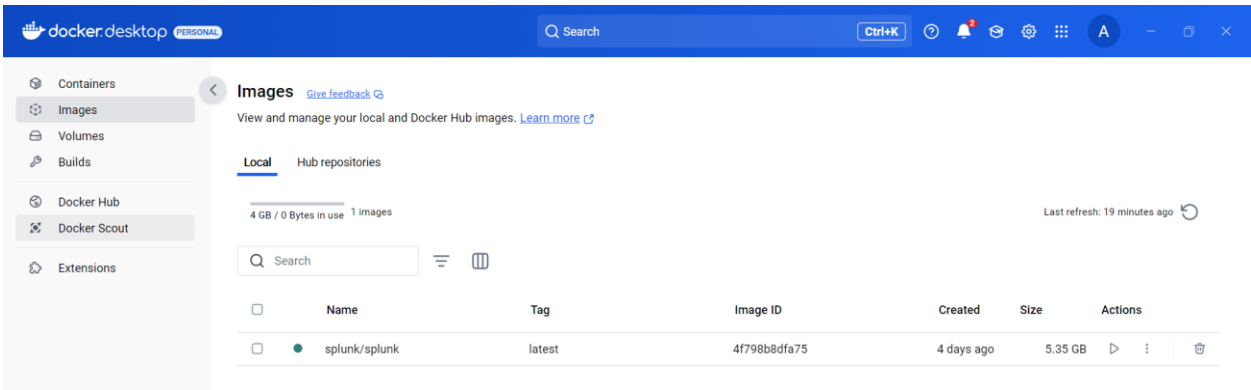# ICS 344 Information Security

Project Phase 2

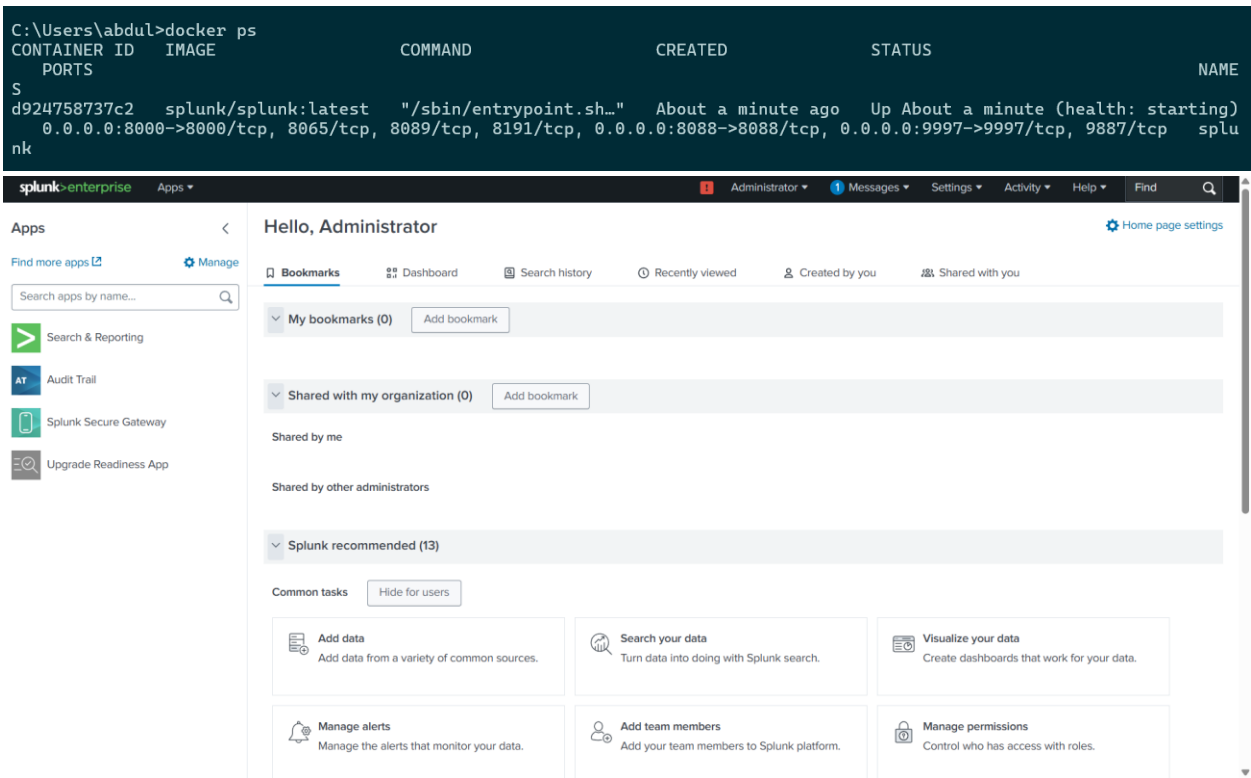Abdulmalik Almaidani – 202031320

Khalid Alshahrani – 202012200

Mohammed Alghanim – 202158990

Task 1.1: Use Kali Linux tool Metasploit to compromise the service.

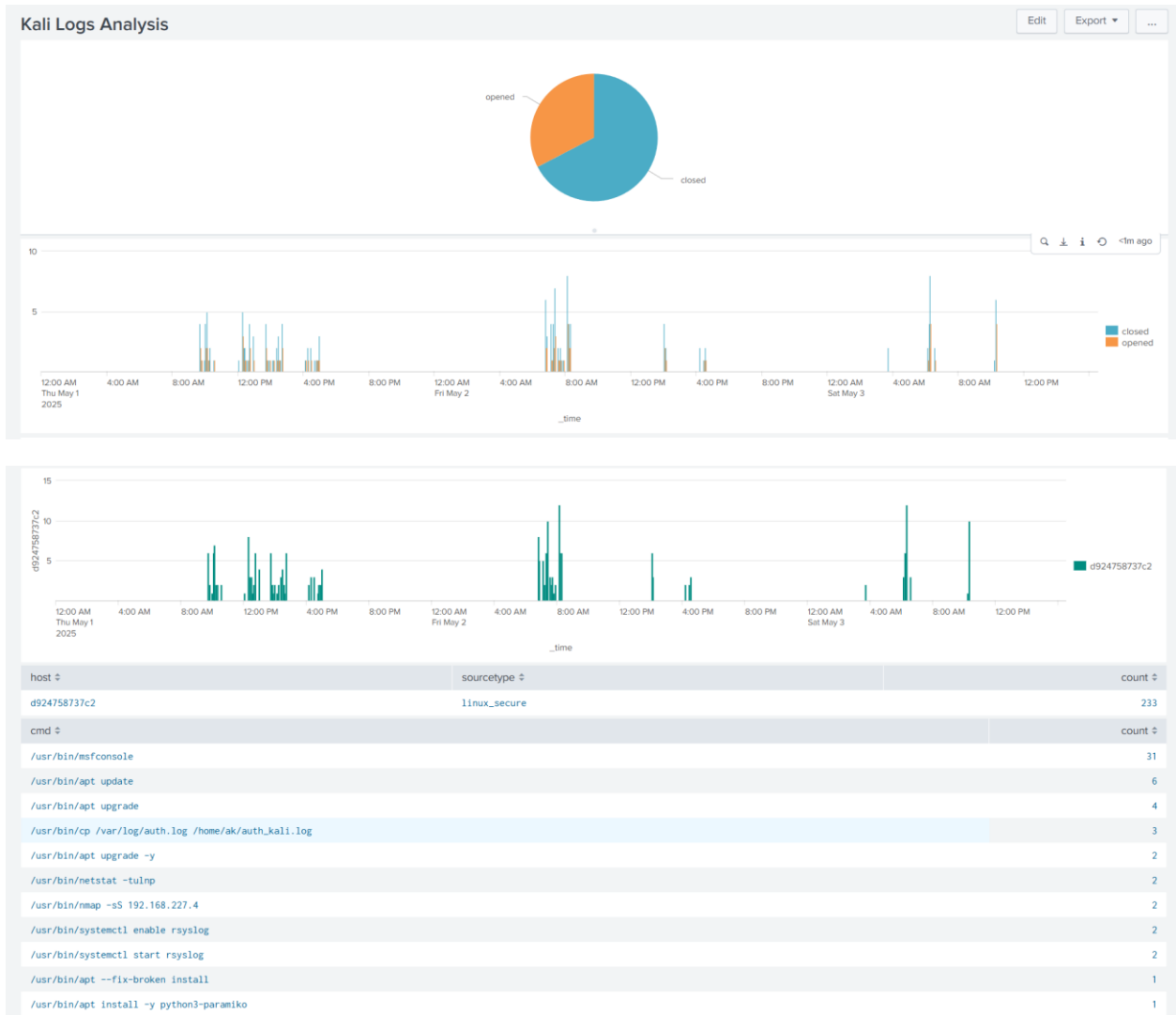1. First, we successfully installed Splunk on Docker Desktop:

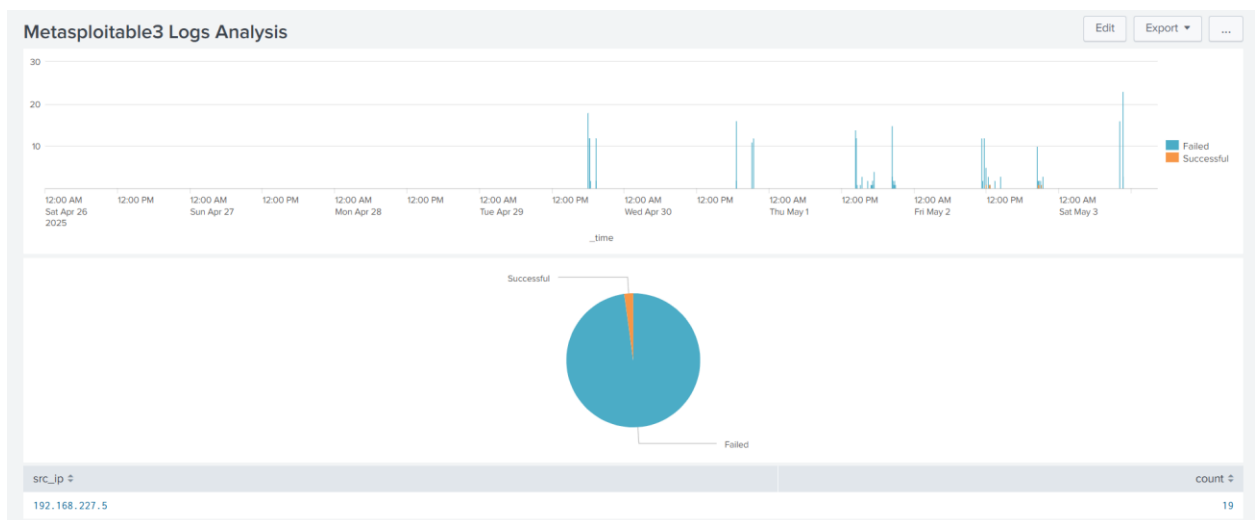2. We run an appropriate code to run the Splunk UI:

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

4. Kali logs analysis:

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:

Metasploitable3 Logs Analysis

src_ip ⇕	count ⇕
192.168.227.5	19

6. Compressions: