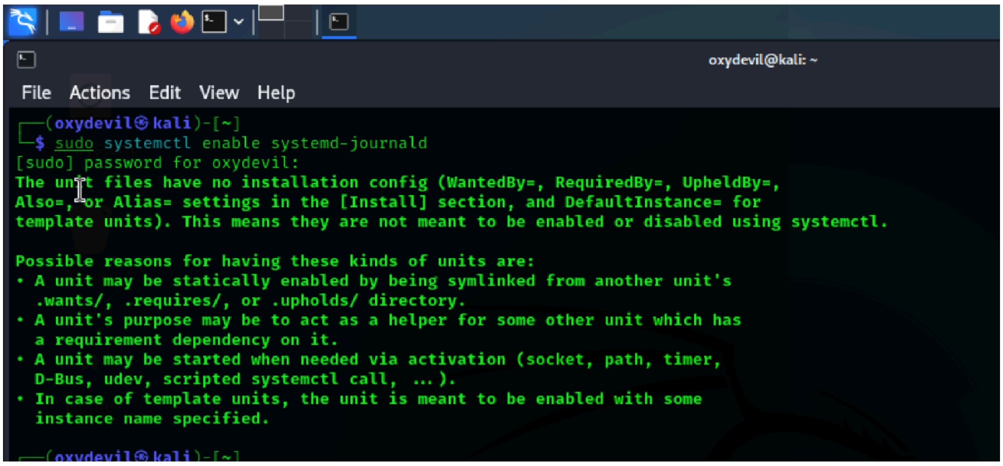
Task 6

SETUP

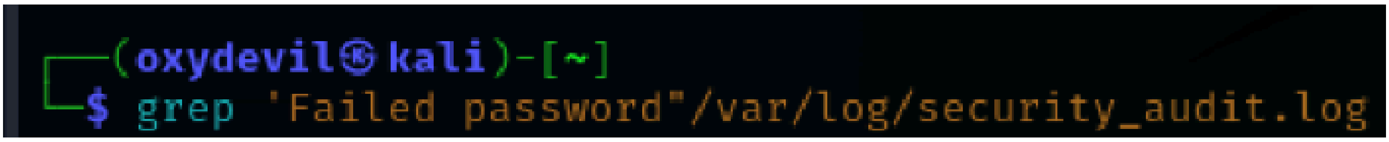


```
┌──(oxydevil㉿kali)-[~]
└─$ sudo systemctl enable systemd-journald
[sudo] password for oxydevil:
The unit files have no installation config (WantedBy=, RequiredBy=, UpheldBy=,
Also=, or Alias= settings in the [Install] section, and DefaultInstance= for
template units). This means they are not meant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

┌──(oxydevil㉿kali)-[~]
```

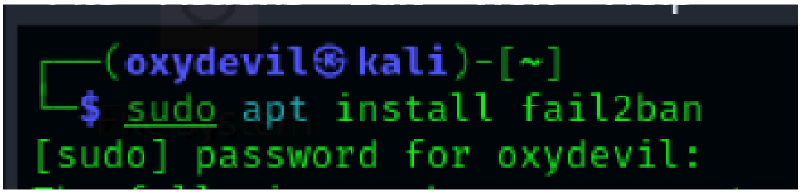
To enable system logging for enhanced security monitoring, first activate the journal service
with the commands:
sudo systemctl enable systemd-journald
sudo systemctl start systemd-journald
For Ubuntu and Debian systems, authentication attempts are logged in /var/log/auth.log by default.
If this file 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



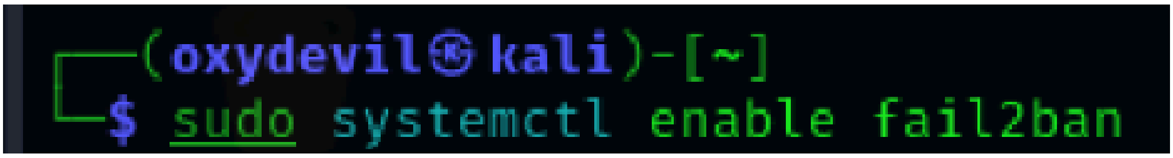
```
┌──(oxydevil㉿kali)-[~]
└─$ grep 'Failed password'/var/log/security_audit.log
```

This command analyzes Logs for Brute-force Attempts

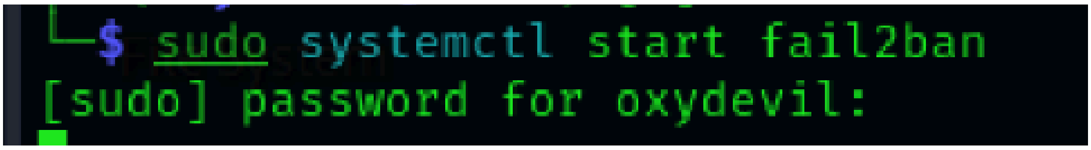
Mitigation:



```
┌──(oxydevil㉿kali)-[~]
└─$ sudo apt install fail2ban
[sudo] password for oxydevil:
```



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

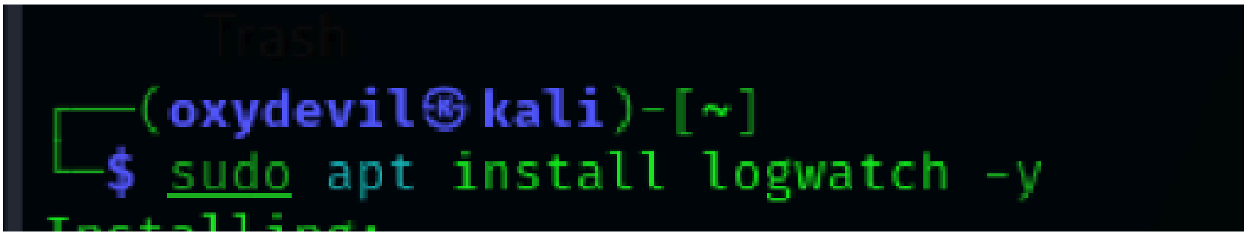


```
└─$ sudo systemctl start fail2ban
[sudo] password for oxydevil:
```

To improve system security, install Fail2Ban using the command sudo apt install fail2ban -y, then enable it with sudo systemctl enable fail2ban, and start the service using sudo systemctl start fail2ban.

Next, modify the configuration file /etc/fail2ban/jail.local by adding [sshd] enabled = true, setting maxretry = 3, bantime = 10m, and findtime = 10m. Finally, restart the service with sudo systemctl restart fail2ban to apply the updates.

Since we already completed these steps in Task 1, there's no need to reinstall it.



```
┌──(oxydevil㉿kali)-[~]
└─$ sudo apt install logwatch -y
Installing:
```

To streamline log monitoring, install Logwatch with sudo apt install logwatch -y, then configure it to send comprehensive log summaries via email using logwatch --detail high --mailto root@localhost.

For remote log storage or advanced filtering, modify /etc/rsyslog.conf by adding *.* @:514 to forward logs to the specified remote server.