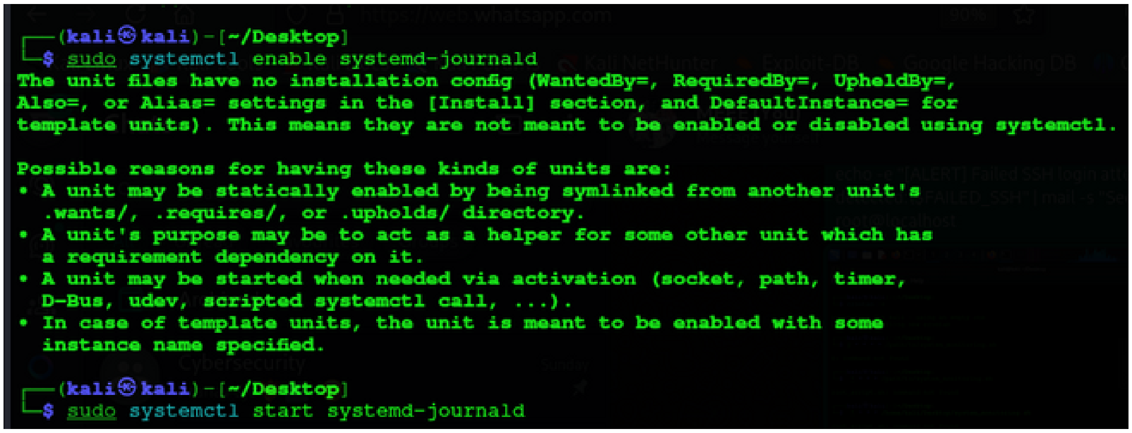
Task 6

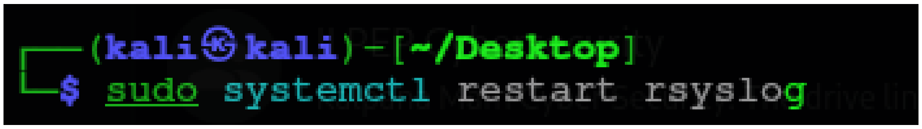
Setup



```
┌──(kali㉿kali)-[~/Desktop]
└─$ 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 systemctl.

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)-[~/Desktop]
└─$ sudo systemctl start systemd-journald
```



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

To enable system logging for enhanced security monitoring, first activate the journal service with the commands:

`sudo systemctl enable systemd-journald`

`sudo systemctl start systemd-journald`

For Ubuntu and Debian systems, authentication attempts are logged in `/var/log/auth.log` by default. If this file is missing, enable it by uncommenting the following line in `/etc/rsyslog.conf`:

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

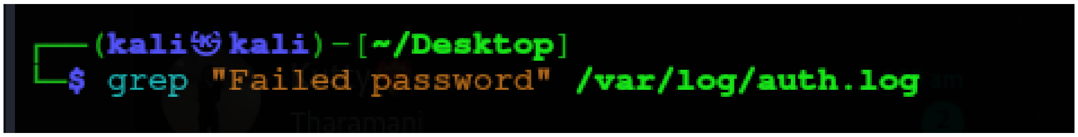
After making the changes, restart the `rsyslog` service using:

`sudo systemctl restart rsyslog`

To simulate multiple failed SSH login attempts for testing purposes, use the command:

`ssh invalid_user@localhost`

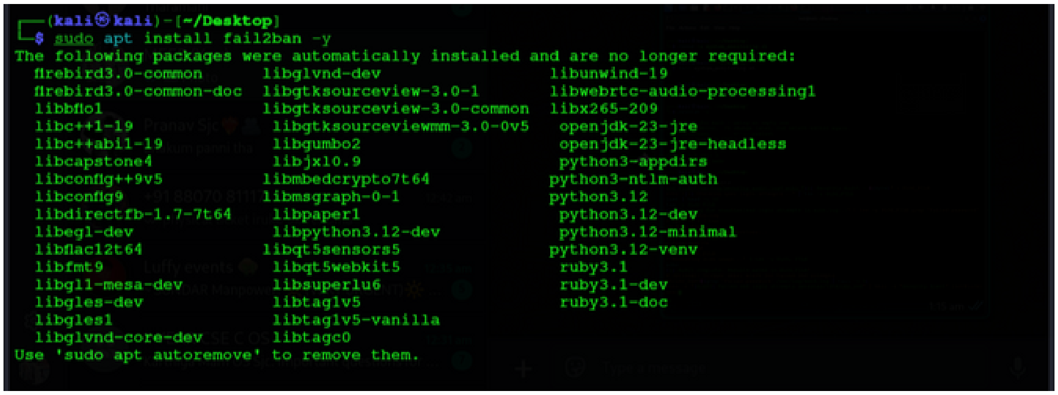
Exploit



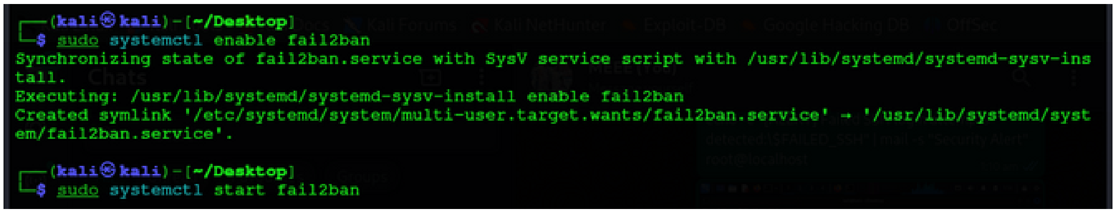
```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep "Failed password" /var/log/auth.log
```

This command analyzes Logs for Brute-force Attempts

Mitigation

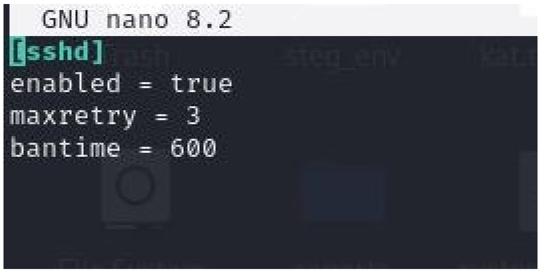


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install fail2ban -y
The following packages were automatically installed and are no longer required:
  firebird3.0-common      libglvnd-dev                  libunwind-19
  firebird3.0-common-doc  libgtksourceview-3.0-1        libwebrtc-audio-processing1
  libbfio1                libgtksourceview-3.0-common   libx265-209
  libc++1-19              libgtksourceviewmm-3.0-0v5    openjdk-23-jre
  libc++abi1-19           libgumbo2                     openjdk-23-jre-headless
  libcapstone4            libjxl0.9                     python3-appdirs
  libconfig++9v5          libmbedcrypto7t64             python3-ntlm-auth
  libconfig9              libmsgraph-0-1                python3.12
  libdirectfb-1.7-7t64    libpaper1                     python3.12-dev
  libegl-dev              libpython3.12-dev             python3.12-minimal
  libflac12t64            libqt5sensors5                python3.12-venv
  libfmt9                 libqt5webkit5                 ruby3.1
  libgl1-mesa-dev         libsuperlu6                   ruby3.1-dev
  libgles-dev             libtaglv5                     ruby3.1-doc
  libgles1                libtaglv5-vanilla
  libglvnd-core-dev       libtagc0
Use 'sudo apt autoremove' to remove them.
```



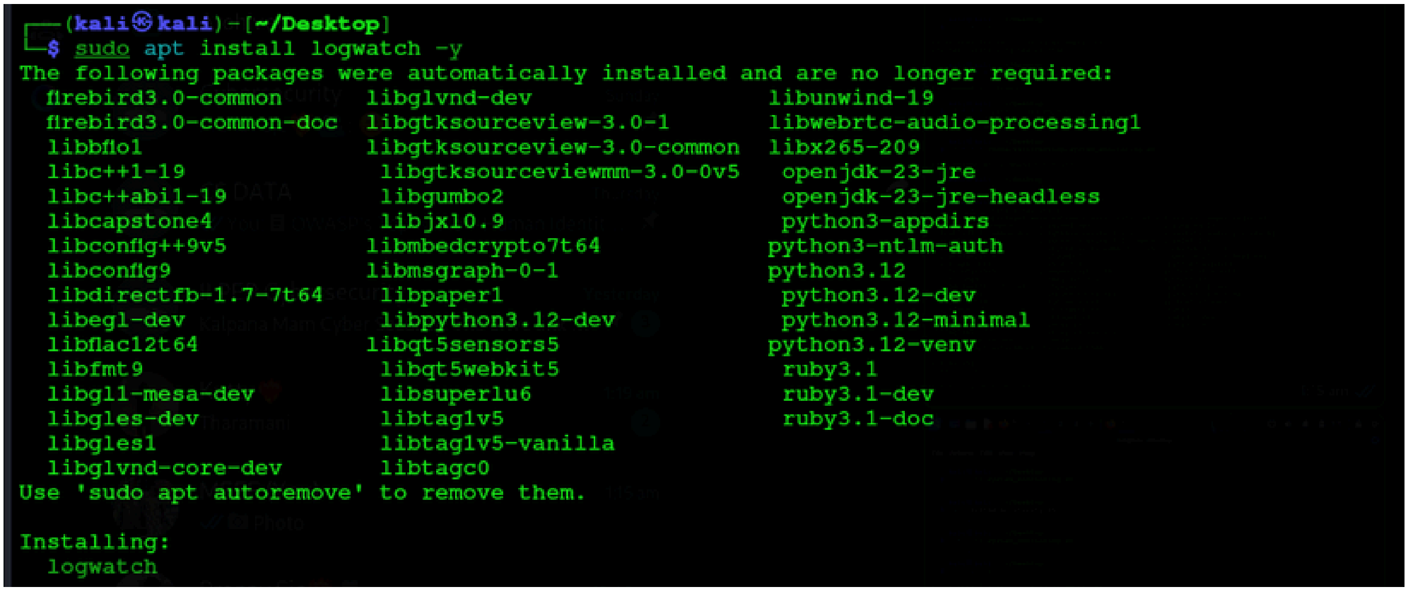
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/systemd/systemd-sysv-ins
tall.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/syst
em/fail2ban.service'.

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



```
  GNU nano 8.2
[sshd]
enabled = true
maxretry = 3
bantime = 600
```

To enhance system security, install fail2ban using sudo apt install fail2ban -y, enable it with sudo systemctl enable fail2ban, and start the service using sudo systemctl start fail2ban. Then, configure /etc/fail2ban/jail.local by adding [sshd] enabled = true, setting maxretry ≣ 3, bantime ≣ 10m, and findtime ≣ 10m, followed by restarting the service with sudo systemctl restart fail2ban to apply the changes. As we have done these steps in task 1 , I’m not gonna install it again.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install logwatch -y
The following packages were automatically installed and are no longer required:
  firebird3.0-common       libglvnd-dev                  libunwind-19
  firebird3.0-common-doc   libgtksourceview-3.0-1        libwebrtc-audio-processing1
  libbfio1                 libgtksourceview-3.0-common   libx265-209
  libc++1-19                libgtksourceviewmm-3.0-0v5    openjdk-23-jre
  libc++abi1-19             libgumbo2                     openjdk-23-jre-headless
  libcapstone4              libjxl0.9                     python3-appdirs
  libconfig++9v5           libmbedcrypto7t64             python3-ntlm-auth
  libconfig9               libmsgraph-0-1                python3.12
  libdirectfb-1.7-7t64      libpaper1                     python3.12-dev
  libegl-dev                libpython3.12-dev             python3.12-minimal
  libflac12t64             libqt5sensors5                python3.12-venv
  libfmt9                   libqt5webkit5                 ruby3.1
  libgl1-mesa-dev           libsuperlu6                   ruby3.1-dev
  libgles-dev               libtaglv5                     ruby3.1-doc
  libgles1                  libtaglv5-vanilla
  libglvnd-core-dev         libtagc0
Use 'sudo apt autoremove' to remove them.

Installing:
  logwatch
```

To automate log monitoring, install logwatch using sudo apt install logwatch -y, then configure it to send detailed log summaries via email with logwatch --detail high --mailto root@localhost. For remote log storage or advanced filtering, edit /etc/rsyslog.conf and add *.* ≣≣REMOTE_SERVER≣≣514 to forward logs to the designated remote server.