```
manikandan@HPVICTUSMANI61:~$ sudo service postfix status
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor p>
     Active: active (exited) since Sun 2024-09-08 12:08:57 IST; 1h 56min ago
       Docs: man:postfix(1)
    Main PID: 7893 (code=exited, status=0/SUCCESS)

Sep 08 12:08:57 HPVICTUSMANI61 systemd[1]: Starting Postfix Mail Transport >
Sep 08 12:08:57 HPVICTUSMANI61 systemd[1]: Finished Postfix Mail Transport >
manikandan@HPVICTUSMANI61:~$ sudo su
root@HPVICTUSMANI61:/home/manikandan# cd
root@HPVICTUSMANI61:~# ls /var/log/
alternatives.log  dist-upgrade  installer  sudo-access.log
apt               dmesg         journal    syslog
auth.log          dmesg.0       kern.log   ubuntu-advantage.log
bootstrap.log     dpkg.log      lastlog    unattended-upgrades
btmp              faillog       private    wtmp
```

```
<3>WSL (907) ERROR: UtilTranslatePathList:2866: Failed to translate C:Users\
MANIKANDAN J L\.cargo\bin
manikandan@HPVICTUSMANI61:~$ sudo su
[sudo] password for manikandan:
root@HPVICTUSMANI61:/home/manikandan# cd
root@HPVICTUSMANI61:~# ls /var/log
alternatives.log  dmesg       journal          syslog
apt               dmesg.0     kern.log         ubuntu-advantage.log
auth.log          dmesg.1.gz  lastlog          unattended-upgrades
bootstrap.log     dpkg.log    mail.log         wtmp
btmp              faillog     private
dist-upgrade      installer   sudo-access.log
root@HPVICTUSMANI61:~# cat /var/log/sudo-access.log
Sep  8 14:05:43 : manikandan : TTY=pts/2 ; PWD=/home/manikandan ; USER=root
;
    COMMAND=/usr/sbin/service postfix status
Sep  8 14:08:47 : manikandan : TTY=pts/2 ; PWD=/home/manikandan ; USER=root
;
    COMMAND=/usr/bin/su
Sep  8 19:48:43 : manikandan : TTY=pts/0 ; PWD=/home/manikandan ; USER=root
;
    COMMAND=/usr/bin/su
root@HPVICTUSMANI61:~# -
```

```
root@HPVICTUSMANI61:~# cat /var/log/sudo-access.log
Sep  8 14:05:43 : manikandan : TTY=pts/2 ; PWD=/home/manikandan ; USER=root
;
    COMMAND=/usr/sbin/service postfix status
Sep  8 14:08:47 : manikandan : TTY=pts/2 ; PWD=/home/manikandan ; USER=root
;
    COMMAND=/usr/bin/su
root@HPVICTUSMANI61:~#
```

```bash
#!/bin/bash

# Set the threshold for sudo attempts
THRESHOLD=3

# Log file to monitor sudo commands
LOG_FILE="/var/log/sudo-access.log"

# Email address to which you want to send notifications
ADMIN_EMAIL="gautham22poy@gmail.com"

# Extract low privilege users from /etc/passwd
LOW_PRIV_USERS=$(awk -F: '$3 >= 1000 && $3 != 65534 {print $1}' /etc/passwd)

echo $LOW_PRIV_USERS

# Loop through the users
for USER in $LOW_PRIV_USERS; do
        # Count sudo command attempts
        SUDO_COUNT=$(grep -c "$USER : user NOT in sudoers" $LOG_FILE)

        # Check if attempts exceed threshold
        if [ $SUDO_COUNT -gt $THRESHOLD ]; then
                # Send email notification
                echo "Threshold reached.. Mailing about - $USER"
                SUBJECT="Excessive sudo attempts by $USER"
                BODY="The user $USER has attempted to use sudo commands $SUDO_COUNT times."
                echo "$BODY" | mail -s "$SUBJECT" "$ADMIN_EMAIL"
        fi
done
```

```
ranslatePathList:2866: Failed to translate C:Users\MANIKANDAN J L\.cargo\bin
$ ls

manikandan@HPVICTUSMANI61:~$ vim dead.letter
manikandan@HPVICTUSMANI61:~$ cd scriipt
-bash: cd: scriipt: No such file or directory
manikandan@HPVICTUSMANI61:~$ cd script
manikandan@HPVICTUSMANI61:~/script$ ls
file.sh
manikandan@HPVICTUSMANI61:~/script$ vim file.sh
manikandan@HPVICTUSMANI61:~/script$ su coderacer
Password:
coderacer@HPVICTUSMANI61:/home/manikandan/script$ sudo -i
[sudo] password for coderacer:
coderacer is not in the sudoers file.  This incident will be reported.
coderacer@HPVICTUSMANI61:/home/manikandan/script$ sudo ls
[sudo] password for coderacer:
coderacer is not in the sudoers file.  This incident will be reported.
coderacer@HPVICTUSMANI61:/home/manikandan/script$ sudo -i
[sudo] password for coderacer:
coderacer is not in the sudoers file.  This incident will be reported.
coderacer@HPVICTUSMANI61:/home/manikandan/script$ sudo ls
[sudo] password for coderacer:
coderacer is not in the sudoers file.  This incident will be reported.
coderacer@HPVICTUSMANI61:/home/manikandan/script$ sudo -i
[sudo] password for coderacer:
coderacer is not in the sudoers file.  This incident will be reported.
coderacer@HPVICTUSMANI61:/home/manikandan/script$ exit
exit
manikandan@HPVICTUSMANI61:~/script$ sudo su
[sudo] password for manikandan:
root@HPVICTUSMANI61:/home/manikandan/script# ls
file.sh
root@HPVICTUSMANI61:/home/manikandan/script# bash file.sh
manikandan coderacer
Threshold reached.. Mailing about-coderacer
root@HPVICTUSMANI61:/home/manikandan/script#
```

M

manikandan2982004@gmail.com 13:53 (7 hours ago)

to root

HPVICTUSMANI61. : Sep 8 13:52:58 : coderacer : user NOT in sudoers ; TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/bin/bash