TASK 6:

Log Analysis & Intrusion Detection:

Setup:

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable systemd-journald
sudo systemctl start systemd-journald
[sudo] password for kali:
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)-[~]
└─$ 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 and 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 these service using:

sudo systemctl restart rsyslog

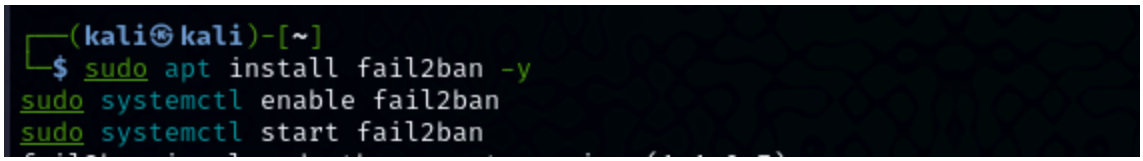
To simulate multiple failed SSH login attempts for testing purposes, use the command:

ssh invalid user@localhost

Exploit:

this analyzes logs for brute-force attempts.

Mitigation:



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 restarting the service with sudo systemctl restart fail2ban to apply the changes.

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 —malito root@localhost.