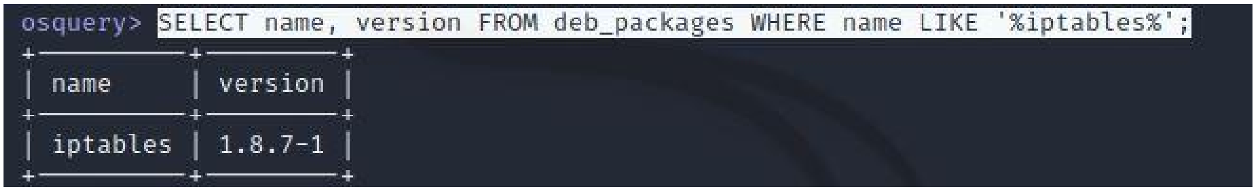
```
osquery> SELECT name, size, used_by, address FROM kernel_modules ORDER BY size DESC LIMIT 10;
+----------------+--------+--------------------------------------+--------------------+
| name           | size   | used_by                              | address            |
+----------------+--------+--------------------------------------+--------------------+
| ext4           | 917504 | -                                    | 0xffffffffc0874000 |
| sunrpc         | 663552 | -                                    | 0xffffffffc0955000 |
| drm            | 634880 | vmwgfx,ttm,drm_kms_helper            | 0xffffffffc02c1000 |
| vmwgfx         | 385024 | -                                    | 0xffffffffc0815000 |
| aesni_intel    | 380928 | -                                    | 0xffffffffc05d9000 |
| usbcore        | 331776 | usbhid,ehci_pci,uhci_hcd,ehci_hcd    | 0xffffffffc03ed000 |
| drm_kms_helper | 307200 | vmwgfx                               | 0xffffffffc0794000 |
| libata         | 294912 | ata_generic,ata_piix                 | 0xffffffffc0539000 |
| bridge         | 274432 | br_netfilter                         | 0xffffffffc0bea000 |
| nf_tables      | 262144 | nft_chain_nat,nft_counter,nft_compat | 0xffffffffc0c47000 |
+----------------+--------+--------------------------------------+--------------------+
```

P1.3a -SELECT name,version,source,maintainer
...> FROM deb_packages
...> WHERE (source <> '') AND (name LIKE '%security%' or maintainer LIKE '%security%');



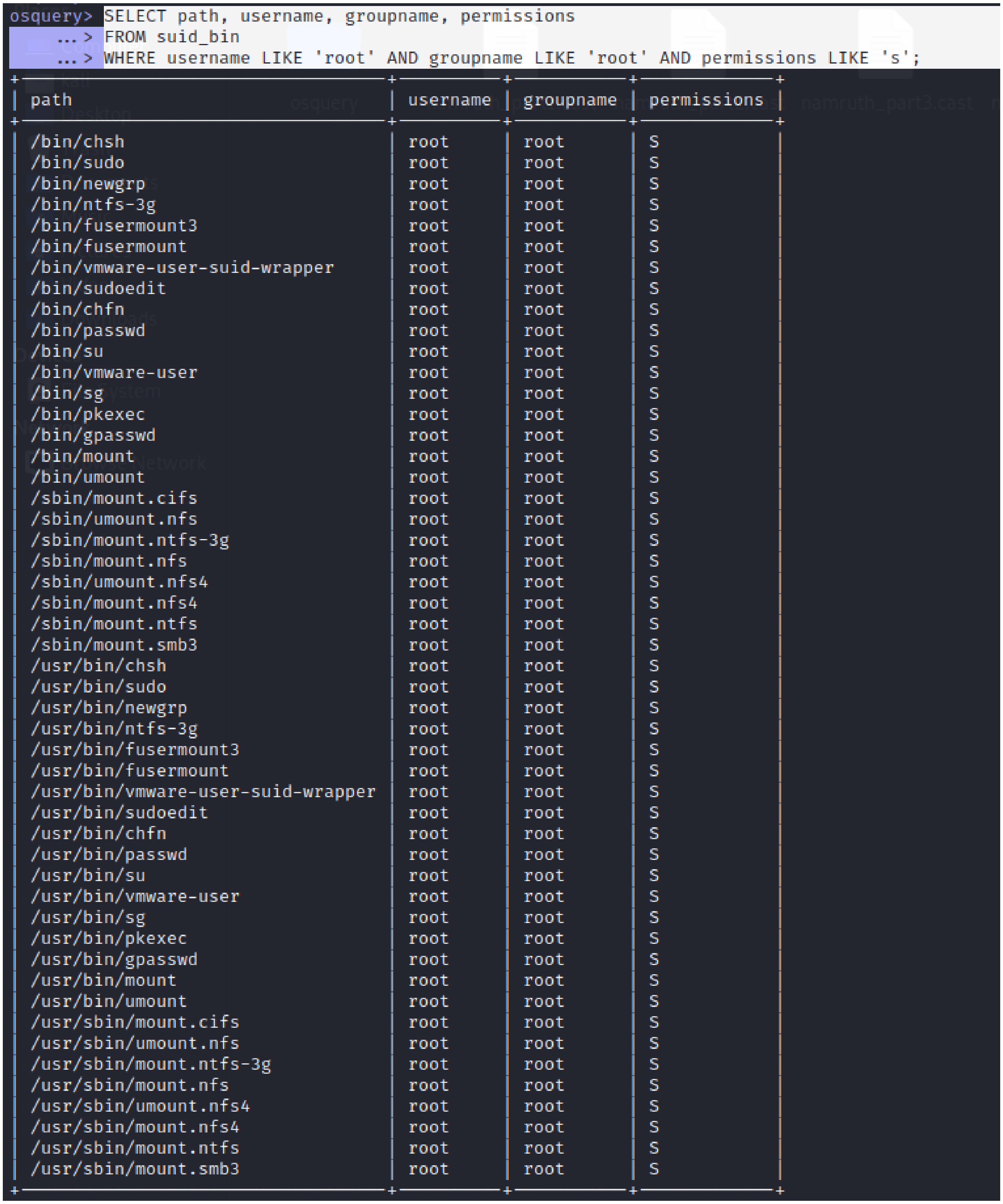
```
osquery> SELECT name,version,source,maintainer
    ... > FROM deb_packages
    ... > WHERE (source <> '') AND (name LIKE '%security%' or maintainer LIKE '%security%');
+------------------------+----------------------+-------------------------------------+--------------------------------------------------------------+
| name                   | version              | source                              | maintainer                                                   |
+------------------------+----------------------+-------------------------------------+--------------------------------------------------------------+
| bully                  | 1.4.00-1+b1          | bully (1.4.00-1)                    | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| cgpt                   | 0~R88-13597.B-1      | vboot-utils                         | Sophie Brun <sophie@offensive-security.com>                  |
| ettercap-common        | 1:0.8.3.1-4          | ettercap                            | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| ettercap-graphical     | 1:0.8.3.1-4          | ettercap                            | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| hashcat-data           | 6.1.1+ds1-1          | hashcat                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| hydra                  | 9.1-1+b2             | hydra (9.1-1)                       | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| hydra-gtk              | 9.1-1+b2             | hydra (9.1-1)                       | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libafflib0v5           | 3.7.19-2             | afflib                              | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libbfio1               | 20170123-6           | libbfio                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libcapstone-dev        | 4.0.2-3+b1           | capstone (4.0.2-3)                  | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libcapstone4           | 4.0.2-3+b1           | capstone (4.0.2-3)                  | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libewf2                | 20140807-2+b2        | libewf (20140807-2)                 | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libnids1.21            | 1.25-1               | libnids                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libradare2-5.0.0       | 5.0.0+dfsg-1         | radare2                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libradare2-common      | 5.0.0+dfsg-1         | radare2                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libradare2-dev         | 5.0.0+dfsg-1         | radare2                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libtsk19               | 4.11.0+dfsg-1        | sleuthkit                           | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libvhdi1               | 20210425-1           | libvhdi                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libvmdk1               | 20200926-2           | libvmdk                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libyara4               | 4.0.5-1              | yara                                | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libyara8               | 4.1.3-1              | yara                                | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| libyara9               | 4.2.0-3              | yara                                | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| ophcrack-cli           | 3.8.0-3              | ophcrack                            | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| python3-binwalk        | 2.3.2+dfsg1-1        | binwalk                             | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| python3-flask-security | 4.0.0-1              | flask-security                      | Debian Python Team <team+python@tracker.debian.org>          |
| python3-scapy          | 2.4.4-4              | scapy                               | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| statsprocessor         | 0.11+git20160316-3+b1 | statsprocessor (0.11+git20160316-3) | Debian Security Tools <team+pkg-security@tracker.debian.org> |
| vboot-kernel-utils     | 0~R88-13597.B-1      | vboot-utils                         | Sophie Brun <sophie@offensive-security.com>                  |
+------------------------+----------------------+-------------------------------------+--------------------------------------------------------------+
```

P1.3b - SELECT name, version FROM deb_packages WHERE name LIKE '%iptables%';



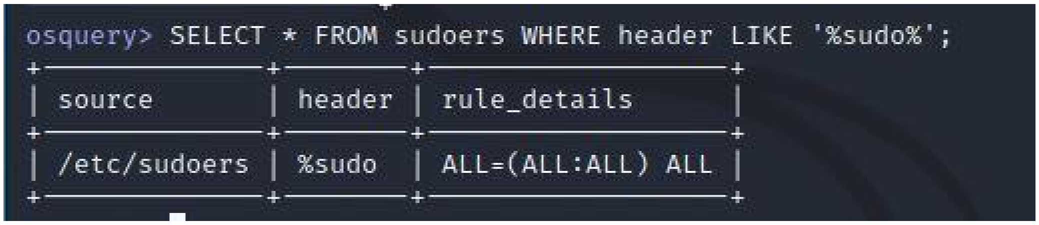
```
osquery> SELECT name, version FROM deb_packages WHERE name LIKE '%iptables%';
+----------+---------+
| name     | version |
+----------+---------+
| iptables | 1.8.7-1 |
+----------+---------+
```

P1.4a - SELECT path, username, groupname, permissions
...> FROM suid_bin
...> WHERE username LIKE 'root' AND groupname LIKE 'root' AND permissions LIKE 's';



```
osquery> SELECT path, username, groupname, permissions
    ...> FROM suid_bin
    ...> WHERE username LIKE 'root' AND groupname LIKE 'root' AND permissions LIKE 's';
+-----------------------------------+----------+-----------+-------------+
| path                              | username | groupname | permissions |
+-----------------------------------+----------+-----------+-------------+
| /bin/chsh                         | root     | root      | S           |
| /bin/sudo                         | root     | root      | S           |
| /bin/newgrp                       | root     | root      | S           |
| /bin/ntfs-3g                      | root     | root      | S           |
| /bin/fusermount3                  | root     | root      | S           |
| /bin/fusermount                   | root     | root      | S           |
| /bin/vmware-user-suid-wrapper     | root     | root      | S           |
| /bin/sudoedit                     | root     | root      | S           |
| /bin/chfn                         | root     | root      | S           |
| /bin/passwd                       | root     | root      | S           |
| /bin/su                           | root     | root      | S           |
| /bin/vmware-user                  | root     | root      | S           |
| /bin/sg                           | root     | root      | S           |
| /bin/pkexec                       | root     | root      | S           |
| /bin/gpasswd                      | root     | root      | S           |
| /bin/mount                        | root     | root      | S           |
| /bin/umount                       | root     | root      | S           |
| /sbin/mount.cifs                  | root     | root      | S           |
| /sbin/umount.nfs                  | root     | root      | S           |
| /sbin/mount.ntfs-3g               | root     | root      | S           |
| /sbin/mount.nfs                   | root     | root      | S           |
| /sbin/umount.nfs4                 | root     | root      | S           |
| /sbin/mount.nfs4                  | root     | root      | S           |
| /sbin/mount.ntfs                  | root     | root      | S           |
| /sbin/mount.smb3                  | root     | root      | S           |
| /usr/bin/chsh                     | root     | root      | S           |
| /usr/bin/sudo                     | root     | root      | S           |
| /usr/bin/newgrp                   | root     | root      | S           |
| /usr/bin/ntfs-3g                  | root     | root      | S           |
| /usr/bin/fusermount3              | root     | root      | S           |
| /usr/bin/fusermount               | root     | root      | S           |
| /usr/bin/vmware-user-suid-wrapper | root     | root      | S           |
| /usr/bin/sudoedit                 | root     | root      | S           |
| /usr/bin/chfn                     | root     | root      | S           |
| /usr/bin/passwd                   | root     | root      | S           |
| /usr/bin/su                       | root     | root      | S           |
| /usr/bin/vmware-user              | root     | root      | S           |
| /usr/bin/sg                       | root     | root      | S           |
| /usr/bin/pkexec                   | root     | root      | S           |
| /usr/bin/gpasswd                  | root     | root      | S           |
| /usr/bin/mount                    | root     | root      | S           |
| /usr/bin/umount                   | root     | root      | S           |
| /usr/sbin/mount.cifs              | root     | root      | S           |
| /usr/sbin/umount.nfs              | root     | root      | S           |
| /usr/sbin/mount.ntfs-3g           | root     | root      | S           |
| /usr/sbin/mount.nfs               | root     | root      | S           |
| /usr/sbin/umount.nfs4             | root     | root      | S           |
| /usr/sbin/mount.nfs4              | root     | root      | S           |
| /usr/sbin/mount.ntfs              | root     | root      | S           |
| /usr/sbin/mount.smb3              | root     | root      | S           |
+-----------------------------------+----------+-----------+-------------+
```

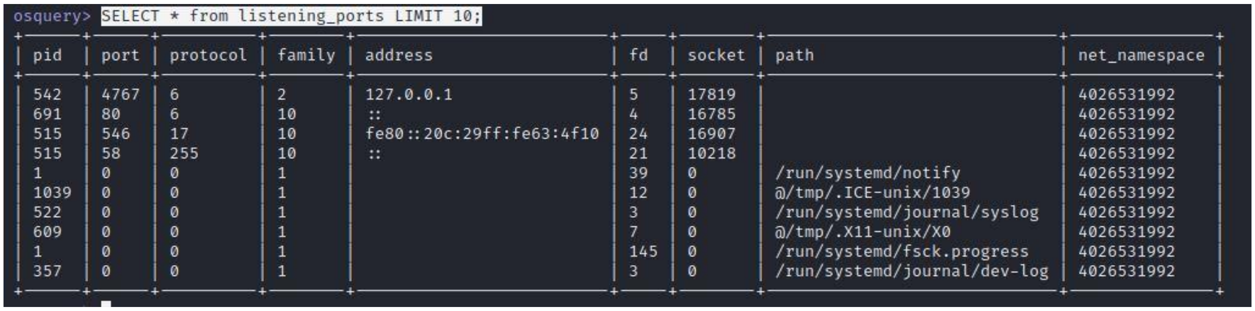
P1.4b - SELECT * FROM sudoers WHERE header LIKE '%sudo%';



```
osquery> SELECT * FROM sudoers WHERE header LIKE '%sudo%';
+--------------+--------+-------------------+
| source       | header | rule_details      |
+--------------+--------+-------------------+
| /etc/sudoers | %sudo  | ALL=(ALL:ALL) ALL |
+--------------+--------+-------------------+
```

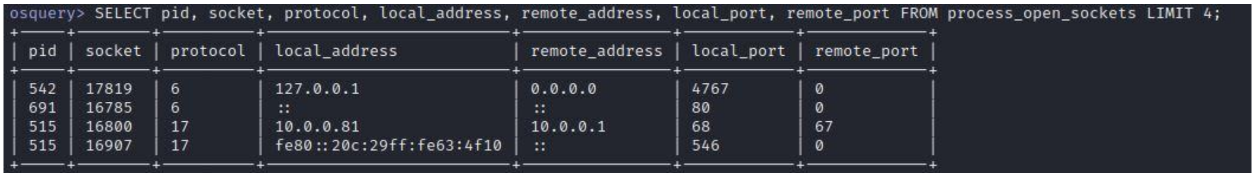
PART 2: NETWORK AND PROCESS MONITORING

P2.1a - SELECT * from listening_ports LIMIT 10;



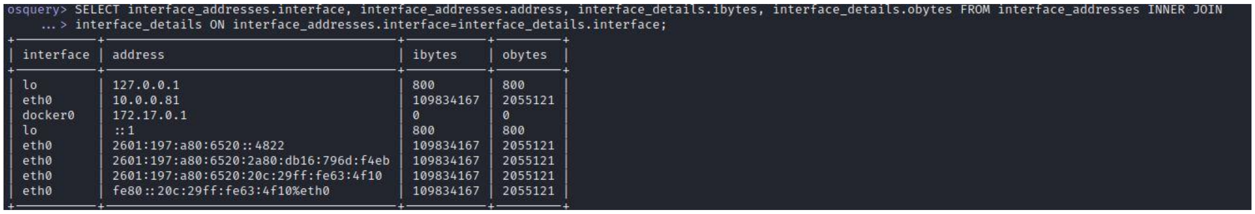
```
osquery> SELECT * from listening_ports LIMIT 10;
+------+------+----------+--------+---------------------------+-----+--------+-----------------------------+---------------+
| pid  | port | protocol | family | address                   | fd  | socket | path                        | net_namespace |
+------+------+----------+--------+---------------------------+-----+--------+-----------------------------+---------------+
| 542  | 4767 | 6        | 2      | 127.0.0.1                 | 5   | 17819  |                             | 4026531992    |
| 691  | 80   | 6        | 10     | ::                        | 4   | 16785  |                             | 4026531992    |
| 515  | 546  | 17       | 10     | fe80::20c:29ff:fe63:4f10  | 24  | 16907  |                             | 4026531992    |
| 515  | 58   | 255      | 10     | ::                        | 21  | 10218  |                             | 4026531992    |
| 1    | 0    | 0        | 1      |                           | 39  | 0      | /run/systemd/notify         | 4026531992    |
| 1039 | 0    | 0        | 1      |                           | 12  | 0      | @/tmp/.ICE-unix/1039        | 4026531992    |
| 522  | 0    | 0        | 1      |                           | 3   | 0      | /run/systemd/journal/syslog | 4026531992    |
| 609  | 0    | 0        | 1      |                           | 7   | 0      | @/tmp/.X11-unix/X0          | 4026531992    |
| 1    | 0    | 0        | 1      |                           | 145 | 0      | /run/systemd/fsck.progress  | 4026531992    |
| 357  | 0    | 0        | 1      |                           | 3   | 0      | /run/systemd/journal/dev-log | 4026531992   |
+------+------+----------+--------+---------------------------+-----+--------+-----------------------------+---------------+
```

P2.1b - SELECT pid, socket, protocol, local_address, remote_address, local_port, remote_port FROM process_open_sockets LIMIT 4;



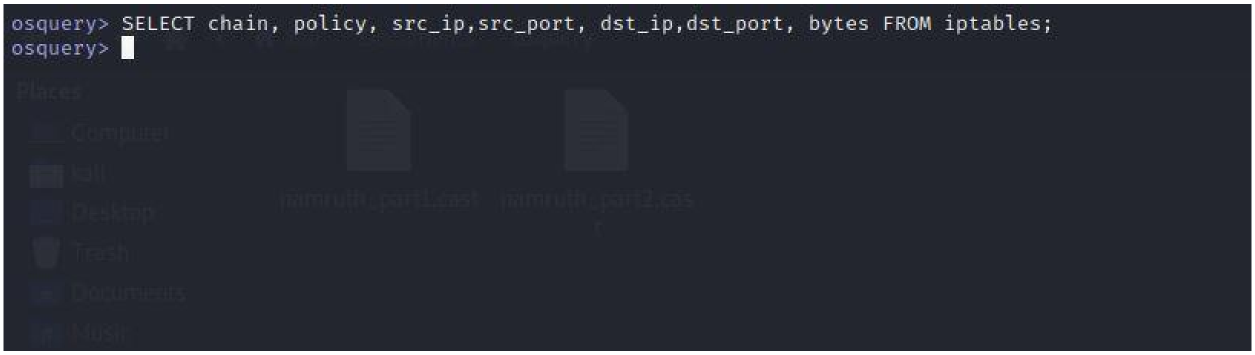
```
osquery> SELECT pid, socket, protocol, local_address, remote_address, local_port, remote_port FROM process_open_sockets LIMIT 4;
+-----+--------+----------+--------------------------+----------------+------------+-------------+
| pid | socket | protocol | local_address            | remote_address | local_port | remote_port |
+-----+--------+----------+--------------------------+----------------+------------+-------------+
| 542 | 17819  | 6        | 127.0.0.1                | 0.0.0.0        | 4767       | 0           |
| 691 | 16785  | 6        | ::                       | ::             | 80         | 0           |
| 515 | 16800  | 17       | 10.0.0.81                | 10.0.0.1       | 68         | 67          |
| 515 | 16907  | 17       | fe80::20c:29ff:fe63:4f10 | ::             | 546        | 0           |
+-----+--------+----------+--------------------------+----------------+------------+-------------+
```

P2.1c -SELECT interface_addresses.interface, interface_addresses.address, interface_details.ibytes, interface_details.obytes FROM interface_addresses INNER JOIN interface_details
ON interface_addresses.interface=interface_details.interface;



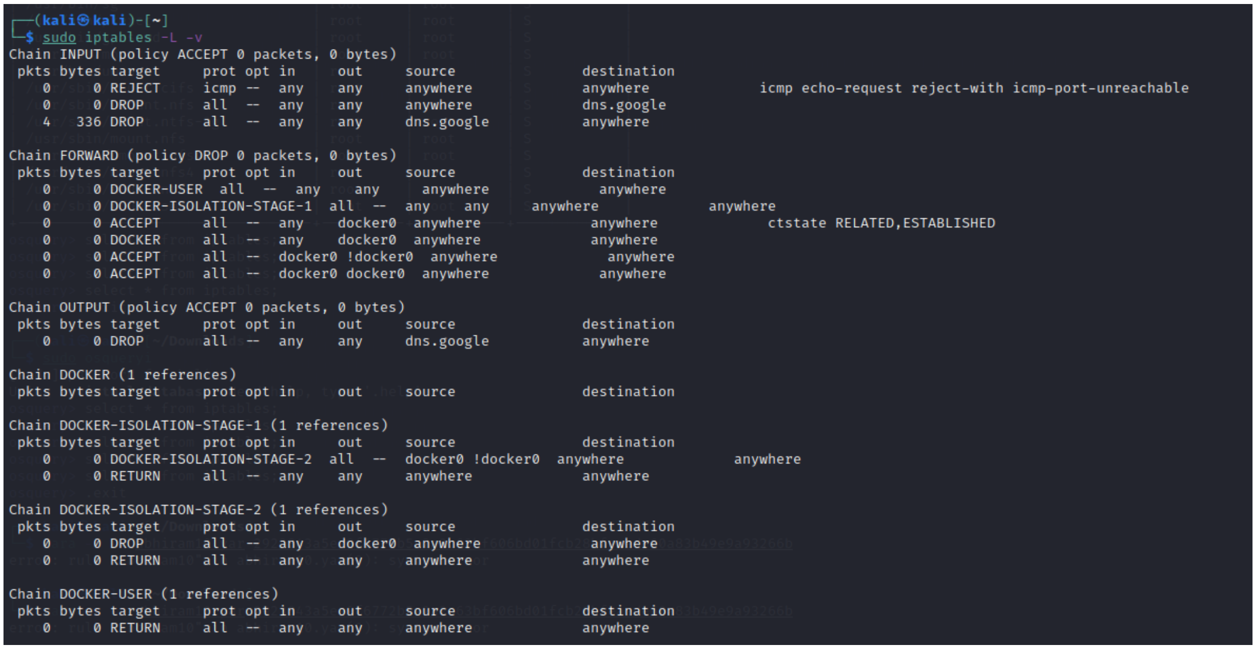
```
osquery> SELECT interface_addresses.interface, interface_addresses.address, interface_details.ibytes, interface_details.obytes FROM interface_addresses INNER JOIN
    ...> interface_details ON interface_addresses.interface=interface_details.interface;
+-----------+-----------------------------------------+-----------+---------+
| interface | address                                 | ibytes    | obytes  |
+-----------+-----------------------------------------+-----------+---------+
| lo        | 127.0.0.1                               | 800       | 800     |
| eth0      | 10.0.0.81                               | 109834167 | 2055121 |
| docker0   | 172.17.0.1                              | 0         | 0       |
| lo        | ::1                                     | 800       | 800     |
| eth0      | 2601:197:a80:6520::4822                 | 109834167 | 2055121 |
| eth0      | 2601:197:a80:6520:2a80:db16:796d:f4eb   | 109834167 | 2055121 |
| eth0      | 2601:197:a80:6520:20c:29ff:fe63:4f10    | 109834167 | 2055121 |
| eth0      | fe80::20c:29ff:fe63:4f10%eth0           | 109834167 | 2055121 |
+-----------+-----------------------------------------+-----------+---------+
```

P2.2a -SELECT chain, policy, src_ip,src_port, dst_ip,dst_port, bytes FROM iptables;



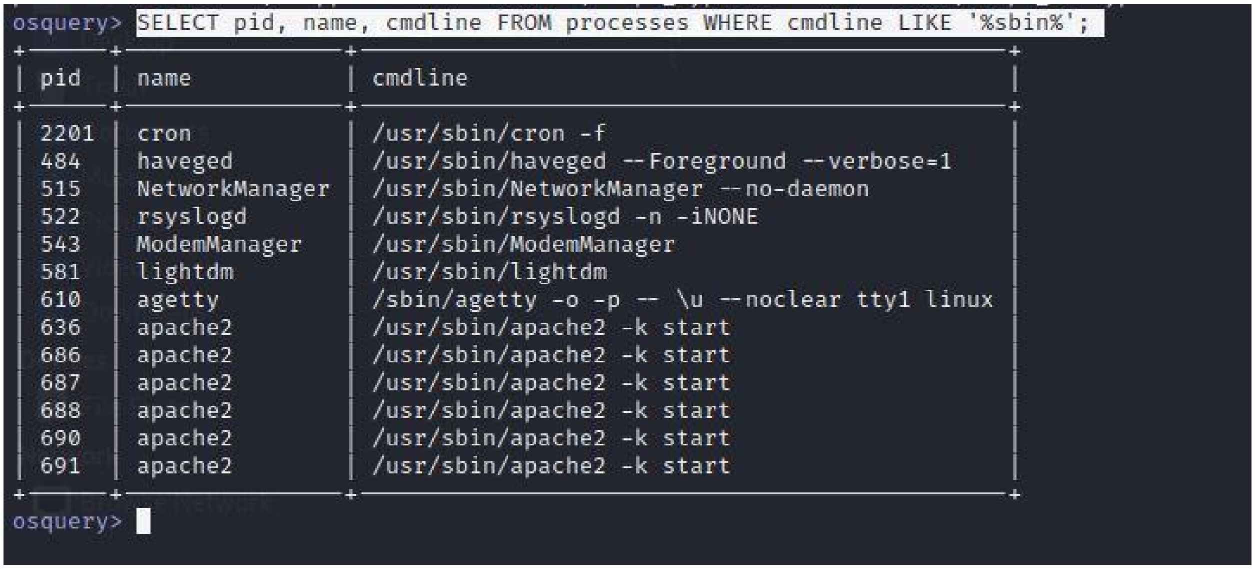
```
osquery> SELECT chain, policy, src_ip,src_port, dst_ip,dst_port, bytes FROM iptables;
osquery> 
```

Kali seems to have a bug in this table implementation as pointed out by TA Vineeth in Piazza. Even though there are iptable rules, they dont seem to be listed here.
IPtables rules are listed in the screenshot below



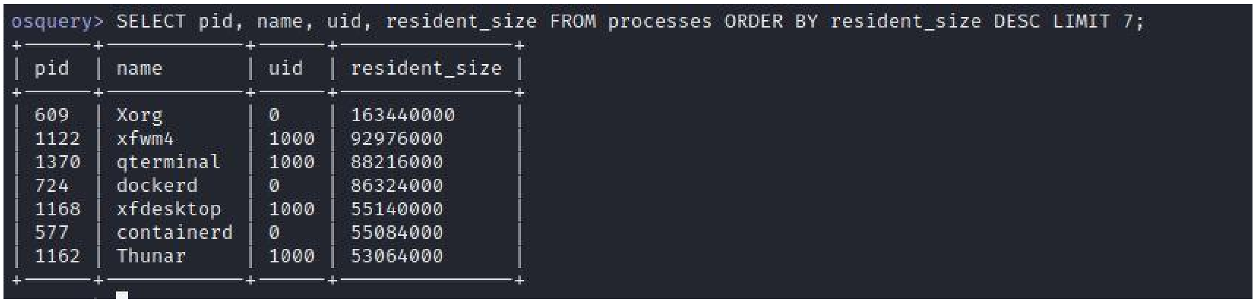
```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     icmp --  any    any     anywhere             anywhere             icmp echo-request reject-with icmp-port-unreachable
    0     0 DROP       all  --  any    any     anywhere             dns.google
    4   336 DROP       all  --  any    any     dns.google           anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DOCKER-USER  all  --  any    any     anywhere             anywhere
    0     0 DOCKER-ISOLATION-STAGE-1  all  --  any    any     anywhere             anywhere
    0     0 ACCEPT     all  --  any    docker0  anywhere             anywhere             ctstate RELATED,ESTABLISHED
    0     0 DOCKER     all  --  any    docker0  anywhere             anywhere
    0     0 ACCEPT     all  --  docker0 !docker0  anywhere             anywhere
    0     0 ACCEPT     all  --  docker0 docker0  anywhere             anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  any    any     dns.google           anywhere

Chain DOCKER (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DOCKER-ISOLATION-STAGE-2  all  --  docker0 !docker0  anywhere             anywhere
    0     0 RETURN     all  --  any    any     anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  any    docker0  anywhere             anywhere
    0     0 RETURN     all  --  any    any     anywhere             anywhere

Chain DOCKER-USER (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RETURN     all  --  any    any     anywhere             anywhere
```

P2.3a - SELECT pid, name, cmdline FROM processes WHERE cmdline LIKE '%sbin%';



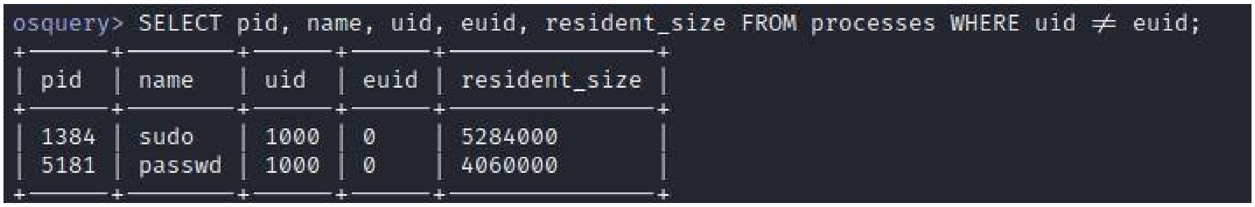
```
osquery> SELECT pid, name, cmdline FROM processes WHERE cmdline LIKE '%sbin%';
+------+----------------+----------------------------------------------+
| pid  | name           | cmdline                                      |
+------+----------------+----------------------------------------------+
| 2201 | cron           | /usr/sbin/cron -f                            |
| 484  | haveged        | /usr/sbin/haveged --Foreground --verbose=1   |
| 515  | NetworkManager | /usr/sbin/NetworkManager --no-daemon         |
| 522  | rsyslogd       | /usr/sbin/rsyslogd -n -iNONE                 |
| 543  | ModemManager   | /usr/sbin/ModemManager                       |
| 581  | lightdm        | /usr/sbin/lightdm                            |
| 610  | agetty         | /sbin/agetty -o -p -- \u --noclear tty1 linux |
| 636  | apache2        | /usr/sbin/apache2 -k start                   |
| 686  | apache2        | /usr/sbin/apache2 -k start                   |
| 687  | apache2        | /usr/sbin/apache2 -k start                   |
| 688  | apache2        | /usr/sbin/apache2 -k start                   |
| 690  | apache2        | /usr/sbin/apache2 -k start                   |
| 691  | apache2        | /usr/sbin/apache2 -k start                   |
+------+----------------+----------------------------------------------+
osquery> 
```

P2.3b - SELECT pid, name, uid, resident_size FROM processes ORDER BY resident_size DESC LIMIT 7;



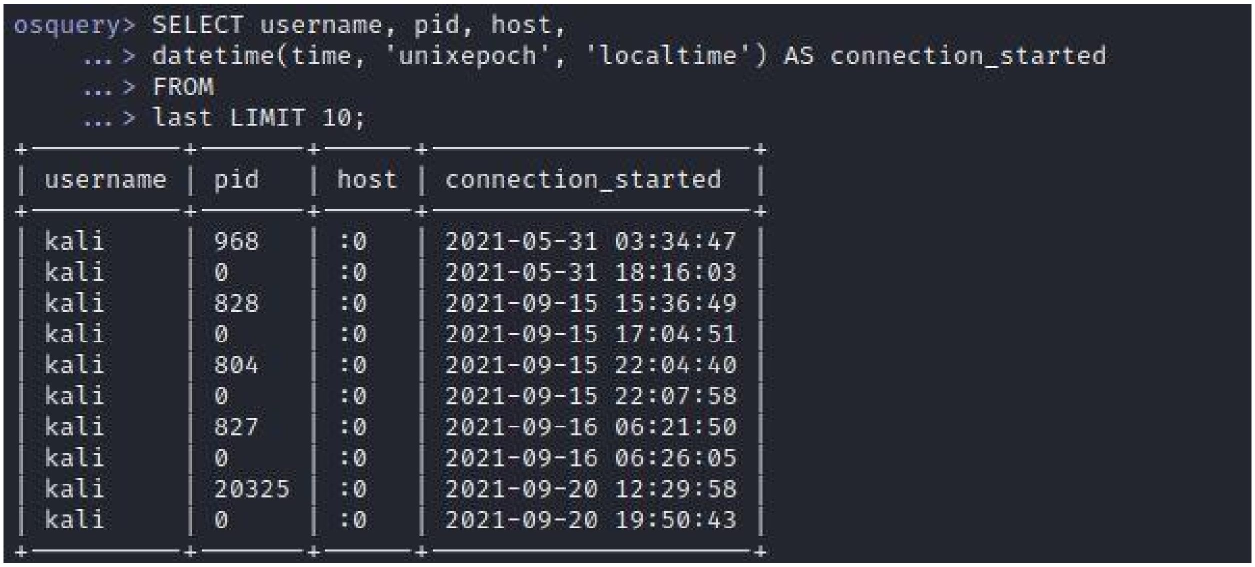
```
osquery> SELECT pid, name, uid, resident_size FROM processes ORDER BY resident_size DESC LIMIT 7;
+------+-------------+------+---------------+
| pid  | name        | uid  | resident_size |
+------+-------------+------+---------------+
| 609  | Xorg        | 0    | 163440000     |
| 1122 | xfwm4       | 1000 | 92976000      |
| 1370 | qterminal   | 1000 | 88216000      |
| 724  | dockerd     | 0    | 86324000      |
| 1168 | xfdesktop   | 1000 | 55140000      |
| 577  | containerd  | 0    | 55084000      |
| 1162 | Thunar      | 1000 | 53064000      |
+------+-------------+------+---------------+
```

P2.3c - SELECT pid, name, uid, euid, resident_size FROM processes WHERE uid != euid;



```
osquery> SELECT pid, name, uid, euid, resident_size FROM processes WHERE uid ≠ euid;
+------+--------+------+------+---------------+
| pid  | name   | uid  | euid | resident_size |
+------+--------+------+------+---------------+
| 1384 | sudo   | 1000 | 0    | 5284000       |
| 5181 | passwd | 1000 | 0    | 4060000       |
+------+--------+------+------+---------------+
```

P2.4a - SELECT username, pid, host,
...> datetime(time, 'unixepoch', 'localtime') AS connection_started
...> FROM
...> last LIMIT 10;

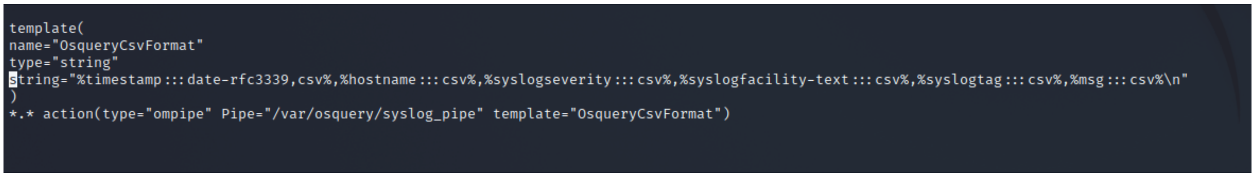


```
osquery> SELECT username, pid, host,
    ...> datetime(time, 'unixepoch', 'localtime') AS connection_started
    ...> FROM
    ...> last LIMIT 10;
+----------+-------+------+---------------------+
| username | pid   | host | connection_started  |
+----------+-------+------+---------------------+
| kali     | 968   | :0   | 2021-05-31 03:34:47 |
| kali     | 0     | :0   | 2021-05-31 18:16:03 |
| kali     | 828   | :0   | 2021-09-15 15:36:49 |
| kali     | 0     | :0   | 2021-09-15 17:04:51 |
| kali     | 804   | :0   | 2021-09-15 22:04:40 |
| kali     | 0     | :0   | 2021-09-15 22:07:58 |
| kali     | 827   | :0   | 2021-09-16 06:21:50 |
| kali     | 0     | :0   | 2021-09-16 06:26:05 |
| kali     | 20325 | :0   | 2021-09-20 12:29:58 |
| kali     | 0     | :0   | 2021-09-20 19:50:43 |
+----------+-------+------+---------------------+
```

PART 3: ENABLING THE EVENTS and Syslog

Syslog is a powerful Linux logging framework that can be used for various logs and events management. It is used as a standard logging format widely across the industry. One of the major advantages of syslog is - logging messages can be classified based on the severity level such as - emergency, warning, informational etc. This will make it easier for anyone who is analyzing the logs to prioritize whats is important based on the use case. It can be used as central logging system to collect logs from various applications and various machines in the network into a centralized syslog server.
OSquery can be linked with syslog to get the events of the system from the osqueryi interface in the form SQL queries.

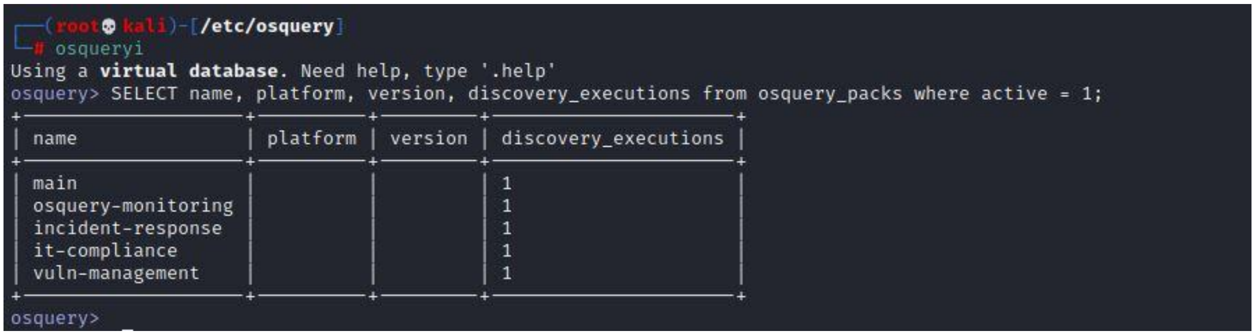
This can be done with the help of some configuration changes to allow syslog to pipe the messages to osquery and osquery can then populate the table with the events received from syslog. An example of what can be added /etc/ryslog.conf is shown in the screenshot below:



```
template(
name="OsqueryCsvFormat"
type="string"
string="%timestamp:::date-rfc3339,csv%,%hostname:::csv%,%syslogseverity:::csv%,%syslogfacility-text:::csv%,%syslogtag:::csv%,%msg:::csv%\n"
)
*.* action(type="ompipe" Pipe="/var/osquery/syslog_pipe" template="OsqueryCsvFormat")
```

After syslog is configured to pipe values into osquery, we can add a configuration file that determines the settings needs to be used by osquery while handling the events. Options such as logger_path, verbose, enable_syslog and many more. OSquery works based on the values set to these options. More of the options can be found in the osquery documentation and digital ocean article linked below in references. [2][3]
One of the additions to these configuration files is the packs - these are extended configuration files provided by osquery community so that they can directly be used without having to write then on our own. These packs can be used for incident-response, vuln-management and more. Active packs in the system are listed below using the osquery_packs table. [4]

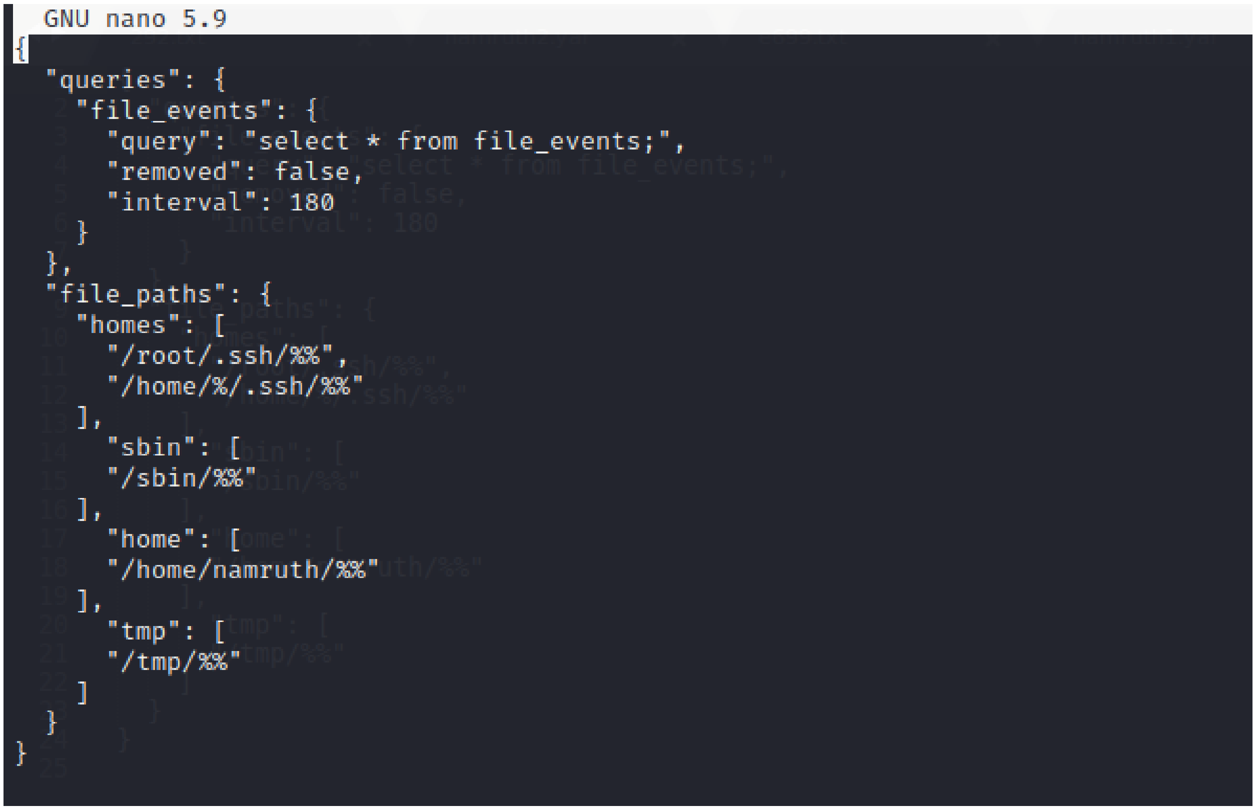
P 3.1



```
┌──(root💀kali)-[/etc/osquery]
└─# osqueryi
Using a virtual database. Need help, type '.help'
osquery> SELECT name, platform, version, discovery_executions from osquery_packs where active = 1;
+--------------------+----------+---------+----------------------+
| name               | platform | version | discovery_executions |
+--------------------+----------+---------+----------------------+
| main               |          |         | 1                    |
| osquery-monitoring |          |         | 1                    |
| incident-response  |          |         | 1                    |
| it-compliance      |          |         | 1                    |
| vuln-management    |          |         | 1                    |
+--------------------+----------+---------+----------------------+
osquery>
```

PART 4: FILE INTEGRITY MONITORING

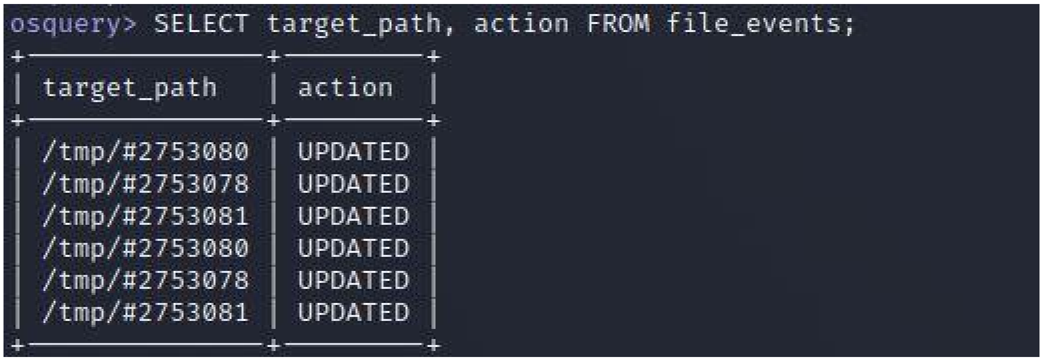
File integrity monitoring can be very useful to keep track of important files and how and when they are being changed. Osquery supports FIM by modifying the configuration file listed above to enable_file_events and few other parameters that need to be changed in the configuration file.
File paths to be monitored has an option to use wildcard characters that can be used to specific files in one level or recursively or ending with specific characters and so on. [5]
For this example, I made a simple pack that I have modified to use monitor the files in /home/namruth. Screenshot of the pack is shown below:



```
  GNU nano 5.9
{
  "queries": {
    "file_events": {
      "query": "select * from file_events;",
      "removed": false,
      "interval": 180
    }
  },
  "file_paths": {
    "homes": [
      "/root/.ssh/%%",
      "/home/%/.ssh/%%"
    ],
      "sbin": [
      "/sbin/%%"
    ],
      "home": [
      "/home/namruth/%%"
    ],
      "tmp": [
      "/tmp/%%"
    ]
  }
}
```

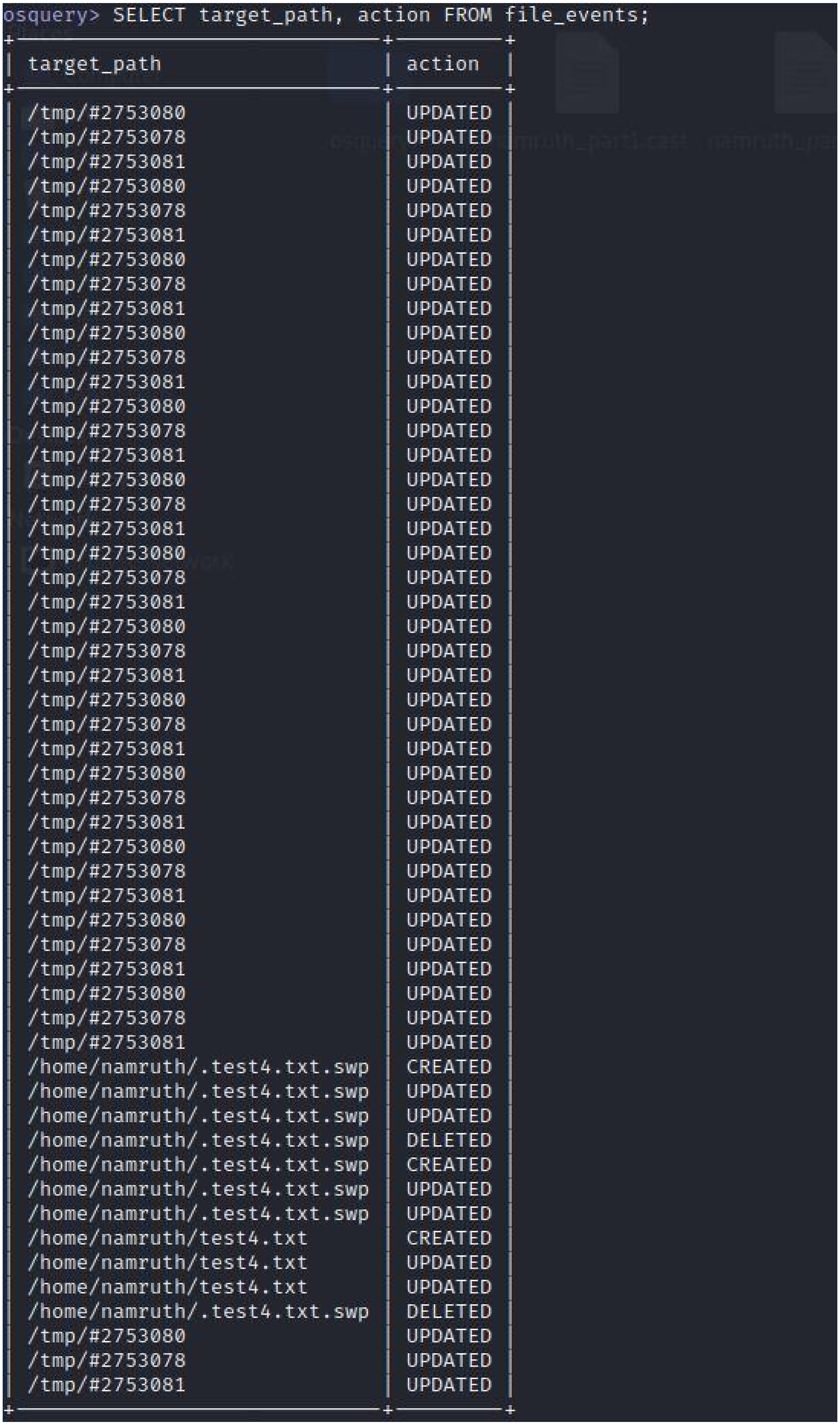
Duration of the interval to run the query can be set (180 seconds in this case) and file paths can be set with wild characters. Path to this pack needs to be added in the osquery.conf file. Screenshots below show the file events generated before and after creating a text file /home/namruth folder which is being monitored.

P4.1



```
osquery> SELECT target_path, action FROM file_events;
+---------------+---------+
| target_path   | action  |
+---------------+---------+
| /tmp/#2753080 | UPDATED |
| /tmp/#2753078 | UPDATED |
| /tmp/#2753081 | UPDATED |
| /tmp/#2753080 | UPDATED |
| /tmp/#2753078 | UPDATED |
| /tmp/#2753081 | UPDATED |
+---------------+---------+
```

P4.2

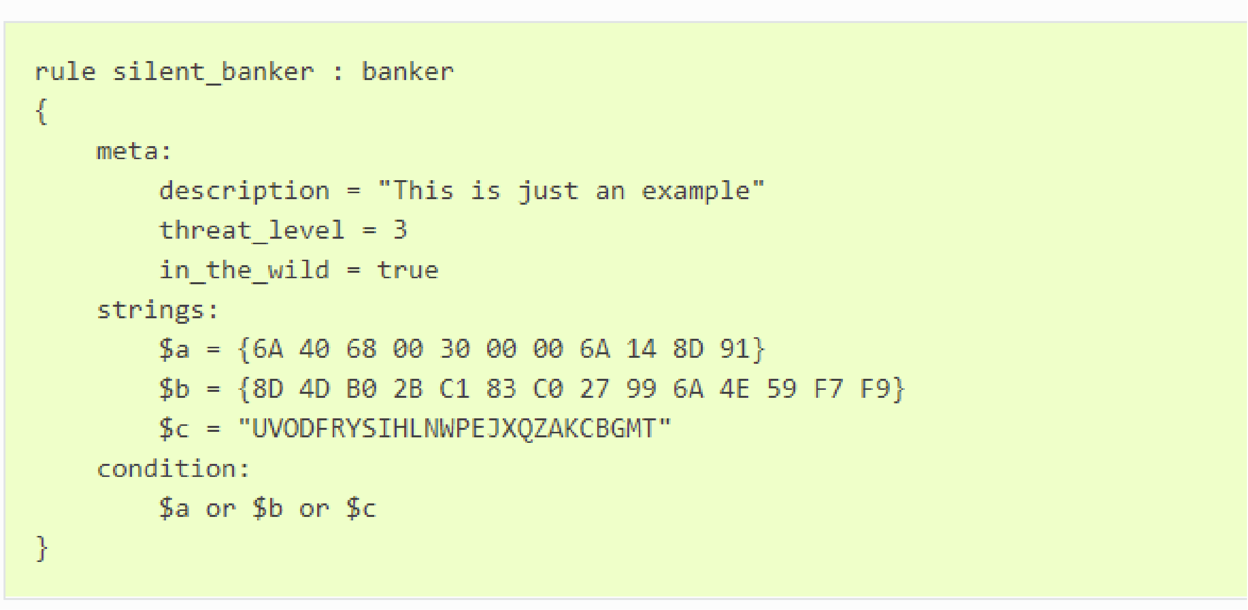


```
osquery> SELECT target_path, action FROM file_events;
+------------------------------+---------+
| target_path                  | action  |
+------------------------------+---------+
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
| /home/namruth/.test4.txt.swp | CREATED |
| /home/namruth/.test4.txt.swp | UPDATED |
| /home/namruth/.test4.txt.swp | UPDATED |
| /home/namruth/.test4.txt.swp | DELETED |
| /home/namruth/.test4.txt.swp | CREATED |
| /home/namruth/.test4.txt.swp | UPDATED |
| /home/namruth/.test4.txt.swp | UPDATED |
| /home/namruth/test4.txt      | CREATED |
| /home/namruth/test4.txt      | UPDATED |
| /home/namruth/test4.txt      | UPDATED |
| /home/namruth/.test4.txt.swp | DELETED |
| /tmp/#2753080                | UPDATED |
| /tmp/#2753078                | UPDATED |
| /tmp/#2753081                | UPDATED |
+------------------------------+---------+
```

PART 5: USING YARA FOR MALWARE ANALYSIS

Yara is a tool used for identifying malware samples. As the number of malware variants grew rapidly in the last few years, this tool can be used to write simple to complex boolean expressions that can be used identify malware families. Any yara file typically has three sections: meta - description of the rule, author etc, strings - strings that can be used to match the malware and condition - boolean expression using the strings and other keywords in yara.[6]

A sample example shown in yara documentation -



```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

P5.1

I uploaded the file on virus total to see its reputation and other properties -https://www.virustotal.com/gui/file/e6995b5428e887d790c6b77b32fddc143658ce2125ba192e8255d1ab70db6cac

I used the "strings" command to identify some of the useful strings in the file.These are:

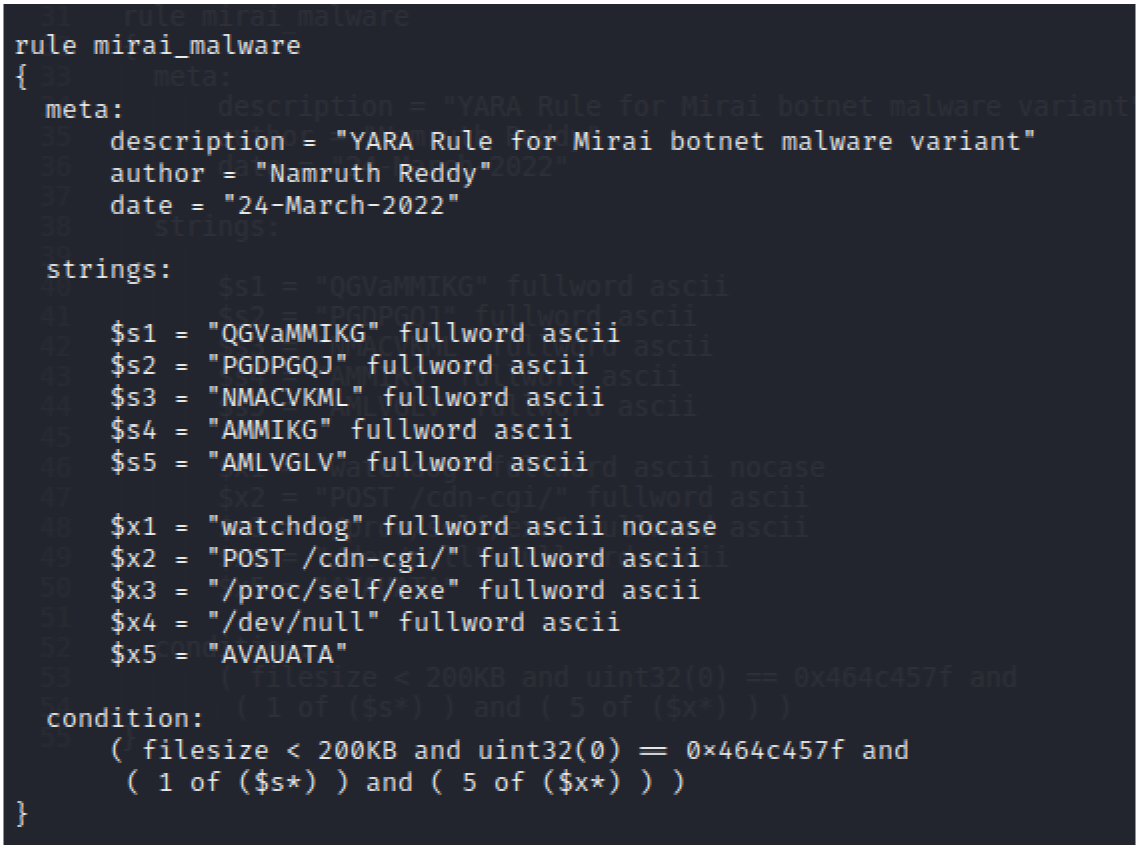
watchdog
Watchdog
WatchDog
/proc/self/exe
POST /cdn-cgi/
AVAUATA

QGVaMMIKG
PGDPGQJ
NMACVKML
AMMIKG
AMLVGLV
NGLEVJ
VPCLQDGP
GLAMFKLE

This file is mirai malware variant.
Some of its unique properties are:

Its file size is typically less than 200KB
It is an ELF executable with magic number 0x7f454c46, converting it to little endian format to be used in the rule below

It contains atleast one the strings listed in the second block above.
It contains watchdog string in various cases
It typically uses the path /proc/self/exe and the http request POST /cdn-cgi/



```
rule mirai_malware
{
  meta:
     description = "YARA Rule for Mirai botnet malware variant"
     author = "Namruth Reddy"
     date = "24-March-2022"

  strings:

     $s1 = "QGVaMMIKG" fullword ascii
     $s2 = "PGDPGQJ" fullword ascii
     $s3 = "NMACVKML" fullword ascii
     $s4 = "AMMIKG" fullword ascii
     $s5 = "AMLVGLV" fullword ascii

     $x1 = "watchdog" fullword ascii nocase
     $x2 = "POST /cdn-cgi/" fullword ascii
     $x3 = "/proc/self/exe" fullword ascii
     $x4 = "/dev/null" fullword ascii
     $x5 = "AVAUATA"

  condition:
     ( filesize < 200KB and uint32(0) == 0×464c457f and
      ( 1 of ($s*) ) and ( 5 of ($x*) ) )
}
```

P5.2

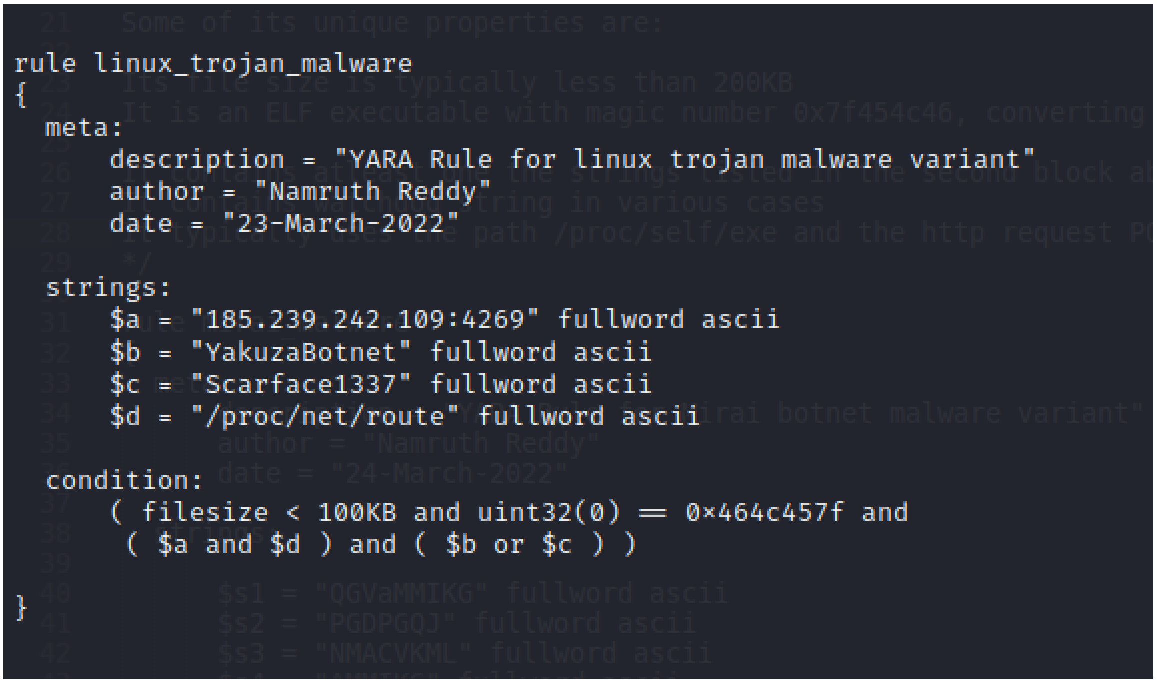
I uploaded the file on virus total to see its reputation and other properties - https://www.virustotal.com/gui/file/2923843a5ee9f6772b5a2a2c63bf606bd01fcb28bfeaede60a83b49e9a93266b/detection

I used the "strings" command to identify some of the useful strings in the file.These are:

185.239.242.109:4269
/proc/net/route
YakuzaBotnet
Scarface1337
Scarface1337Self Rep Fucking NeTiS and Thisity 0n Ur FuCkInG FoReHeAd We BiG L33T HaxErS
/proc/net/route

This file is a linux trojan variant malware.
It usually communicates to the IP 185.239.242.109:4269 and accesses files in the location /proc/net/route
It also contains useful words like Scarface1337 and YakuzaBotnet

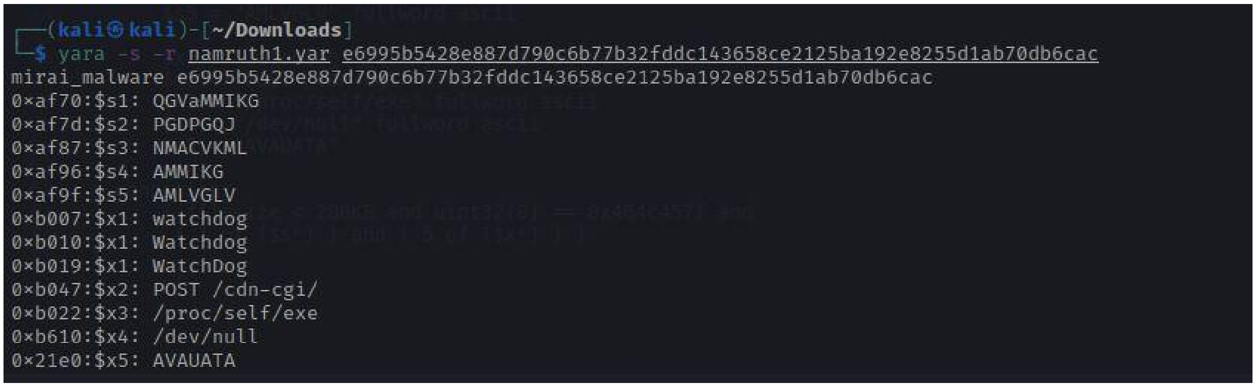
File size of such malware is typicall < 100KB
It is an ELF executable with magic number 0x7f454c46, converting it to little endian format to be used in the rule below



```
rule linux_trojan_malware
{
  meta:
     description = "YARA Rule for linux trojan malware variant"
     author = "Namruth Reddy"
     date = "23-March-2022"

  strings:
     $a = "185.239.242.109:4269" fullword ascii
     $b = "YakuzaBotnet" fullword ascii
     $c = "Scarface1337" fullword ascii
     $d = "/proc/net/route" fullword ascii

  condition:
     ( filesize < 100KB and uint32(0) == 0x464c457f and
      ( $a and $d ) and ( $b or $c ) )

}
```

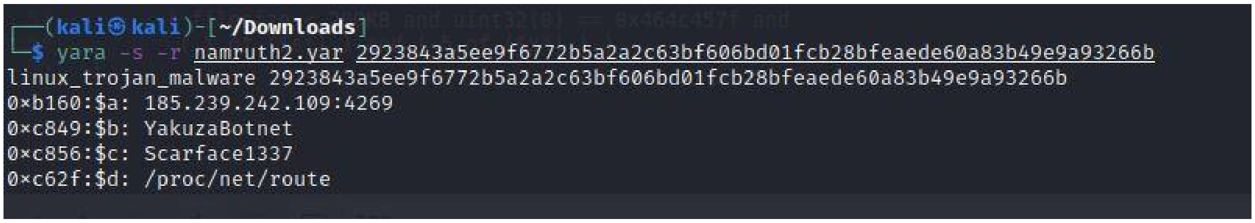
After writing the yara rules for both the files, we execute yara to see if they are being identified correctly. Output of both the files are shown below:

P5.3



```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara -s -r namruth1.yar e6995b5428e887d790c6b77b32fddc143658ce2125ba192e8255d1ab70db6cac
mirai_malware e6995b5428e887d790c6b77b32fddc143658ce2125ba192e8255d1ab70db6cac
0×af70:$s1: QGVaMMIKG
0×af7d:$s2: PGDPGQJ
0×af87:$s3: NMACVKML
0×af96:$s4: AMMIKG
0×af9f:$s5: AMLVGLV
0×b007:$x1: watchdog
0×b010:$x1: Watchdog
0×b019:$x1: WatchDog
0×b047:$x2: POST /cdn-cgi/
0×b022:$x3: /proc/self/exe
0×b610:$x4: /dev/null
0×21e0:$x5: AVAUATA
```

P5.4



```
┌──(kali㉿kali)-[~/Downloads]
└─$ yara -s -r namruth2.yar 2923843a5ee9f6772b5a2a2c63bf606bd01fcb28bfeaede60a83b49e9a93266b
linux_trojan_malware 2923843a5ee9f6772b5a2a2c63bf606bd01fcb28bfeaede60a83b49e9a93266b
0×b160:$a: 185.239.242.109:4269
0×c849:$b: YakuzaBotnet
0×c856:$c: Scarface1337
0×c62f:$d: /proc/net/route
```

PART 6: USING OSQUERY AND YARA TO IDENTIFY MALWARE SAMPLES

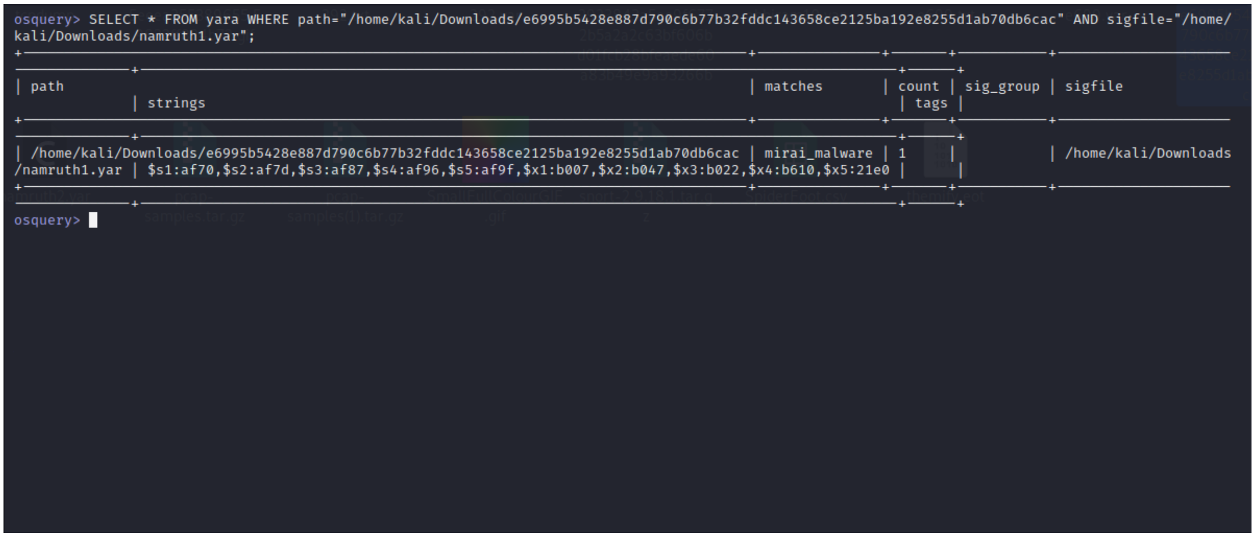
Osquery can be integrated with yara to check for file integrity event changes. There are two types of yara tables: [7]

1. Yara_events - this table can be used for auto yara detection when a specific file integrity event is triggered.
2. Yara - this is an on demand scan of a specific file.

Using the yara rules and malware files given in the assignment, yara on demand scan is executed and the values are populated in the yara table as shown below:

P6.1

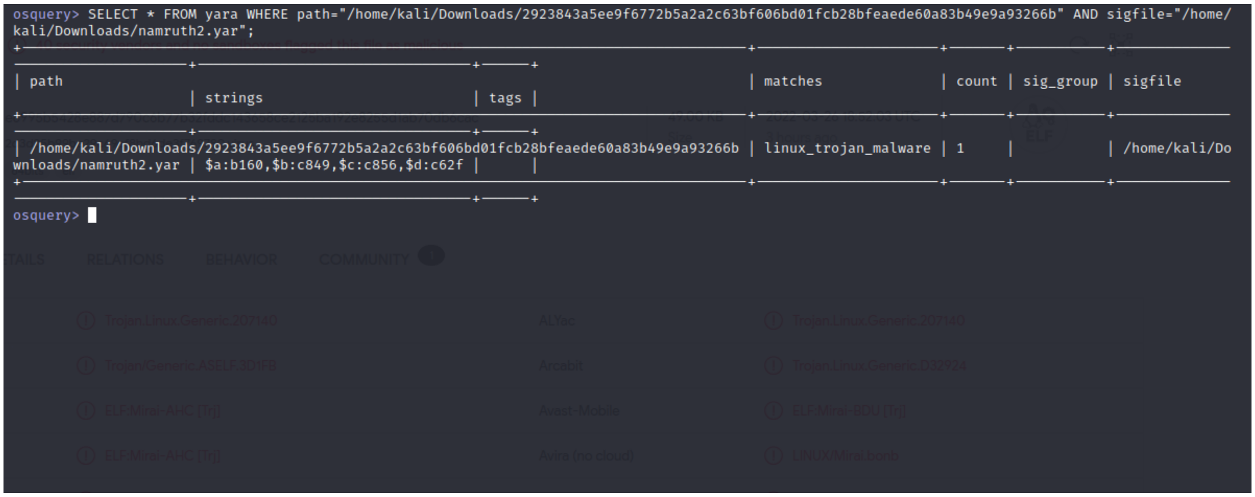
SELECT * FROM yara WHERE path="/home/kali/Downloads/e6995b5428e887d790c6b77b32fddc143658ce2125ba192e8255d1ab70db6cac" AND sigfile="/home/kali/Downloads/namruth1.yar";



```
osquery> SELECT * FROM yara WHERE path="/home/kali/Downloads/e6995b5428e887d790c6b77b32fddc143658ce2125ba192e8255d1ab70db6cac" AND sigfile="/home/
kali/Downloads/namruth1.yar";
+-----------------------------------------------------------------------------------+---------------+-------+-----------+---------------------
--------------+-------------------------------------------------------------------------------------------------------+-------+
| path                                                                              | matches       | count | sig_group | sigfile
              | strings                                                                                               | tags |
+-----------------------------------------------------------------------------------+---------------+-------+-----------+---------------------
--------------+-------------------------------------------------------------------------------------------------------+-------+
| /home/kali/Downloads/e6995b5428e887d790c6b77b32fddc143658ce2125ba192e8255d1ab70db6cac | mirai_malware | 1     |           | /home/kali/Downloads
/namruth1.yar | $s1:af70,$s2:af7d,$s3:af87,$s4:af96,$s5:af9f,$x1:b007,$x2:b047,$x3:b022,$x4:b610,$x5:21e0 |      |
+-----------------------------------------------------------------------------------+---------------+-------+-----------+---------------------
--------------+-------------------------------------------------------------------------------------------------------+-------+
osquery> 
```

P6.2

SELECT * FROM yara WHERE path="/home/kali/Downloads/2923843a5ee9f6772b5a2a2c63bf606bd01fcb28bfeaede60a83b49e9a93266b" AND sigfile="/home/kali/Downloads/namruth2.yar";



```
osquery> SELECT * FROM yara WHERE path="/home/kali/Downloads/2923843a5ee9f6772b5a2a2c63bf606bd01fcb28bfeaede60a83b49e9a93266b" AND sigfile="/home/
kali/Downloads/namruth2.yar";
+--------------------------------------------------------------------------------------+----------------------+-------+-----------+-------------
----------------------+--------------------------------------+-------+
| path                                                                                 | matches              | count | sig_group | sigfile
                      | strings                              | tags  |
+--------------------------------------------------------------------------------------+----------------------+-------+-----------+-------------
----------------------+--------------------------------------+-------+
| /home/kali/Downloads/2923843a5ee9f6772b5a2a2c63bf606bd01fcb28bfeaede60a83b49e9a93266b | linux_trojan_malware | 1     |           | /home/kali/Do
wnloads/namruth2.yar | $a:b160,$b:c849,$c:c856,$d:c62f |       |
+--------------------------------------------------------------------------------------+----------------------+-------+-----------+-------------
----------------------+--------------------------------------+-------+
osquery> █
```

References:

[1] - https://osquery.readthedocs.io/en/stable/
[2] - https://www.digitalocean.com/community/tutorials/how-to-monitor-your-system-security-with-osquery-on-ubuntu-16-04
[3] - https://osquery.readthedocs.io/en/stable/deployment/syslog/
[4] - https://osquery.readthedocs.io/en/stable/deployment/configuration/
[5] - https://osquery.readthedocs.io/en/stable/deployment/file-integrity-monitoring/
[6] - https://yara.readthedocs.io/en/stable/
[7] - https://osquery.readthedocs.io/en/stable/deployment/yara/