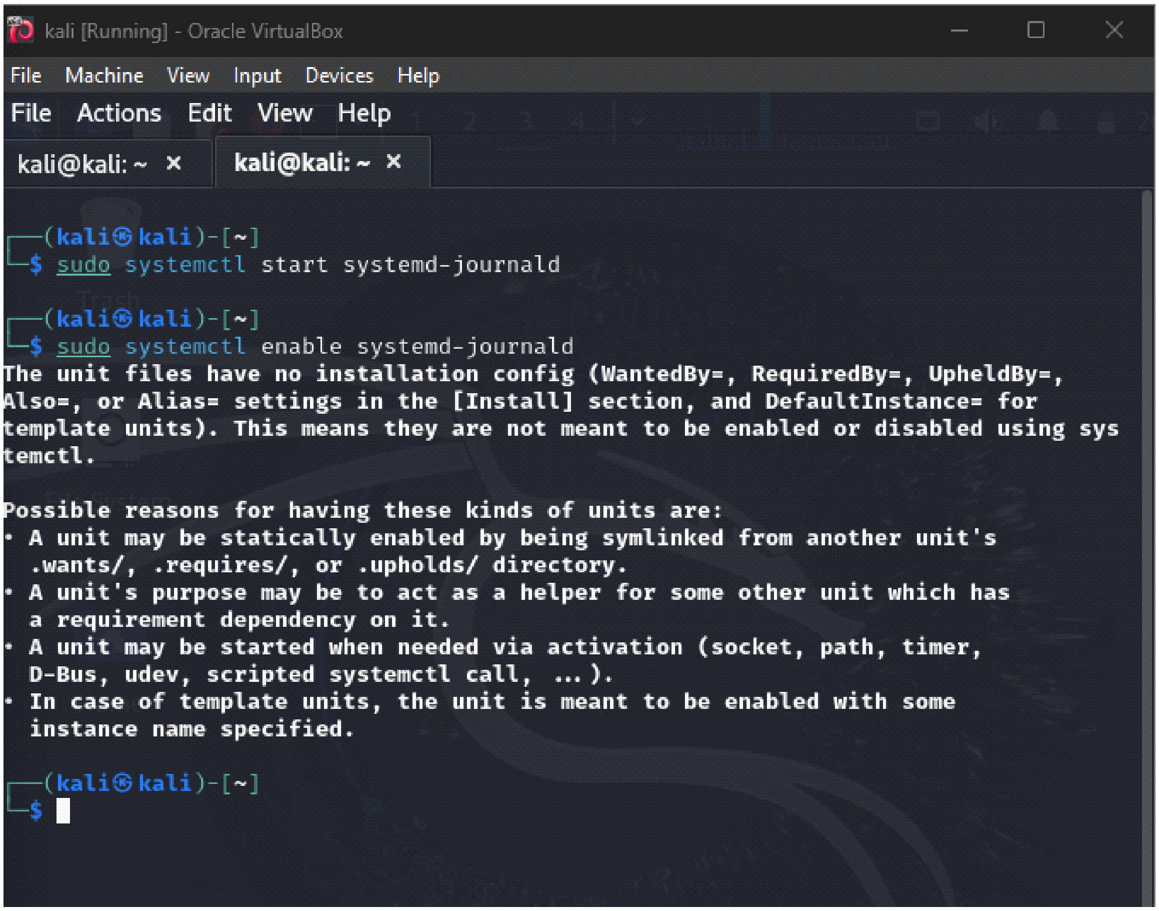
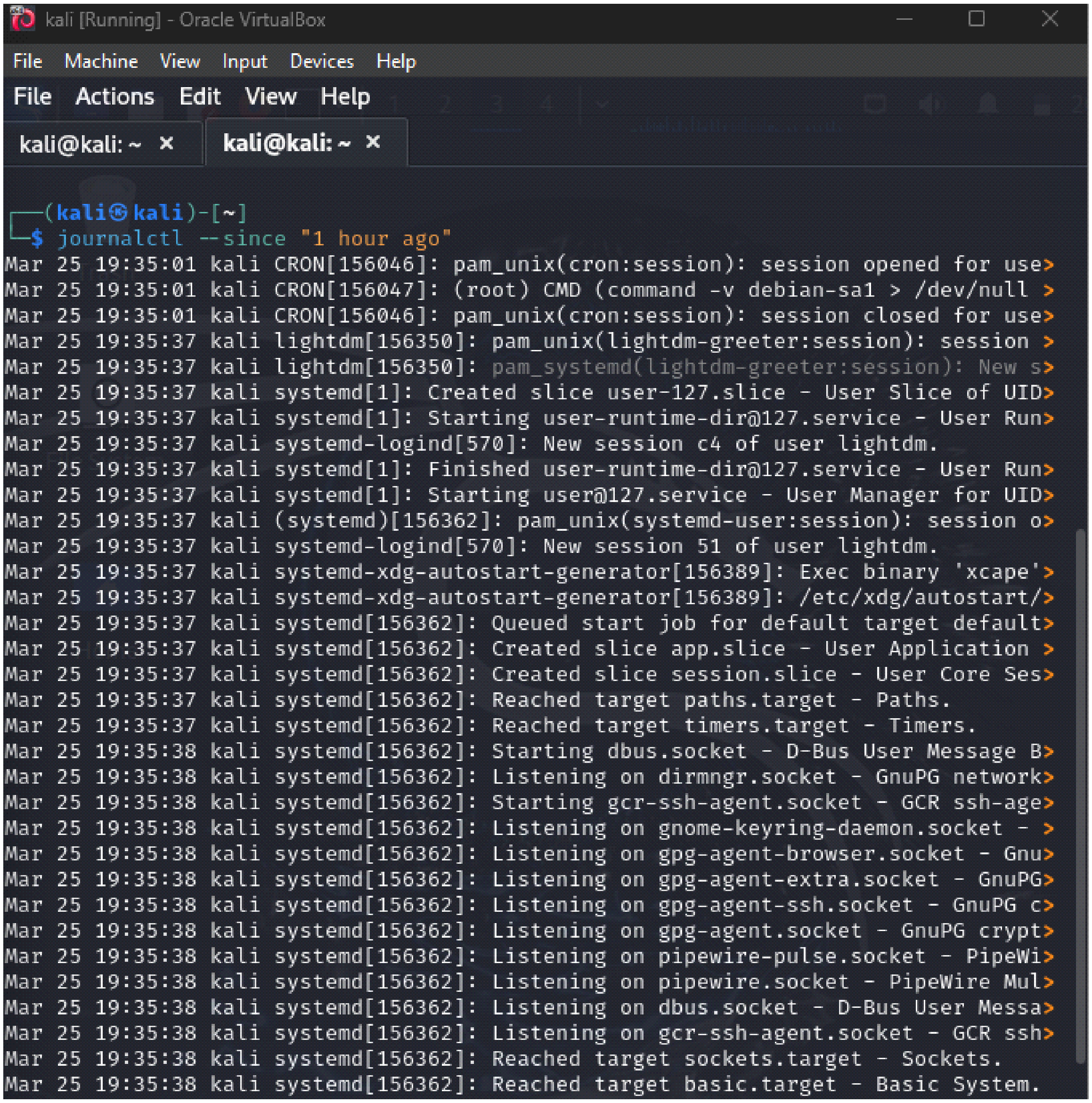
Task 6: Log Analysis & Intrusion Detection

Setup:

Ensure System Logging is Enabled


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start systemd-journald

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable systemd-journald
The unit files have no installation config (WantedBy=, RequiredBy=, UpheldBy=,
Also=, or Alias= settings in the [Install] section, and DefaultInstance= for
template units). This means they are not meant to be enabled or disabled using sys
temctl.

Possible reasons for having these kinds of units are:
• A unit may be statically enabled by being symlinked from another unit's
  .wants/, .requires/, or .upholds/ directory.
• A unit's purpose may be to act as a helper for some other unit which has
  a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer,
  D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some
  instance name specified.

┌──(kali㉿kali)-[~]
└─$ 
```

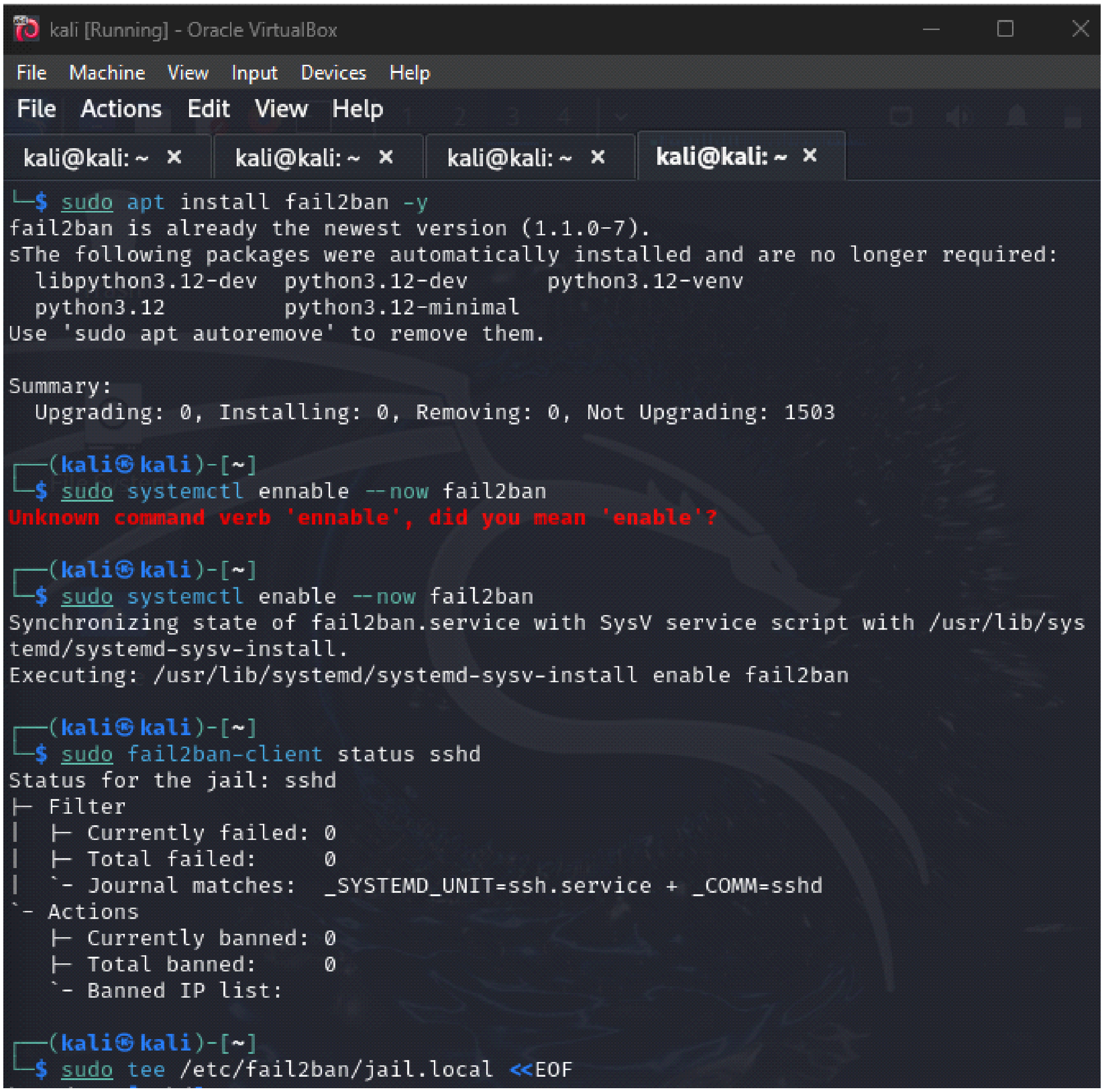

kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ journalctl --since "1 hour ago"
Mar 25 19:35:01 kali CRON[156046]: pam_unix(cron:session): session opened for use>
Mar 25 19:35:01 kali CRON[156047]: (root) CMD (command -v debian-sa1 > /dev/null >
Mar 25 19:35:01 kali CRON[156046]: pam_unix(cron:session): session closed for use>
Mar 25 19:35:37 kali lightdm[156350]: pam_unix(lightdm-greeter:session): session >
Mar 25 19:35:37 kali lightdm[156350]: pam_systemd(lightdm-greeter:session): New s>
Mar 25 19:35:37 kali systemd[1]: Created slice user-127.slice - User Slice of UID>
Mar 25 19:35:37 kali systemd[1]: Starting user-runtime-dir@127.service - User Run>
Mar 25 19:35:37 kali systemd-logind[570]: New session c4 of user lightdm.
Mar 25 19:35:37 kali systemd[1]: Finished user-runtime-dir@127.service - User Run>
Mar 25 19:35:37 kali systemd[1]: Starting user@127.service - User Manager for UID>
Mar 25 19:35:37 kali (systemd)[156362]: pam_unix(systemd-user:session): session o>
Mar 25 19:35:37 kali systemd-logind[570]: New session 51 of user lightdm.
Mar 25 19:35:37 kali systemd-xdg-autostart-generator[156389]: Exec binary 'xcape'>
Mar 25 19:35:37 kali systemd-xdg-autostart-generator[156389]: /etc/xdg/autostart/>
Mar 25 19:35:37 kali systemd[156362]: Queued start job for default target default>
Mar 25 19:35:37 kali systemd[156362]: Created slice app.slice - User Application >
Mar 25 19:35:37 kali systemd[156362]: Created slice session.slice - User Core Ses>
Mar 25 19:35:37 kali systemd[156362]: Reached target paths.target - Paths.
Mar 25 19:35:37 kali systemd[156362]: Reached target timers.target - Timers.
Mar 25 19:35:38 kali systemd[156362]: Starting dbus.socket - D-Bus User Message B>
Mar 25 19:35:38 kali systemd[156362]: Listening on dirmngr.socket - GnuPG network>
Mar 25 19:35:38 kali systemd[156362]: Starting gcr-ssh-agent.socket - GCR ssh-age>
Mar 25 19:35:38 kali systemd[156362]: Listening on gnome-keyring-daemon.socket - >
Mar 25 19:35:38 kali systemd[156362]: Listening on gpg-agent-browser.socket - Gnu>
Mar 25 19:35:38 kali systemd[156362]: Listening on gpg-agent-extra.socket - GnuPG>
Mar 25 19:35:38 kali systemd[156362]: Listening on gpg-agent-ssh.socket - GnuPG c>
Mar 25 19:35:38 kali systemd[156362]: Listening on gpg-agent.socket - GnuPG crypt>
Mar 25 19:35:38 kali systemd[156362]: Listening on pipewire-pulse.socket - PipeWi>
Mar 25 19:35:38 kali systemd[156362]: Listening on pipewire.socket - PipeWire Mul>
Mar 25 19:35:38 kali systemd[156362]: Listening on dbus.socket - D-Bus User Messa>
Mar 25 19:35:38 kali systemd[156362]: Listening on gcr-ssh-agent.socket - GCR ssh>
Mar 25 19:35:38 kali systemd[156362]: Reached target sockets.target - Sockets.
Mar 25 19:35:38 kali systemd[156362]: Reached target basic.target - Basic System.
```

Mitigation

1. Implement Fail2Ban to Block Repeated Failed Attempts:

Install Fail2Ban


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~

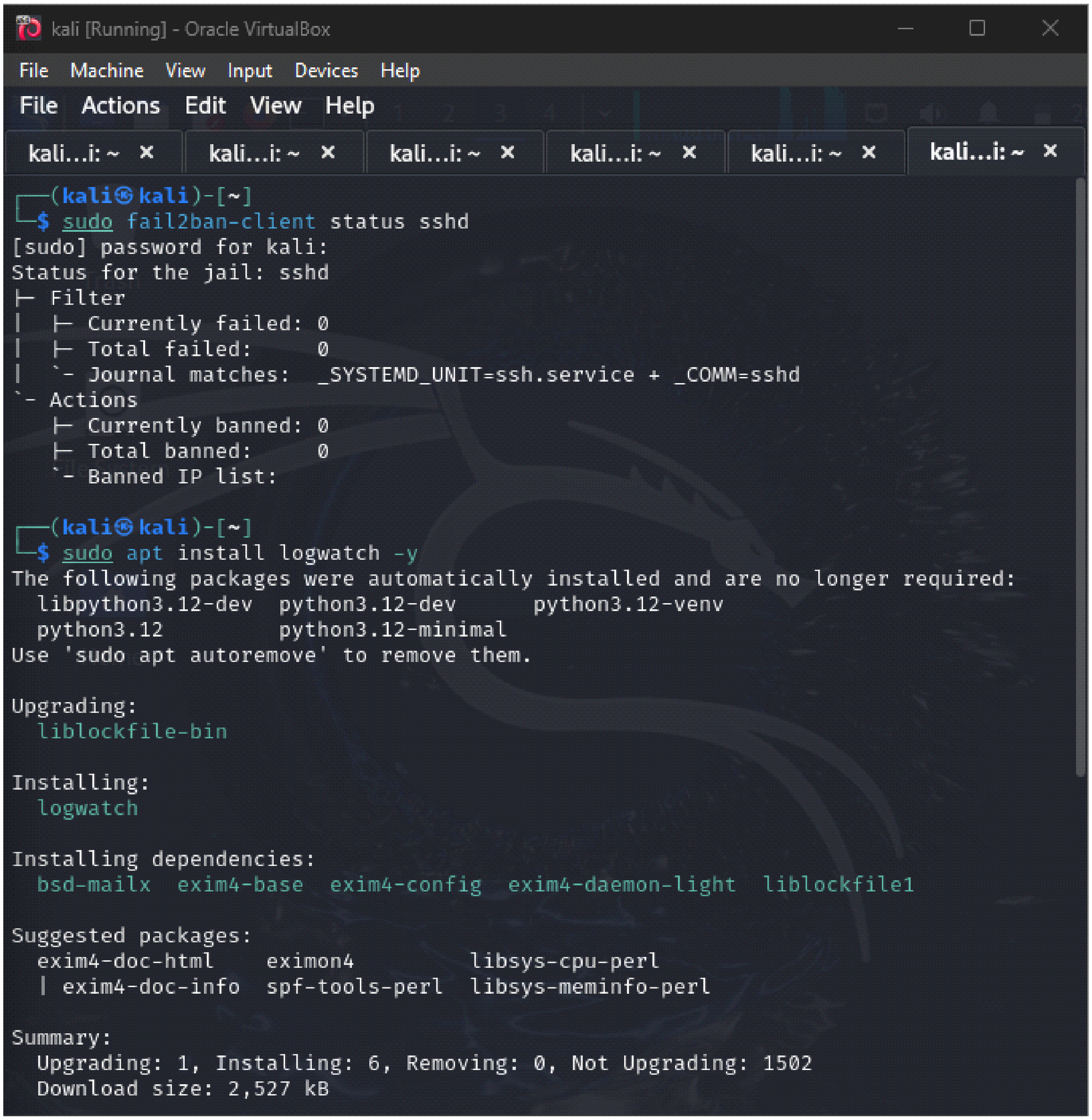
```
└─$ sudo apt install fail2ban -y
fail2ban is already the newest version (1.1.0-7).
sThe following packages were automatically installed and are no longer required:
  libpython3.12-dev  python3.12-dev      python3.12-venv
  python3.12         python3.12-minimal
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1503

┌──(kali㉿kali)-[~]
└─$ sudo systemctl ennable --now fail2ban
Unknown command verb 'ennable', did you mean 'enable'?

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable --now fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/sys
temd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable 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:

┌──(kali㉿kali)-[~]
└─$ sudo tee /etc/fail2ban/jail.local <<EOF
```

Check if an IP is banned:

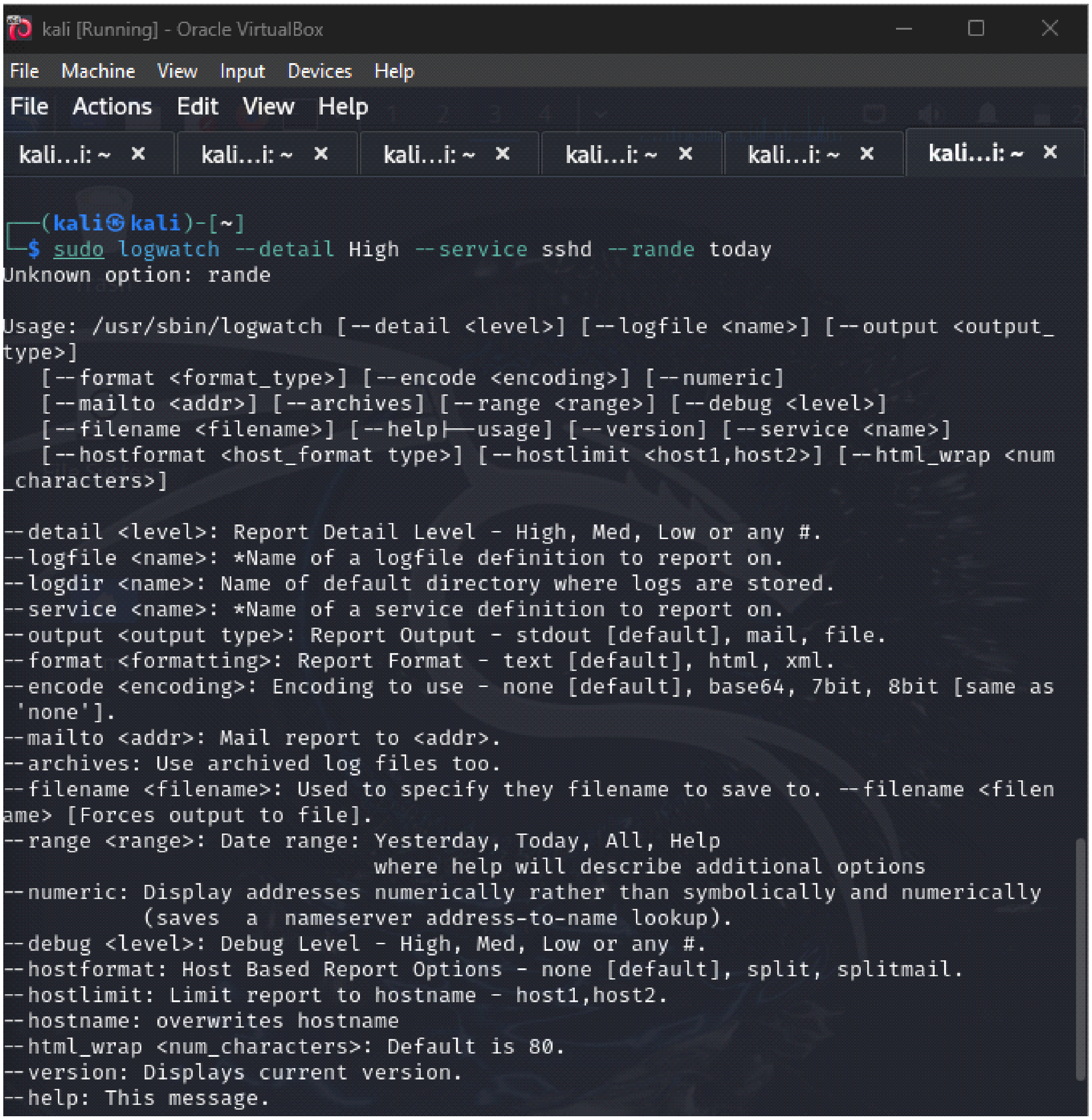
```
sudo fail2ban-client status sshdss
```

Automate Log Monitoring with logwatch

```
sudo apt install logwatch -y
sudo logwatch --detail High --service sshd --range today
```


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali…i: ~ ✕ kali…i: ~ ✕ kali…i: ~ ✕ kali…i: ~ ✕ kali…i: ~ ✕ kali…i: ~ ✕

```
┌──(kali㉿kali)-[~]
└─$ sudo fail2ban-client status sshd
[sudo] password for kali:
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:

┌──(kali㉿kali)-[~]
└─$ sudo apt install logwatch -y
The following packages were automatically installed and are no longer required:
  libpython3.12-dev  python3.12-dev      python3.12-venv
  python3.12         python3.12-minimal
Use 'sudo apt autoremove' to remove them.

Upgrading:
  liblockfile-bin

Installing:
  logwatch

Installing dependencies:
  bsd-mailx  exim4-base  exim4-config  exim4-daemon-light  liblockfile1

Suggested packages:
  exim4-doc-html    eximon4         libsys-cpu-perl
  | exim4-doc-info  spf-tools-perl  libsys-meminfo-perl

Summary:
  Upgrading: 1, Installing: 6, Removing: 0, Not Upgrading: 1502
  Download size: 2,527 kB
```


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali…i: ~ ×
kali…i: ~ ×
kali…i: ~ ×
kali…i: ~ ×
kali…i: ~ ×
kali…i: ~ ×

```
┌──(kali㉿kali)-[~]
└─$ sudo logwatch --detail High --service sshd --rande today
Unknown option: rande

Usage: /usr/sbin/logwatch [--detail <level>] [--logfile <name>] [--output <output_
type>]
   [--format <format_type>] [--encode <encoding>] [--numeric]
   [--mailto <addr>] [--archives] [--range <range>] [--debug <level>]
   [--filename <filename>] [--help|--usage] [--version] [--service <name>]
   [--hostformat <host_format type>] [--hostlimit <host1,host2>] [--html_wrap <num
_characters>]

--detail <level>: Report Detail Level - High, Med, Low or any #.
--logfile <name>: *Name of a logfile definition to report on.
--logdir <name>: Name of default directory where logs are stored.
--service <name>: *Name of a service definition to report on.
--output <output type>: Report Output - stdout [default], mail, file.
--format <formatting>: Report Format - text [default], html, xml.
--encode <encoding>: Encoding to use - none [default], base64, 7bit, 8bit [same as
 'none'].
--mailto <addr>: Mail report to <addr>.
--archives: Use archived log files too.
--filename <filename>: Used to specify they filename to save to. --filename <filen
ame> [Forces output to file].
--range <range>: Date range: Yesterday, Today, All, Help
                             where help will describe additional options
--numeric: Display addresses numerically rather than symbolically and numerically
           (saves  a  nameserver address-to-name lookup).
--debug <level>: Debug Level - High, Med, Low or any #.
--hostformat: Host Based Report Options - none [default], split, splitmail.
--hostlimit: Limit report to hostname - host1,host2.
--hostname: overwrites hostname
--html_wrap <num_characters>: Default is 80.
--version: Displays current version.
--help: This message.
```