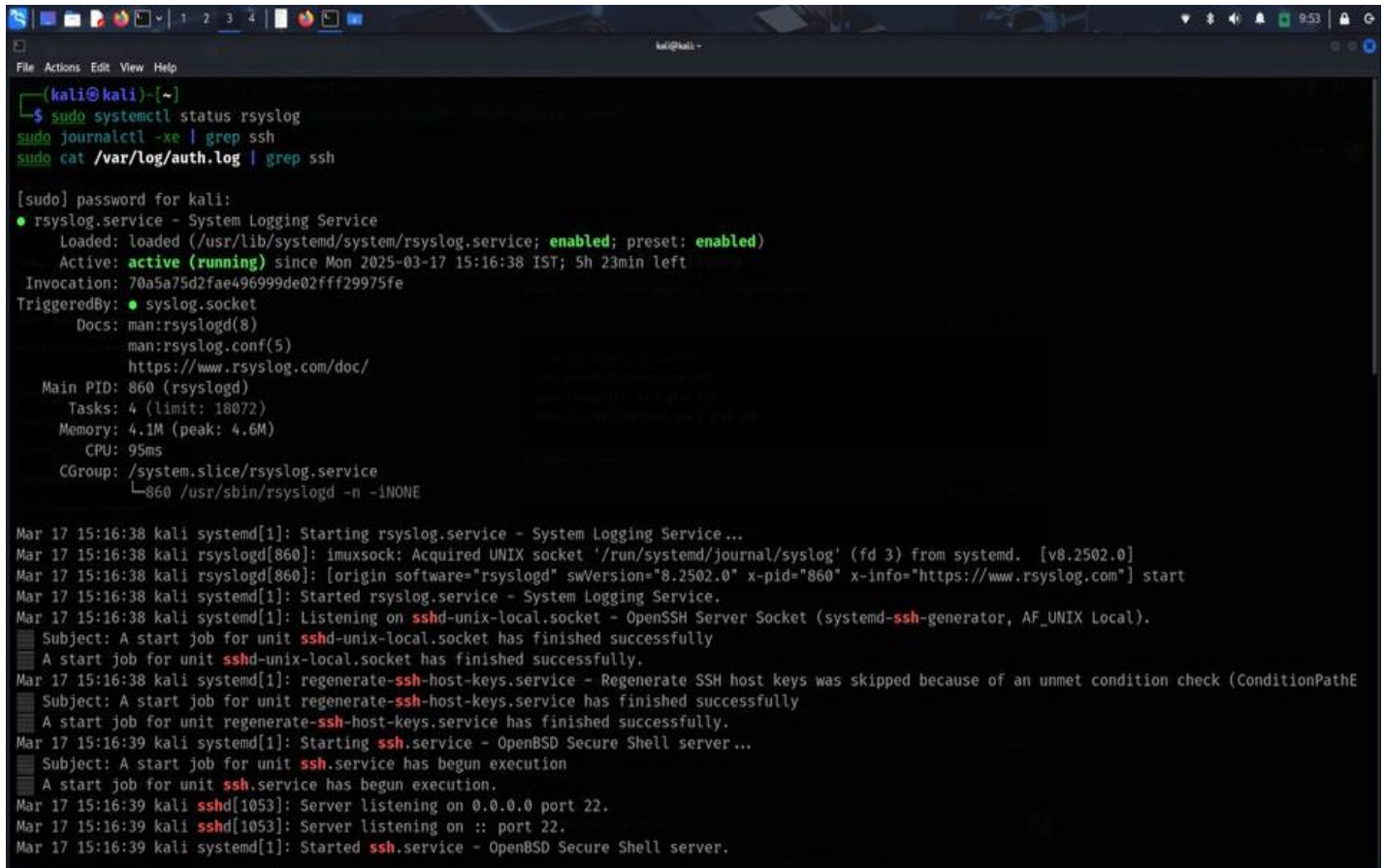


POC TASK 6

- **Setup: Enable System Logging:**

Ensure system logging is active and capturing SSH events.

- **Verify logging is enabled:**



```
(kali@kali)-[~]
└─$ sudo systemctl status rsyslog
sudo journalctl -xe | grep ssh
sudo cat /var/log/auth.log | grep ssh

[sudo] password for kali:
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-03-17 15:16:38 IST; 5h 23min left
   Invocation: 70a5a75d2fae496999de02fff29975fe
   TriggeredBy: ● syslog.socket
   Docs: man:rsyslogd(8)
         man:rsyslog.conf(5)
         https://www.rsyslog.com/doc/
   Main PID: 860 (rsyslogd)
   Tasks: 4 (limit: 18072)
   Memory: 4.1M (peak: 4.6M)
   CPU: 95ms
   CGroup: /system.slice/rsyslog.service
           └─860 /usr/sbin/rsyslogd -n -lNONE

Mar 17 15:16:38 kali systemd[1]: Starting rsyslog.service - System Logging Service...
Mar 17 15:16:38 kali rsyslogd[860]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2502.0]
Mar 17 15:16:38 kali rsyslogd[860]: [origin software="rsyslogd" swVersion="8.2502.0" x-pid="860" x-info="https://www.rsyslog.com"] start
Mar 17 15:16:38 kali systemd[1]: Started rsyslog.service - System Logging Service.
Mar 17 15:16:38 kali systemd[1]: Listening on sshd-unix-local.socket - OpenSSH Server Socket (systemd-ssh-generator, AF_UNIX Local).
■ Subject: A start job for unit sshd-unix-local.socket has finished successfully
■ A start job for unit sshd-unix-local.socket has finished successfully.
Mar 17 15:16:38 kali systemd[1]: regenerate-ssh-host-keys.service - Regenerate SSH host keys was skipped because of an unmet condition check (ConditionPathE
■ Subject: A start job for unit regenerate-ssh-host-keys.service has finished successfully
■ A start job for unit regenerate-ssh-host-keys.service has finished successfully.
Mar 17 15:16:39 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
■ Subject: A start job for unit ssh.service has begun execution
■ A start job for unit ssh.service has begun execution.
Mar 17 15:16:39 kali sshd[1053]: Server listening on 0.0.0.0 port 22.
Mar 17 15:16:39 kali sshd[1053]: Server listening on :: port 22.
Mar 17 15:16:39 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

sudo systemctl status rsyslog sudo

journalctl -xe | grep ssh

sudo cat /var/log/auth.log | grep ssh

- **If logging is not enabled** Enable and restart rsyslog if needed;

sudo systemctl enable rsyslog

sudo systemctl restart rsyslog

- **Simulate Multiple Failed SSH Login Attempts**

Run a brute-force simulation to generate logs and Attempt SSH login with incorrect credentials

ssh user@localhost

Enter incorrect passwords multiple times **Alternatively,**

simulate automated attacks with Hydra: hydra -l root -P

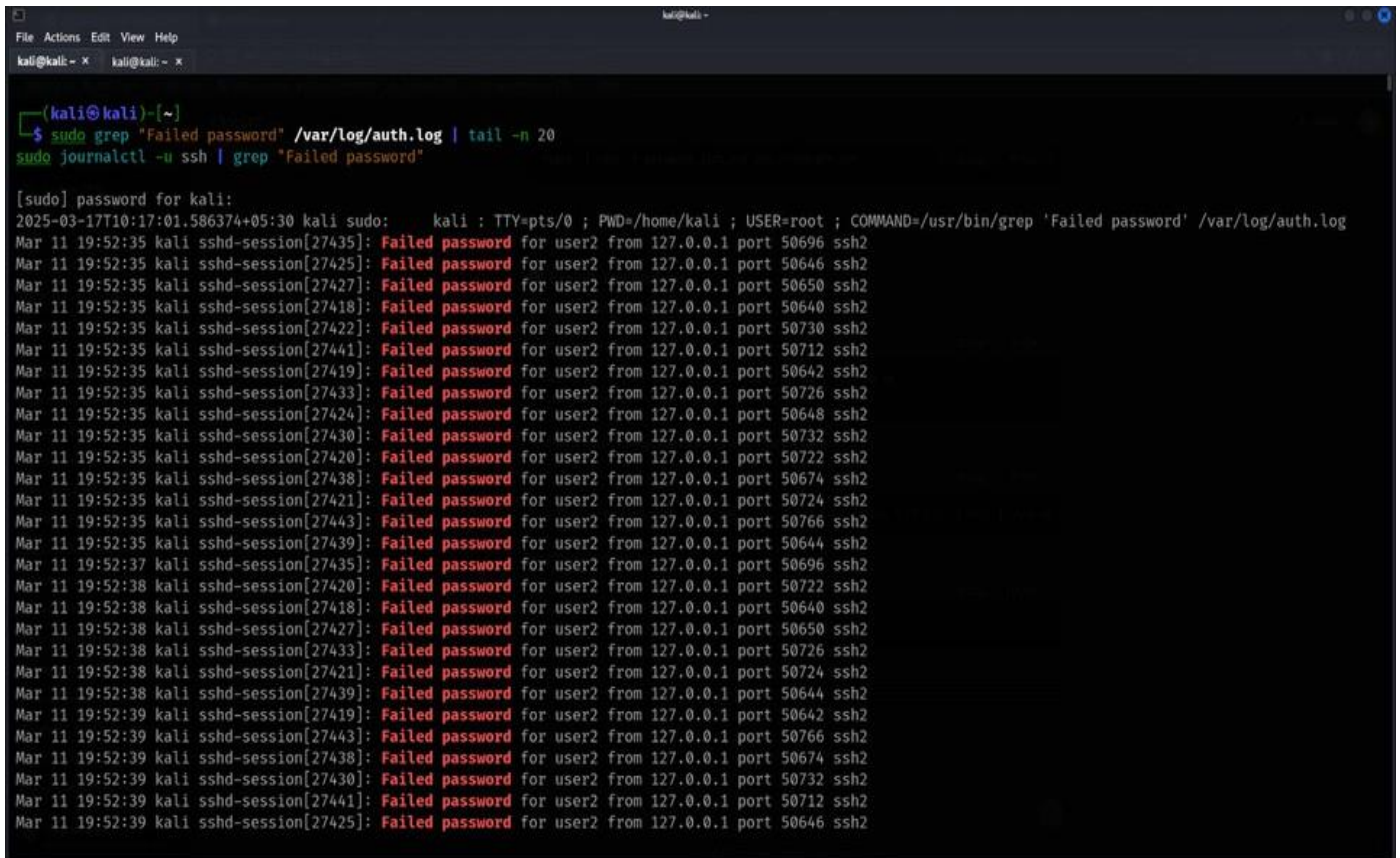
password_list.txt ssh://<target-ip>

- **Exploit: Log Analysis**

Extract failed login attempts using grep.

sudo grep "Failed password" /var/log/auth.log | tail -n 20

sudo journalctl -u ssh | grep "Failed password"



```
(kali@kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log | tail -n 20
sudo journalctl -u ssh | grep "Failed password"

[sudo] password for kali:
2025-03-17T10:17:01.586374+05:30 kali sudo:    kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
Mar 11 19:52:35 kali sshd-session[27435]: Failed password for user2 from 127.0.0.1 port 50696 ssh2
Mar 11 19:52:35 kali sshd-session[27425]: Failed password for user2 from 127.0.0.1 port 50646 ssh2
Mar 11 19:52:35 kali sshd-session[27427]: Failed password for user2 from 127.0.0.1 port 50650 ssh2
Mar 11 19:52:35 kali sshd-session[27418]: Failed password for user2 from 127.0.0.1 port 50640 ssh2
Mar 11 19:52:35 kali sshd-session[27422]: Failed password for user2 from 127.0.0.1 port 50730 ssh2
Mar 11 19:52:35 kali sshd-session[27441]: Failed password for user2 from 127.0.0.1 port 50712 ssh2
Mar 11 19:52:35 kali sshd-session[27419]: Failed password for user2 from 127.0.0.1 port 50642 ssh2
Mar 11 19:52:35 kali sshd-session[27433]: Failed password for user2 from 127.0.0.1 port 50726 ssh2
Mar 11 19:52:35 kali sshd-session[27424]: Failed password for user2 from 127.0.0.1 port 50648 ssh2
Mar 11 19:52:35 kali sshd-session[27430]: Failed password for user2 from 127.0.0.1 port 50732 ssh2
Mar 11 19:52:35 kali sshd-session[27420]: Failed password for user2 from 127.0.0.1 port 50722 ssh2
Mar 11 19:52:35 kali sshd-session[27438]: Failed password for user2 from 127.0.0.1 port 50674 ssh2
Mar 11 19:52:35 kali sshd-session[27421]: Failed password for user2 from 127.0.0.1 port 50724 ssh2
Mar 11 19:52:35 kali sshd-session[27443]: Failed password for user2 from 127.0.0.1 port 50766 ssh2
Mar 11 19:52:35 kali sshd-session[27439]: Failed password for user2 from 127.0.0.1 port 50644 ssh2
Mar 11 19:52:37 kali sshd-session[27435]: Failed password for user2 from 127.0.0.1 port 50696 ssh2
Mar 11 19:52:38 kali sshd-session[27420]: Failed password for user2 from 127.0.0.1 port 50722 ssh2
Mar 11 19:52:38 kali sshd-session[27418]: Failed password for user2 from 127.0.0.1 port 50640 ssh2
Mar 11 19:52:38 kali sshd-session[27427]: Failed password for user2 from 127.0.0.1 port 50650 ssh2
Mar 11 19:52:38 kali sshd-session[27433]: Failed password for user2 from 127.0.0.1 port 50726 ssh2
Mar 11 19:52:38 kali sshd-session[27421]: Failed password for user2 from 127.0.0.1 port 50724 ssh2
Mar 11 19:52:38 kali sshd-session[27439]: Failed password for user2 from 127.0.0.1 port 50644 ssh2
Mar 11 19:52:39 kali sshd-session[27419]: Failed password for user2 from 127.0.0.1 port 50642 ssh2
Mar 11 19:52:39 kali sshd-session[27443]: Failed password for user2 from 127.0.0.1 port 50766 ssh2
Mar 11 19:52:39 kali sshd-session[27438]: Failed password for user2 from 127.0.0.1 port 50674 ssh2
Mar 11 19:52:39 kali sshd-session[27430]: Failed password for user2 from 127.0.0.1 port 50732 ssh2
Mar 11 19:52:39 kali sshd-session[27441]: Failed password for user2 from 127.0.0.1 port 50712 ssh2
Mar 11 19:52:39 kali sshd-session[27425]: Failed password for user2 from 127.0.0.1 port 50646 ssh2
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
Mar 12 21:27:26 kali sshd-session[56987]: Failed password for root from 127.0.0.1 port 49354 ssh2  
Mar 12 21:27:27 kali sshd-session[56990]: Failed password for root from 127.0.0.1 port 49370 ssh2  
Mar 12 21:27:27 kali sshd-session[56967]: Failed password for root from 127.0.0.1 port 49346 ssh2  
Mar 12 21:27:29 kali sshd-session[56987]: Failed password for root from 127.0.0.1 port 49354 ssh2  
Mar 12 21:27:29 kali sshd-session[57010]: Failed password for root from 127.0.0.1 port 49382 ssh2  
Mar 12 21:27:30 kali sshd-session[56990]: Failed password for root from 127.0.0.1 port 49370 ssh2  
Mar 12 21:27:31 kali sshd-session[56967]: Failed password for root from 127.0.0.1 port 49346 ssh2  
Mar 12 21:27:33 kali sshd-session[56990]: Failed password for root from 127.0.0.1 port 49370 ssh2  
Mar 12 21:27:33 kali sshd-session[56987]: Failed password for root from 127.0.0.1 port 49354 ssh2  
Mar 12 21:27:33 kali sshd-session[57010]: Failed password for root from 127.0.0.1 port 49382 ssh2  
Mar 12 21:27:34 kali sshd-session[56967]: Failed password for root from 127.0.0.1 port 49346 ssh2  
Mar 12 21:27:36 kali sshd-session[57010]: Failed password for root from 127.0.0.1 port 49382 ssh2  
Mar 12 21:27:36 kali sshd-session[56967]: Failed password for root from 127.0.0.1 port 49346 ssh2  
Mar 12 21:27:37 kali sshd-session[56990]: Failed password for root from 127.0.0.1 port 49370 ssh2  
Mar 12 21:27:39 kali sshd-session[57010]: Failed password for root from 127.0.0.1 port 49382 ssh2  
Mar 12 21:30:08 kali sshd-session[58562]: Failed password for root from 127.0.0.1 port 41870 ssh2  
Mar 12 21:30:08 kali sshd-session[58560]: Failed password for root from 127.0.0.1 port 41872 ssh2  
Mar 12 21:30:09 kali sshd-session[58561]: Failed password for root from 127.0.0.1 port 41874 ssh2  
Mar 12 21:31:19 kali sshd-session[59277]: Failed password for root from 127.0.0.1 port 39264 ssh2  
Mar 12 21:31:20 kali sshd-session[59275]: Failed password for root from 127.0.0.1 port 39262 ssh2  
Mar 12 21:31:20 kali sshd-session[59276]: Failed password for root from 127.0.0.1 port 39258 ssh2  
Mar 12 21:31:20 kali sshd-session[59274]: Failed password for root from 127.0.0.1 port 39260 ssh2  
  
(kali@kali)~  
$ sudo cat /var/log/auth.log | awk '/Failed password/{print $(NF-3)}' | sort | uniq -c | sort -nr | head  
  
1 COMMAND=/usr/bin/grep  
  
(kali@kali)~  
$ sudo grep "Accepted password" /var/log/auth.log  
  
2025-03-17T10:18:31.506184+05:30 kali sudo:      kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Accepted password' /var/log/auth.log  
  
(kali@kali)~  
$
```

- **Find brute-force attempts (multiple failures from the same IP):**

```
sudo cat /var/log/auth.log | awk '/Failed password/{print $(NF-3)}' | sort | uniq -c | sort -nr | head
```

- **Identify successful logins:**

```
sudo grep "Accepted password" /var/log/auth.log
```

- **Mitigation: Implement Fail2Ban**

Install and configure Fail2Ban to block repeated failed attempts.

```
sudo apt update && sudo apt install fail2ban -y
```

```
sudo systemctl enable fail2ban
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~  
kali@kali: ~  
  
(kali@kali)~  
$ sudo apt update && sudo apt install fail2ban -y  
sudo systemctl enable fail2ban  
  
Hit:1 https://brave-browser-apt-release.s3.brave.com stable InRelease  
Hit:2 https://brave-browser-apt-beta.s3.brave.com stable InRelease  
Get:3 http://kali.download/kali kali-rolling InRelease [41.5 kB]  
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [20.7 MB]  
Hit:5 https://download.sublimetext.com apt/stable/ InRelease  
Get:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.3 MB]  
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]  
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [267 kB]  
Fetched 70.4 MB in 6s (11.1 MB/s)  
384 packages can be upgraded. Run 'apt list --upgradable' to see them.  
fail2ban is already the newest version (1.1.0-7).  
The following packages were automatically installed and are no longer required:  
  cpp-13 libical3t64 libmsgraph-0-1 libpython3.12-minimal libtag1v5 python3-six  
  cpp-13-x86-64-linux-gnu libimobiledevice6 libpaper1 libpython3.12-stdlib libtag1v5-vanilla python3.11  
  gcc-13-base libjim0.82t64 libperl5.38t64 libpython3.12t64 libtagc0 python3.11-minimal  
  imagemagick-6-common libldap-2.5-0 libplacebo338 libqt6dbus6t64 libusbmuxd6 python3.12  
  libassuan0 libllvm17t64 libplist3 libqt6gui6t64 libutempter0 python3.12-dev  
  libavfilter9 libmagickcore-6.q16-7-extra libpoppler134 libqt6network6t64 libwebRTC-audio-processing1 python3.12-minimal  
  libavformat60 libmagickcore-6.q16-7t64 libpostproc57 libqt6opengl6t64 linux-image-6.8.11-amd64  
  libconfig+9v5 libmagickwand-6.q16-7t64 libpython3.11-minimal libqt6widgets6t64 perl-modules-5.38  
  libdirectfb-1.7-7t64 libmbcrypto7t64 libpython3.11-stdlib libssh-gcrypt-4 python3-pexpect  
  libgspell-1-2 libmfx1 libpython3.12-dev libswscale7 python3-ptyprocess  
Use 'sudo apt autoremove' to remove them.  
  
Summary:  
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 384  
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban  
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
```

- **Configure SSH Jail:**

`sudo nano /etc/fail2ban/jail.local`

- **Add these lines:**

```
GNU nano 8.3 /etc/fail2ban/jail.local  
[sshd]  
enabled = true  
port = ssh  
filter = sshd  
logpath = /var/log/auth.log  
maxretry = 5  
bantime = 600  
  
[Read 8 lines]  
^G Help ^G Write Out ^F Where Is ^K Cut ^T Execute ^C Location ^M-U Undo ^M-A Set Mark ^M-] To Bracket  
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^_ Go To Line ^M-E Redo ^M-6 Copy ^M-B Where Was
```

[sshd]

enabled = true

port = ssh

filter = sshd

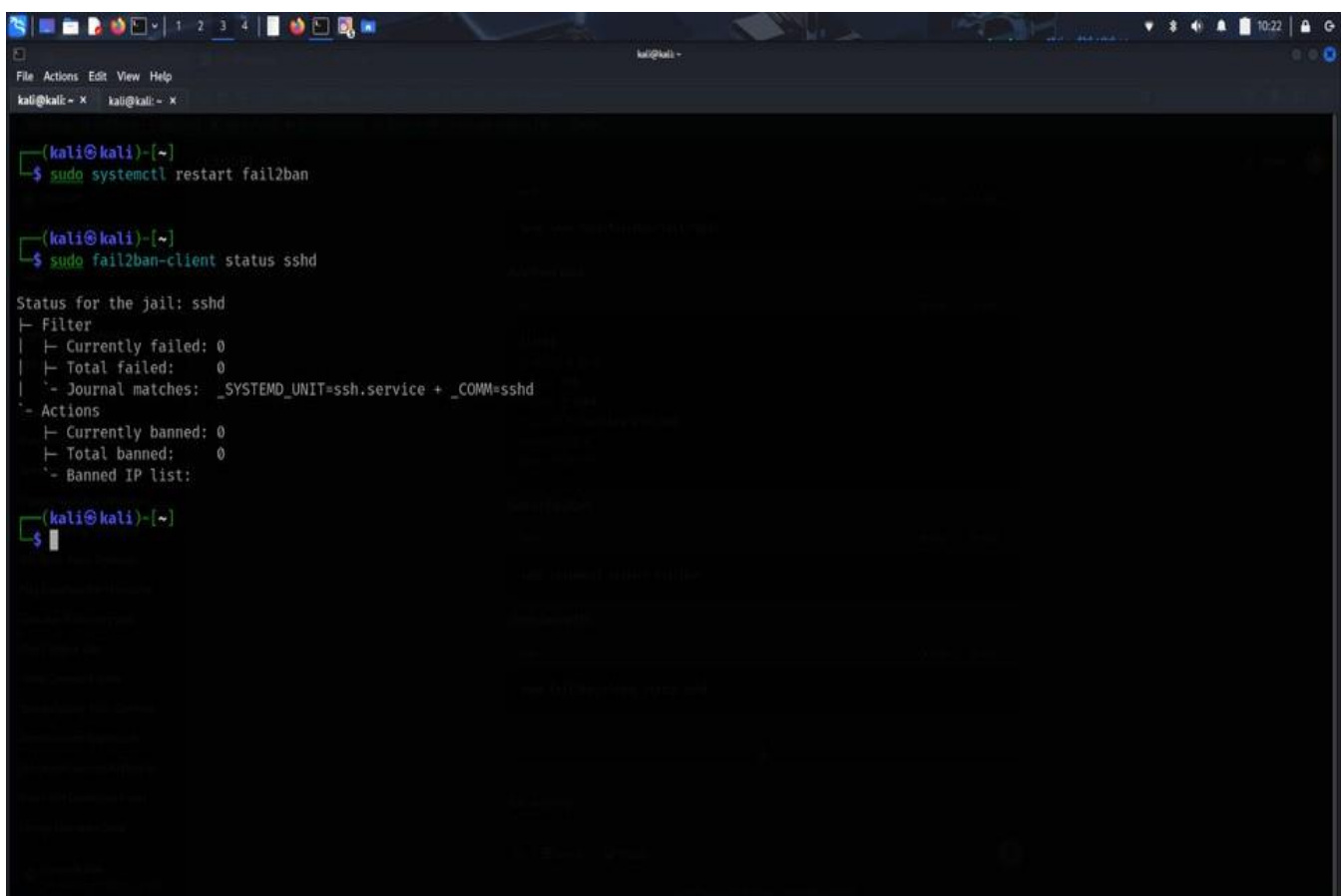
logpath = /var/log/auth.log

maxretry = 5

bantime = 600

- **Restart Fail2Ban:**

`sudo systemctl restart fail2ban`

A terminal window on a Kali Linux system. The user runs 'sudo systemctl restart fail2ban'. Then, they run 'sudo fail2ban-client status sshd'. The output shows the status for the jail 'sshd', including filter, currently failed, total failed, journal matches, actions, currently banned, total banned, and a banned IP list. The terminal is dark-themed with green and red text for commands and output respectively. The window title is 'kali@kali -'.

```
(kali@kali)~$ sudo systemctl restart 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:
```

- **Check banned IPs:**

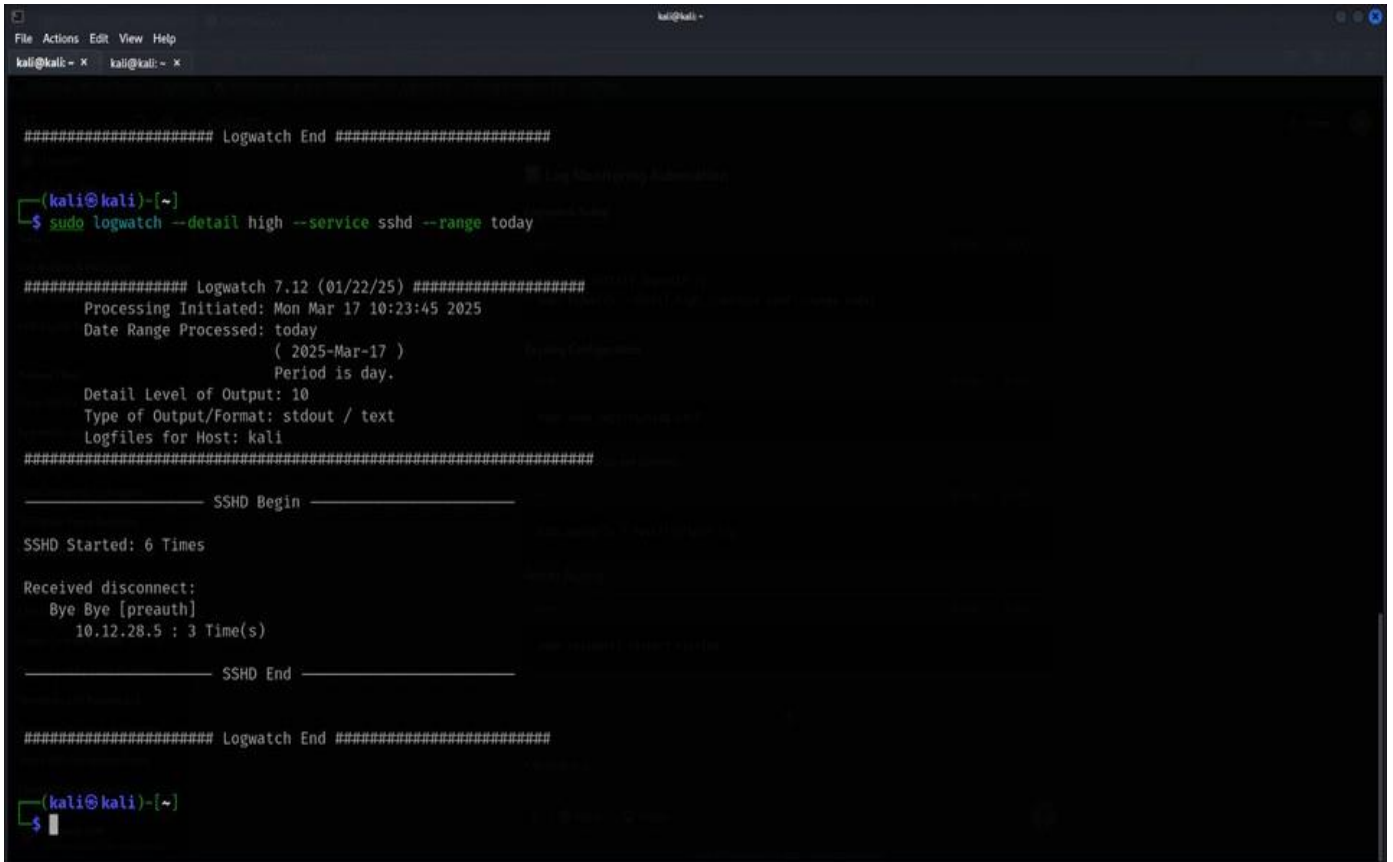
`sudo fail2ban-client status sshd`

- **Log Monitoring Automation**

Logwatch Setup

`sudo apt install logwatch -y`

`sudo logwatch --detail high --service sshd --range today`



```
##### Logwatch End #####

(kali@kali)-[~]
$ sudo logwatch --detail high --service sshd --range today

##### Logwatch 7.12 (01/22/25) #####
Processing Initiated: Mon Mar 17 10:23:45 2025
Date Range Processed: today
                      ( 2025-Mar-17 )
                      Period is day.
Detail Level of Output: 10
Type of Output/Format: stdout / text
Logfiles for Host: kali

#####

----- SSHD Begin -----

SSHD Started: 6 Times

Received disconnect:
Bye Bye [preauth]
10.12.28.5 : 3 Time(s)

----- SSHD End -----

##### Logwatch End #####

(kali@kali)-[~]
$
```

- **Rsyslog Configuration**

`sudo nano /etc/rsyslog.conf`

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
##### Logwatch 7.12 (01/22/25) #####  
Processing Initiated: Mon Mar 17 10:23:45 2025  
Date Range Processed: today  
                        ( 2025-Mar-17 )  
Period is day.  
Detail Level of Output: 10  
Type of Output/Format: stdout / text  
Logfiles for Host: kali  
#####  
----- SSHD Begin -----  
SSHD Started: 6 Times  
Received disconnect:  
Bye Bye [preauth]  
10.12.28.5 : 3 Time(s)  
----- SSHD End -----  
##### Logwatch End #####  
  
(kali@kali)-[~]  
$ sudo nano /etc/rsyslog.conf  
  
(kali@kali)-[~]  
$ sudo systemctl restart rsyslog  
  
(kali@kali)-[~]  
$
```

- **Ensure these lines are present:**

auth,authpriv.* /var/log/auth.log

- **Restart Rsyslog:**

sudo systemctl restart rsyslog