POC TASK 6

Log Analysis and Intrusion Detection:

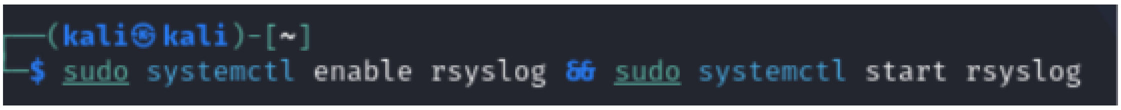
Objective

- Enable and configure system logging (rsyslog) to collect logs.
- Analyze logs for suspicious activities such as failed SSH logins.
- Deploy an Intrusion Detection System (IDS) for real-time threat detection.

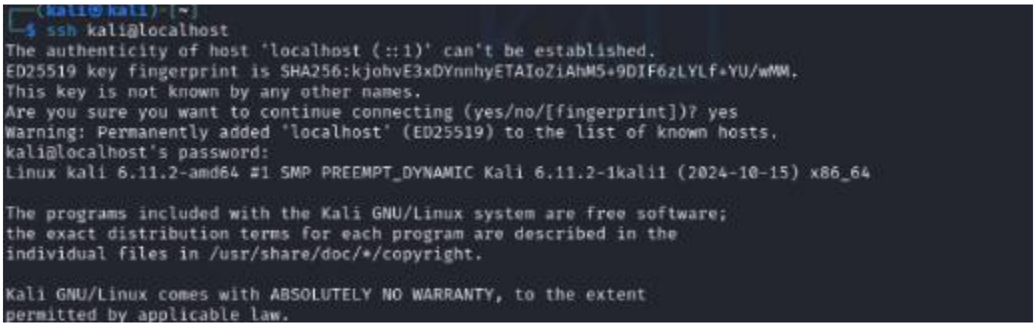
Tools Used:

- rsyslog (System Logging)
- journalctl (System Log Viewer)
- grep (Log Filtering)
- Snort (Intrusion Detection System)

rsryslog:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable rsyslog && sudo systemctl start rsyslog
```

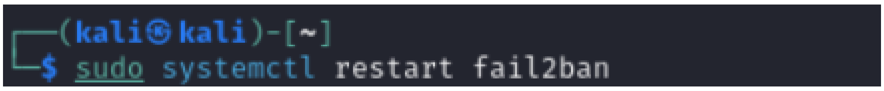


```
┌──(kali㉿kali)-[~]
└─$ ssh kali@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:kjohvE3xDYnnhyETAIoZiAhM5+9DIF6zLYLf+YU/wMM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
kali@localhost's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

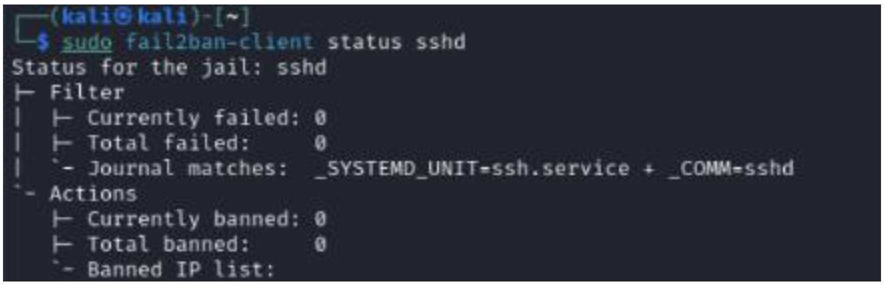
Mitigration:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban
```

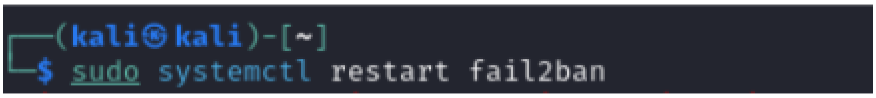
The fail2ban is configured to Block ip address.

Implementing fail2ban:



```
┌──(kali㉿kali)-[~]
└─$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=ssh.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

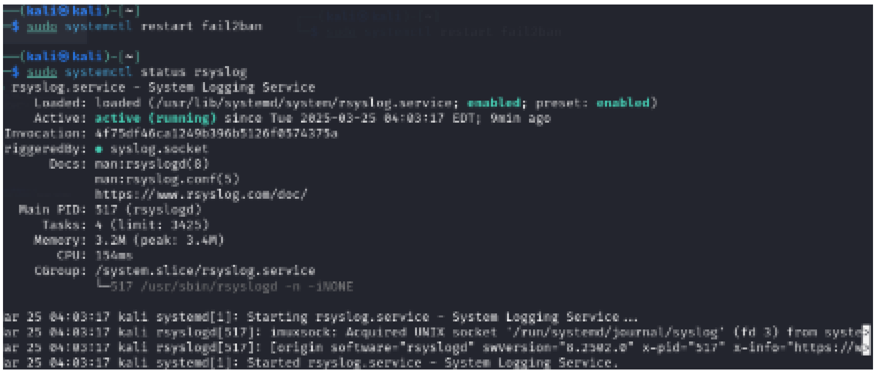
Restarting fail2ban:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban
```

- We are restarting fail2ban To apply new configuration
- The command is “sudo systemctl restart fail2ban”.

Set up Log monitoring Automation:



```
──(kali㉿kali)-[~]
─$ sudo systemctl restart fail2ban

──(kali㉿kali)-[~]
─$ sudo systemctl status rsyslog
 rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-03-25 04:03:17 EDT; 9min ago
Invocation: 4f75df46ca1249b396b5126f0574375a
riggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 517 (rsyslogd)
      Tasks: 4 (limit: 3425)
     Memory: 3.2M (peak: 3.4M)
        CPU: 154ms
     CGroup: /system.slice/rsyslog.service
             └─517 /usr/sbin/rsyslogd -n -iNONE

ar 25 04:03:17 kali systemd[1]: Starting rsyslog.service - System Logging Service...
ar 25 04:03:17 kali rsyslogd[517]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from syste
ar 25 04:03:17 kali rsyslogd[517]: [origin software="rsyslogd" swVersion="8.2502.0" x-pid="517" x-info="https://w
ar 25 04:03:17 kali systemd[1]: Started rsyslog.service - System Logging Service.
```

Logwatch send reports for the user through email.