ICS 344 Information Security

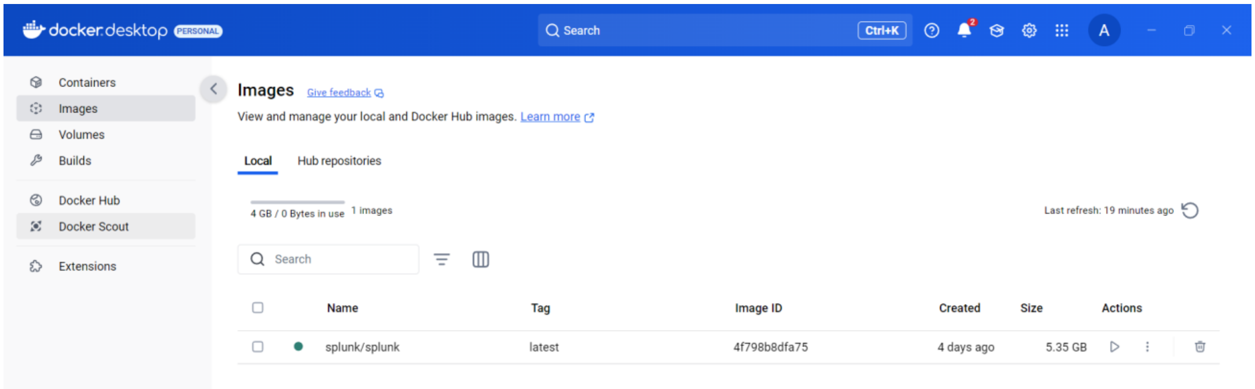
Project Phase 2

Abdulmalik Almaidani – 202031320

Khalid Alshahrani – 202012200

Mohammed Alghanim – 202158990

1. First, we successfully installed Splunk on Docker Desktop:



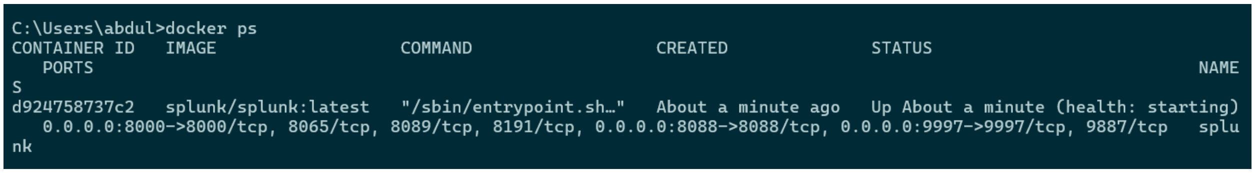
View and manage your local and Docker Hub images. Learn more

4 GB / 0 Bytes in use 1 images

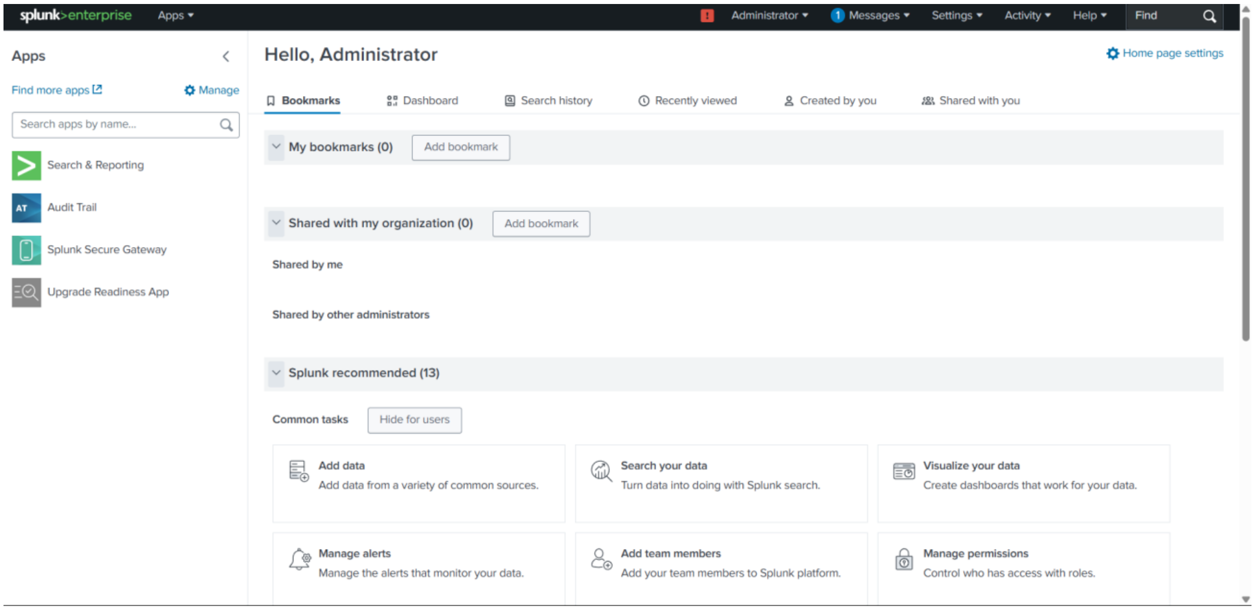
Last refresh: 19 minutes ago

□		Name	Tag	Image ID	Created	Size	Actions
□	●	splunk/splunk	latest	4f798b8dfa75	4 days ago	5.35 GB	

2. We run an appropriate code to run the Splunk UI:



```
C:\Users\abdul>docker ps
CONTAINER ID   IMAGE                   COMMAND                  CREATED              STATUS                                      NAME
    PORTS
S
d924758737c2   splunk/splunk:latest    "/sbin/entrypoint.sh…"   About a minute ago   Up About a minute (health: starting)
    0.0.0.0:8000->8000/tcp, 8065/tcp, 8089/tcp, 8191/tcp, 0.0.0.0:8088->8088/tcp, 0.0.0.0:9997->9997/tcp, 9887/tcp   splu
nk
```



Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

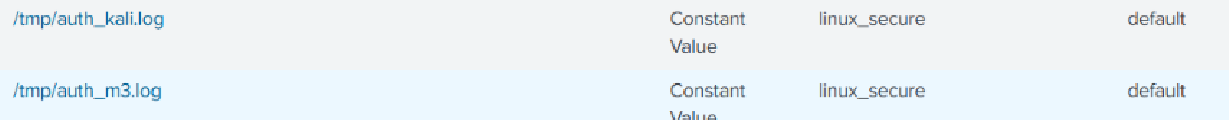
Visualize your data
Create dashboards that work for your data.

Manage alerts
Manage the alerts that monitor your data.

Add team members
Add your team members to Splunk platform.

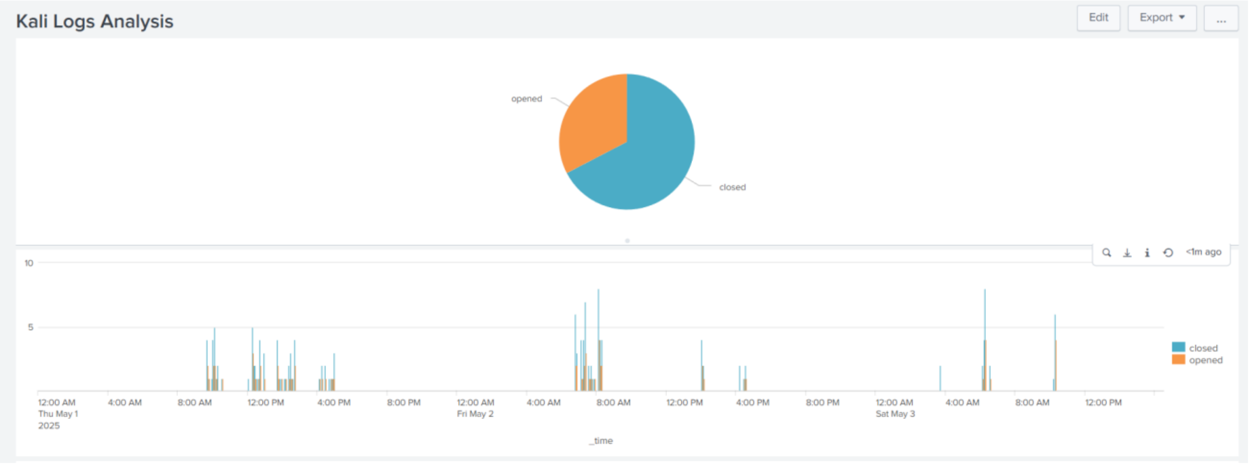
Manage permissions
Control who has access with roles.

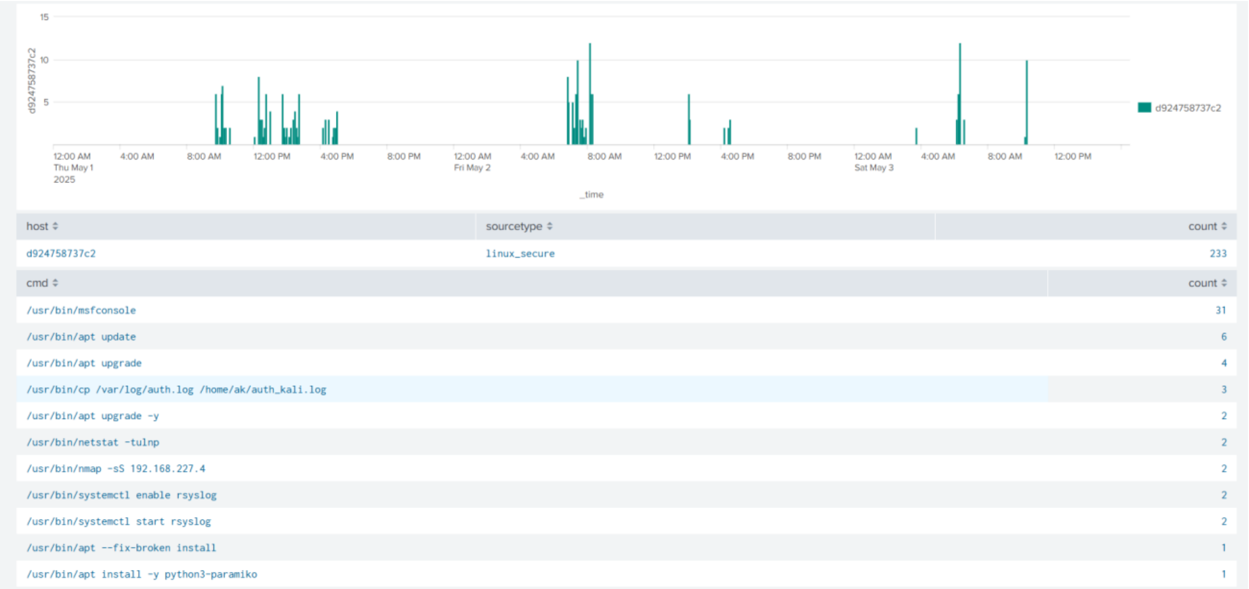
3. Integrate logs from the victim environment & the attacker environment into the SIEM platform:



/tmp/auth_kali.log	Constant Value	linux_secure	default
/tmp/auth_m3.log	Constant Value	linux_secure	default

4. Kali logs analysis:

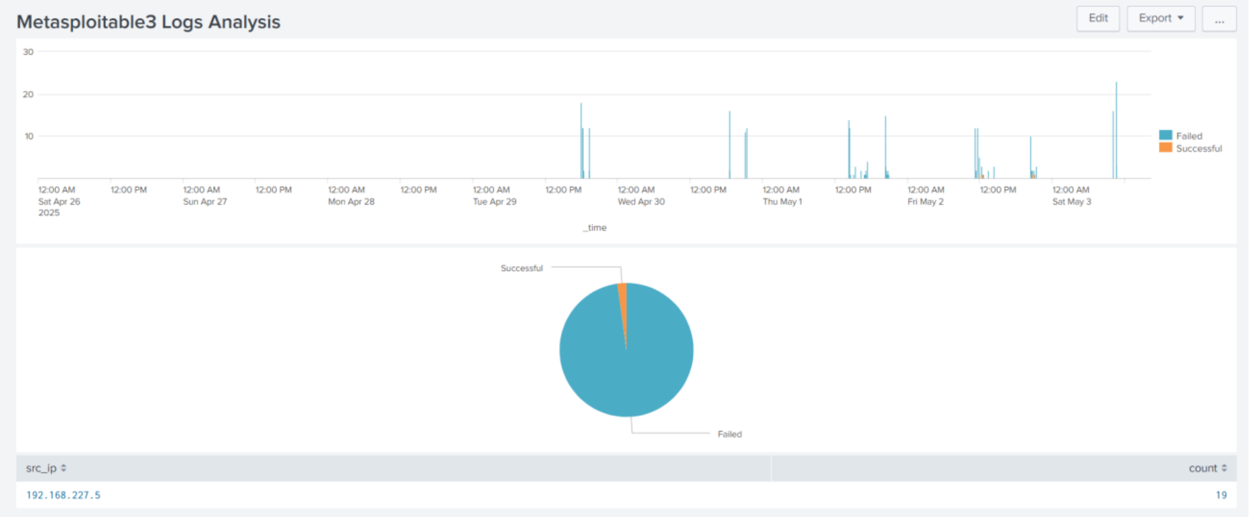




host ⇕	sourcetype ⇕	count ⇕
d924758737c2	linux_secure	233

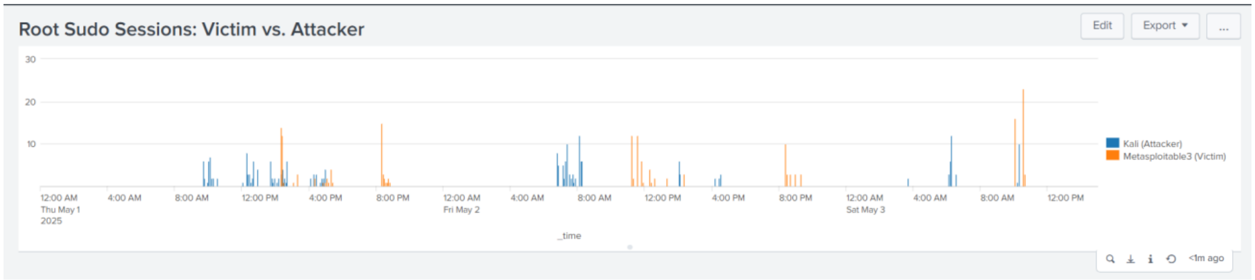
cmd ⇕	count ⇕
/usr/bin/msfconsole	31
/usr/bin/apt update	6
/usr/bin/apt upgrade	4
/usr/bin/cp /var/log/auth.log /home/ak/auth_kali.log	3
/usr/bin/apt upgrade -y	2
/usr/bin/netstat -tulnp	2
/usr/bin/nmap -sS 192.168.227.4	2
/usr/bin/systemctl enable rsyslog	2
/usr/bin/systemctl start rsyslog	2
/usr/bin/apt --fix-broken install	1
/usr/bin/apt install -y python3-paramiko	1

5. Metasploitable3 logs analysis:



src_ip ⇕	count ⇕
192.168.227.5	19

6. Compressions:


Root Sudo Sessions: Victim vs. Attacker
Edit
Export ▾
...
30
20
10
12:00 AM
Thu May 1
2025
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Fri May 2
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Sat May 3
4:00 AM
8:00 AM
12:00 PM
_time
Kali (Attacker)
Metasploitable3 (Victim)
<1m ago