PRATICAL 1

QUESTION 1

-how can you identify abnormal login attempts on a network using log data?

ANSWER

To identify abnormal login attempts on a network;

<1>--Ensure all the log data are centralized in a log management system. Examples of log management system include splunk, SIEM(Security information and event management), ELK stack. With the help of the SIEM collector which parses log files into a standard format and can be recorded by the SIEM and translated for event correlation while the SIEM sensor collects data from the network media

<2>--A baseline must be set so as to identify abnormal login attempts on the network.The baseline simply shows what the normal behavior of the network and anything outside the network baselines is considered abnormal.

<3>--Check log data for **IoC (Indicator of compromise)--** Indicator of compromise includes logins from different geographical locations within a short period of time which indicates stolen credentials, looking out for multiple failed login attempts which is a sign of brute force attack or an IP address is trying to login into multiple accounts.

<4>--Real time monitoring and alerts is important for monitoring of abnormal login attempts.

QUESTION 2

Collect logs from a Windows/Linux server using free tools like OSQuery or Sysmon. Import the logs into a SIEM tool like Splunk (Free version) or ELK Stack. Write a query to detect abnormal login attempts (e.g., multiple failed login attempts in a short period).

SOLUTION

I installed osquery on my linux

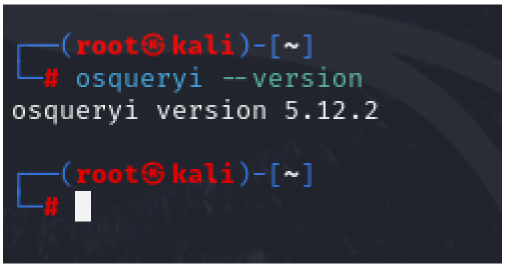
I used the following command to install osquery on my linux

sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 1484120AC4E9F8A1A577AEEE97A80C63C9D8B80B

sudo add-apt-repository 'deb [arch=amd64] https://pkg.osquery.io/deb deb main'

sudo apt-get update
sudo apt-get install osquery

Then i checked which version of osquery I installed



```
┌──(root㉿kali)-[~]
└─# osqueryi --version
osqueryi version 5.12.2

┌──(root㉿kali)-[~]
└─# 
```

I also installed SPLUNK on my linux using this command

<1> --- sudo wget -O splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz"

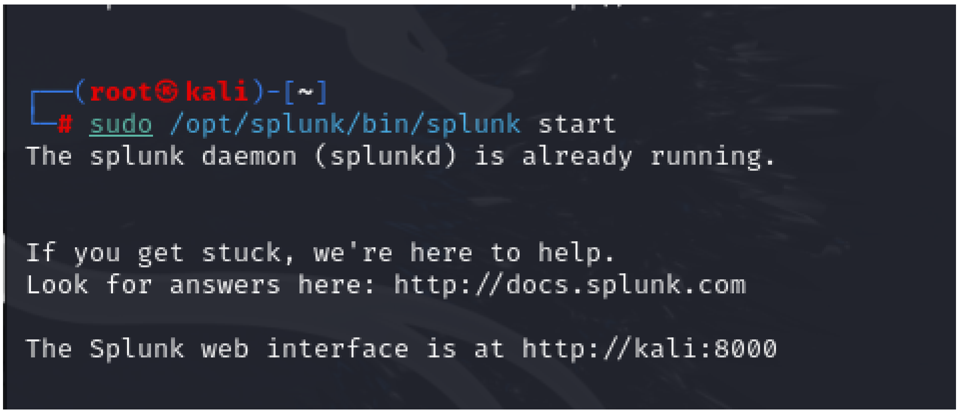
<2>-- sudo tar -xvzf splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz -C /opt

<3>-- sudo /opt/splunk/bin/splunk start --accept-license

After inputting this command, i was instructed to create a username and password. After creating a username and password, i did complete the command with

<4>-- sudo /opt/splunk/bin/splunk enable boot-start

---After this, it gave me a link to go to so i can access **splunk**

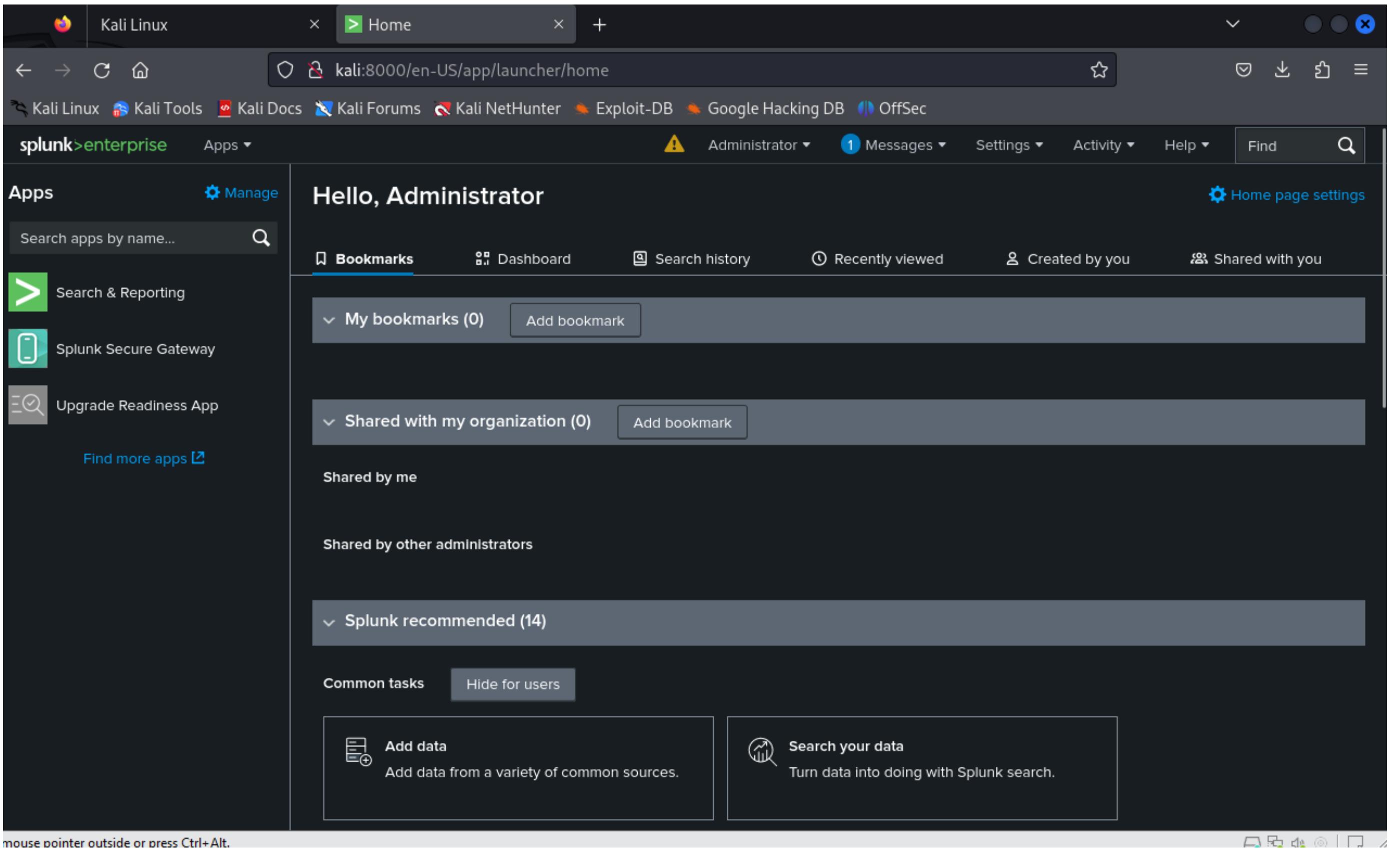


```
┌──(root㉿kali)-[~]
└─# sudo /opt/splunk/bin/splunk start
The splunk daemon (splunkd) is already running.


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kali:8000
```

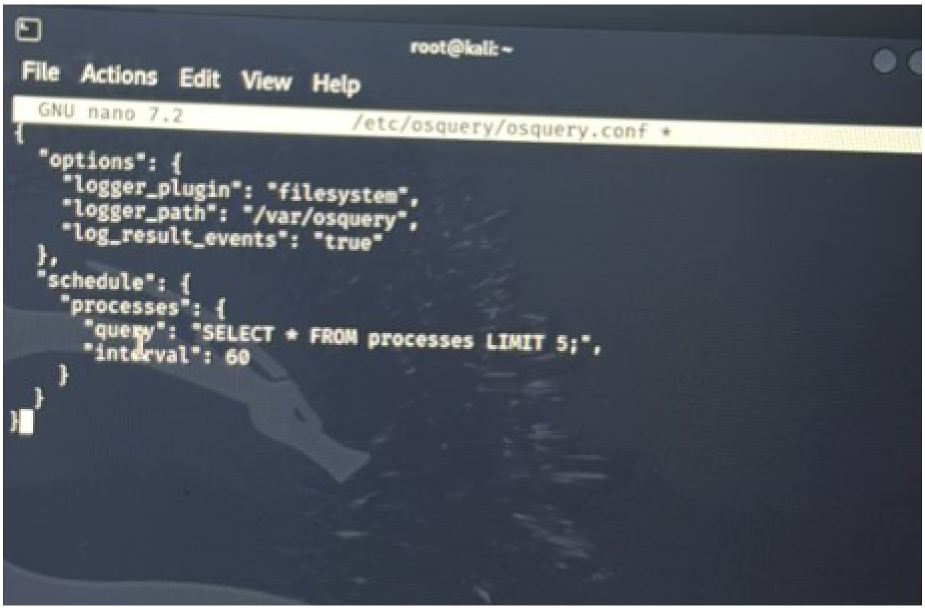
After visiting the webpage, I signed in using the details i created after inputting the 3rd command on installing **splunk**



I created a file using the command

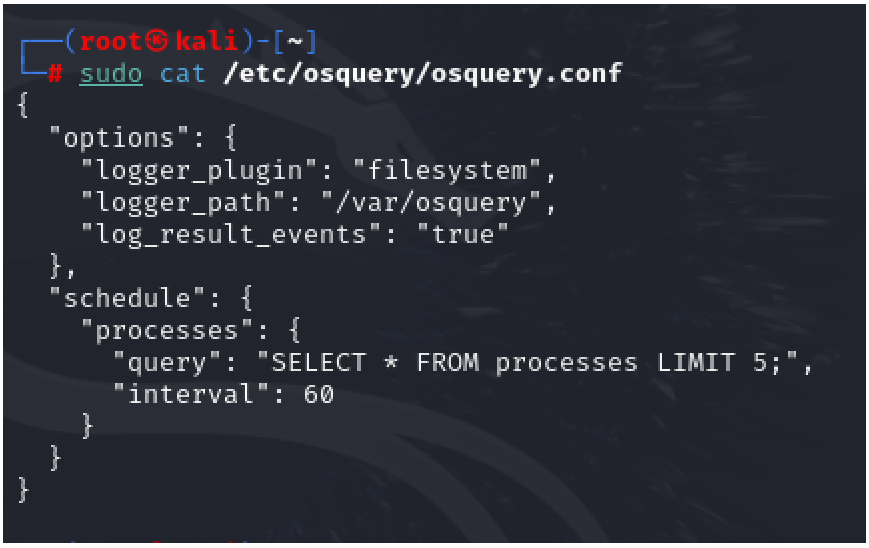
sudo nano /etc/osquery/osquery.conf

then i created a script inside of the file and saved it



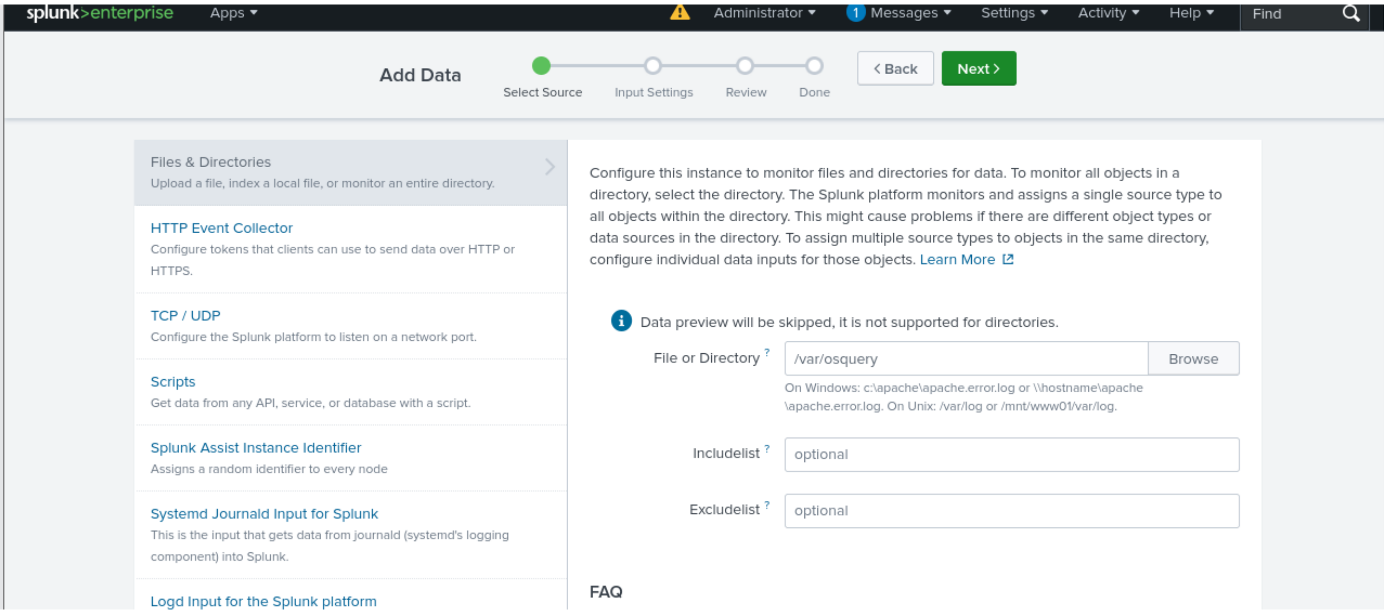
```
  GNU nano 7.2                 /etc/osquery/osquery.conf *
{
  "options": {
    "logger_plugin": "filesystem",
    "logger_path": "/var/osquery",
    "log_result_events": "true"
  },
  "schedule": {
    "processes": {
      "query": "SELECT * FROM processes LIMIT 5;",
      "interval": 60
    }
  }
}
```

FILE SAVED and i displayed the file using the **CAT** command



```
┌──(root㉿kali)-[~]
└─# sudo cat /etc/osquery/osquery.conf
{
  "options": {
    "logger_plugin": "filesystem",
    "logger_path": "/var/osquery",
    "log_result_events": "true"
  },
  "schedule": {
    "processes": {
      "query": "SELECT * FROM processes LIMIT 5;",
      "interval": 60
    }
  }
}
```

I then opened my **splunk,** visited settings--data inputs -- files and directory and browsed for **/var/osquery/** and selected all



Add Data

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Logd Input for the Splunk platform

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

Data preview will be skipped, it is not supported for directories.

File or Directory ? /var/osquery

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Includelist ? optional

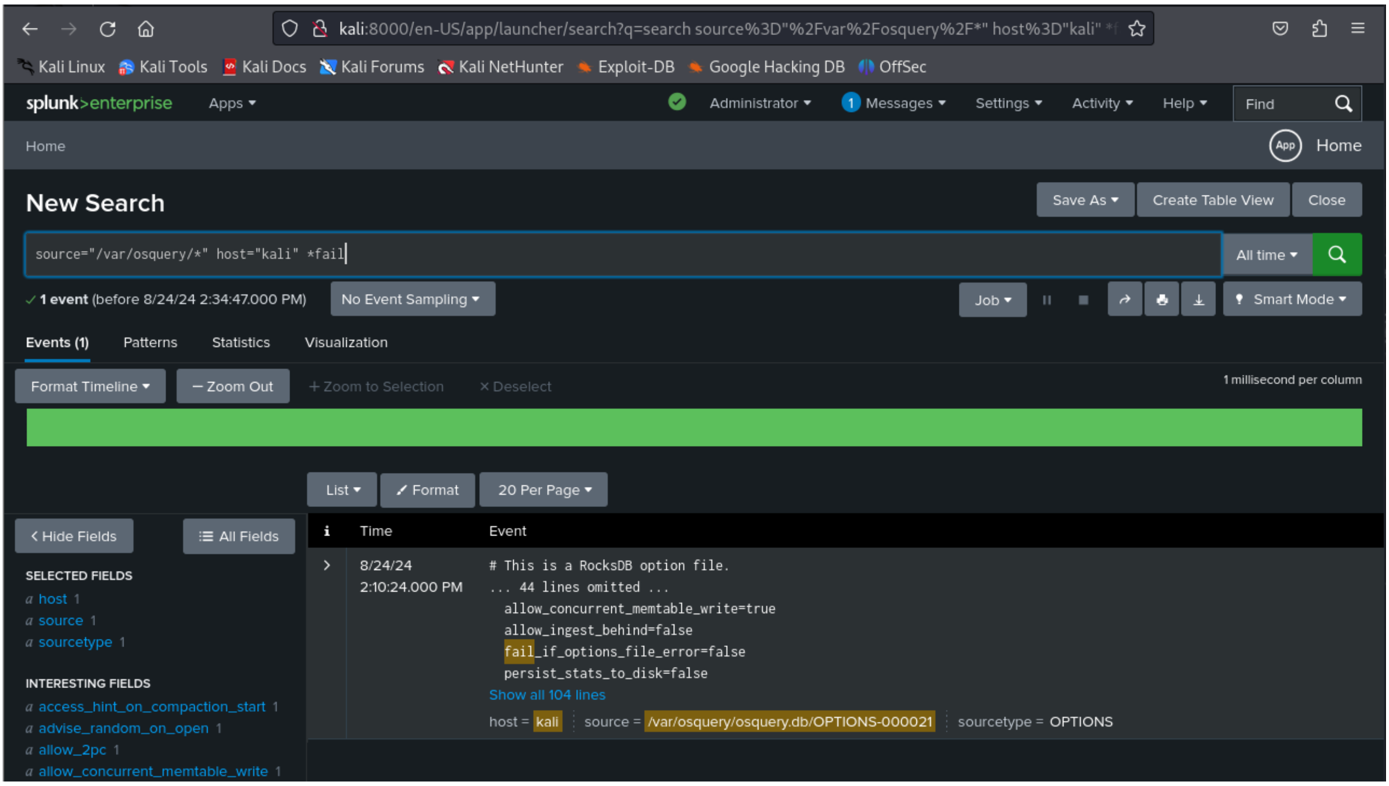
Excludelist ? optional

FAQ

I added the data and searched

I searched the splunk and used the filter

source="/var/osquery/*" host="kali" *fail



```
source="/var/osquery/*" host="kali" *fail
```

✓ **1 event** (before 8/24/24 2:34:47.000 PM)

8/24/24 2:10:24.000 PM

```
# This is a RocksDB option file.
... 44 lines omitted ...
  allow_concurrent_memtable_write=true
  allow_ingest_behind=false
  fail_if_options_file_error=false
  persist_stats_to_disk=false
```

Show all 104 lines

host = kali | source = /var/osquery/osquery.db/OPTIONS-000021 | sourcetype = OPTIONS

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a access_hint_on_compaction_start 1
- a advise_random_on_open 1
- a allow_2pc 1
- a allow_concurrent_memtable_write 1