Round 1 : Linux Automation
Screen Captures

SECTION 1 :

1) ADDING A NEW USER ‘CODECYCLE’

```
janesh@janesh-VirtualBox:~$ sudo adduser codecycle
[sudo] password for janesh:
Sorry, try again.
[sudo] password for janesh:
info: Adding user `codecycle' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `codecycle' (1001) ...
info: Adding new user `codecycle' (1001) with group `codecycle (1001)' ...
info: Creating home directory `/home/codecycle' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for codecycle
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `codecycle' to supplemental / extra groups `users' ...
info: Adding user `codecycle' to group `users' ...
janesh@janesh-VirtualBox:~$ id codecycle
uid=1001(codecycle) gid=1001(codecycle) groups=1001(codecycle),100(users)
janesh@janesh-VirtualBox:~$
```

2) EXPLORING THE DIRECTORIES

```
janesh@janesh-VirtualBox:~$ pwd
/home/janesh
janesh@janesh-VirtualBox:~$ cd ../
janesh@janesh-VirtualBox:/home$ pwd
/home
janesh@janesh-VirtualBox:/home$ cd codecycle/
bash: cd: codecycle/: Permission denied
janesh@janesh-VirtualBox:/home$ whoami
janesh
janesh@janesh-VirtualBox:/home$ su codecycle
Password:
codecycle@janesh-VirtualBox:/home$ whoami
codecycle
codecycle@janesh-VirtualBox:/home$ pwd
/home
codecycle@janesh-VirtualBox:/home$ exit
exit
janesh@janesh-VirtualBox:/home$
```

3) EDITED MAIN.CF FILE

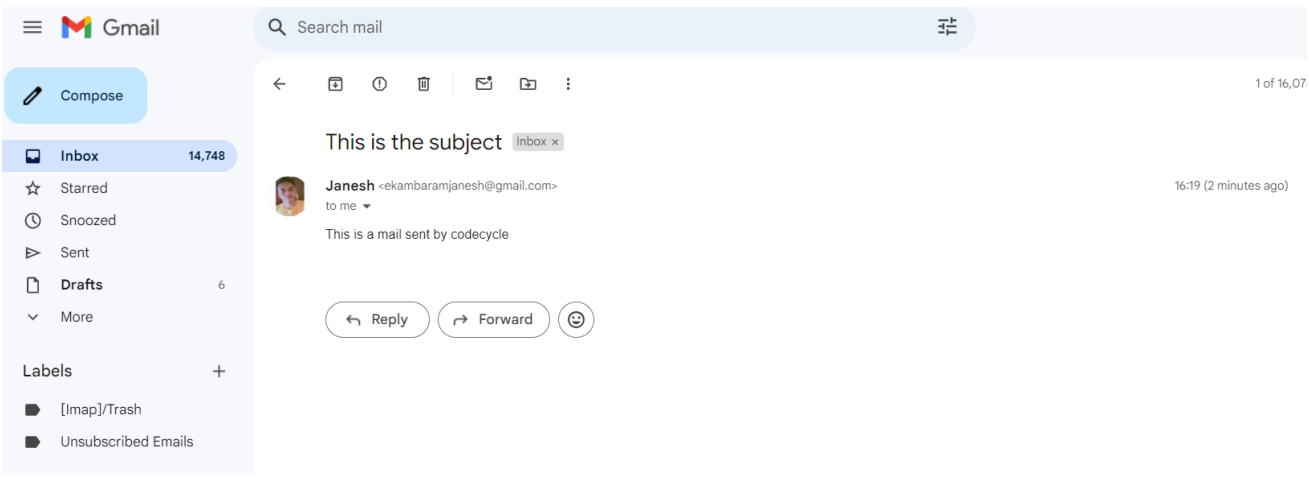
```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = janesh-VirtualBox
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, janesh-VirtualBox, localhost.localdomain, , localhost
relayhost = [smtp.gmail.com]:587
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
smtp_sasl_auth_enable = yes
smtp_tls_security_level = encrypt
smtp_sasl_security_options = noanonymous
```

4) WORKING WITH MAIN.CF AND SASL_PASSWORD FILES

```
janesh@janesh-VirtualBox:/$ sudo su
root@janesh-VirtualBox:/# cd /etc/postfix
root@janesh-VirtualBox:/etc/postfix# cp main.cf main.cf.bkp
root@janesh-VirtualBox:/etc/postfix# vim main.cf
root@janesh-VirtualBox:/etc/postfix# hostname
janesh-VirtualBox
root@janesh-VirtualBox:/etc/postfix# vim main.cf
root@janesh-VirtualBox:/etc/postfix# vim main.cf
root@janesh-VirtualBox:/etc/postfix# cd /etc/postfix/sasl/
root@janesh-VirtualBox:/etc/postfix/sasl# vim sasl_passwd
root@janesh-VirtualBox:/etc/postfix/sasl# vim main.cf
root@janesh-VirtualBox:/etc/postfix/sasl# cd /etc/postfix
root@janesh-VirtualBox:/etc/postfix# vim main.cf
root@janesh-VirtualBox:/etc/postfix# cd /etc/postfix/sasl/
root@janesh-VirtualBox:/etc/postfix/sasl# vim sasl_passwd
root@janesh-VirtualBox:/etc/postfix/sasl# postmap sasl_passwd
postmap: warning: /etc/postfix/main.cf, line 49: overriding earlier entry: smtp_tls_security_level=may
root@janesh-VirtualBox:/etc/postfix/sasl# chmod 600 sasl_passwd*
root@janesh-VirtualBox:/etc/postfix/sasl# ls
sasl_passwd  sasl_passwd.db
root@janesh-VirtualBox:/etc/postfix/sasl# cd /
root@janesh-VirtualBox:/# service postfix status
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: enabled)
     Active: active (exited) since Sun 2024-09-08 15:50:05 IST; 27min ago
       Docs: man:postfix(1)
    Process: 4750 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 4750 (code=exited, status=0/SUCCESS)
        CPU: 1ms
```

5) SENDING THE MAIL FROM THE TERMINAL AND CONFIRMING IN GMAIL

```
janesh@janesh-VirtualBox:/$ echo 'This is a mail sent by codecycle' | mail -s 'This is the subject' ekambaramjanesh@gmai
l.com
janesh@janesh-VirtualBox:/$
```



SECTION 2 :

1) CHECKING IF USER ‘CODECYCLE’ HAS SUDO PERMISSIONS

```
janesh@janesh-VirtualBox:/$ su codecycle
Password:
codecycle@janesh-VirtualBox:/$ cd
codecycle@janesh-VirtualBox:~$ sudo -i
[sudo] password for codecycle:
codecycle is not in the sudoers file.
This incident has been reported to the administrator.
codecycle@janesh-VirtualBox:~$ exit
exit
janesh@janesh-VirtualBox:/$
```

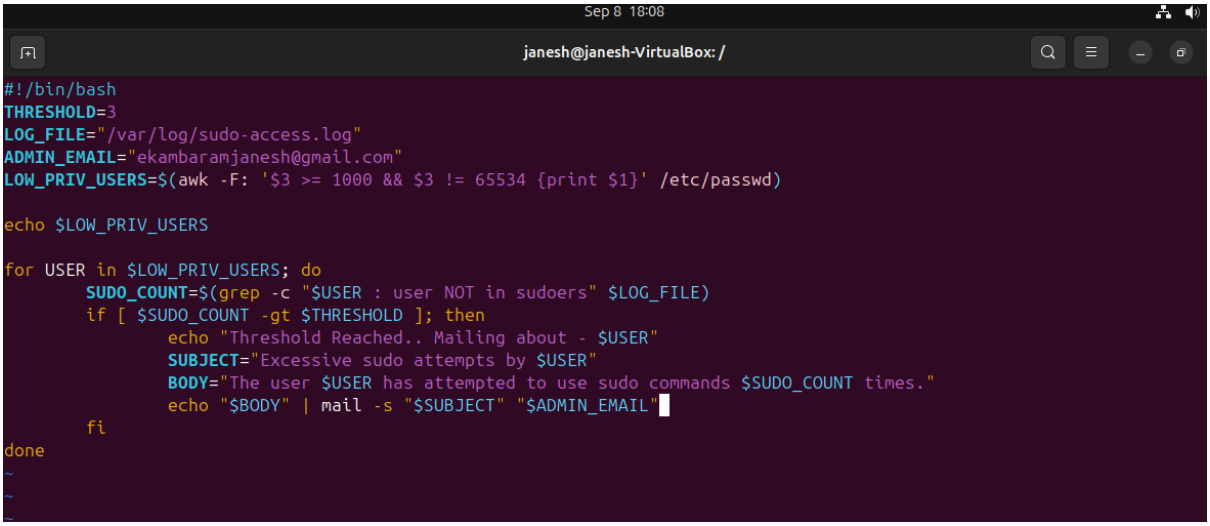
2) EDITING SUDOERS FILE

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
Defaults        logfile=/var/log/sudo-access.log
# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"
```

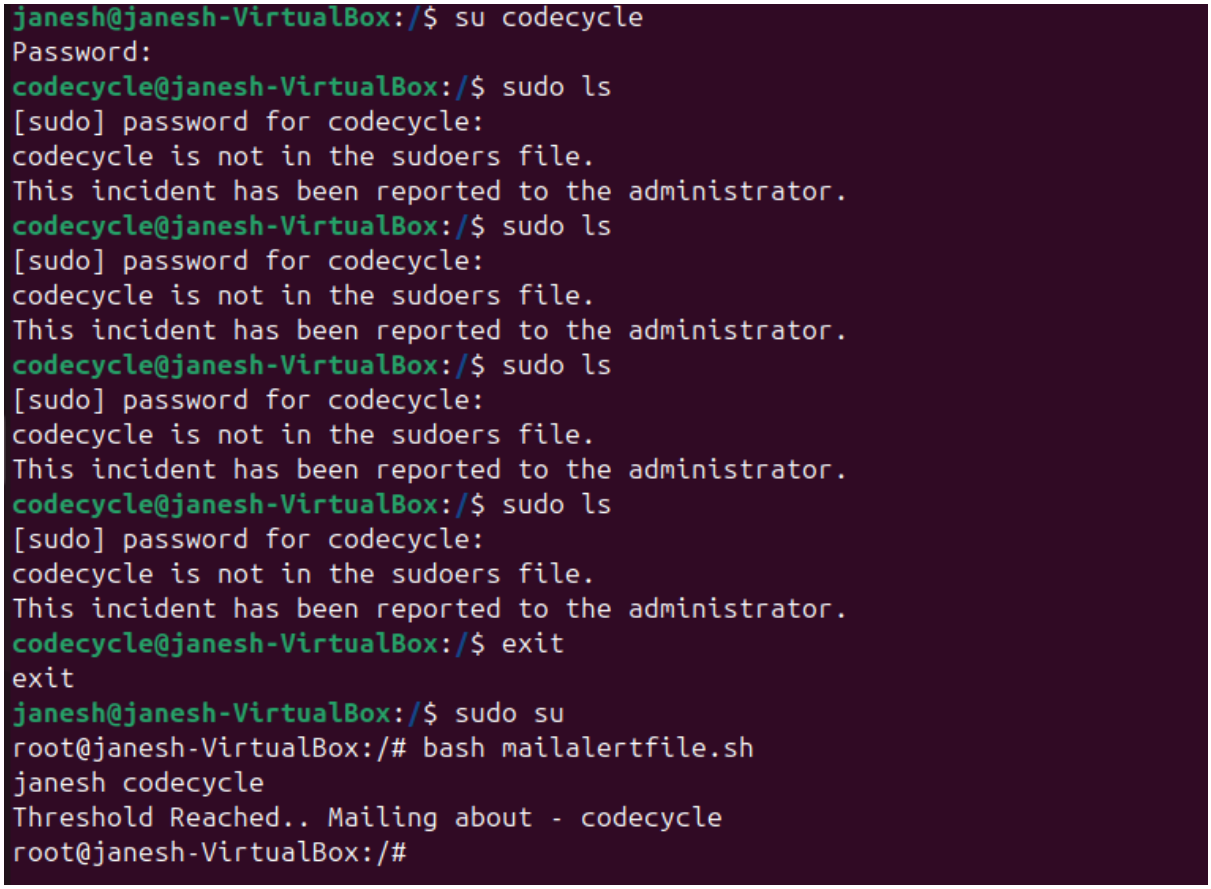
3) GETTING FILE LOGS

```
root@janesh-VirtualBox:~# ls /var/log/
alternatives.log  btmp                  dmesg            hp         openvpn            sysstat
apport.log        cloud-init.log        dpkg.log         installer  private            unattended-upgrades
apt               cloud-init-output.log faillog          journal    README             wtmp
auth.log          cups                  fontconfig.log   kern.log   speech-dispatcher
boot.log          cups-browsed          gdm3             lastlog    sssd
bootstrap.log     dist-upgrade          gpu-manager.log  mail.log   syslog
root@janesh-VirtualBox:~# exit
exit
janesh@janesh-VirtualBox:/$ sudo service postfix status
[sudo] password for janesh:
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: enabled)
     Active: active (exited) since Sun 2024-09-08 15:50:05 IST; 1h 3min ago
       Docs: man:postfix(1)
    Process: 4750 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 4750 (code=exited, status=0/SUCCESS)
        CPU: 1ms

Sep 08 15:50:05 janesh-VirtualBox systemd[1]: Starting postfix.service - Postfix Mail Transport Agent...
Sep 08 15:50:05 janesh-VirtualBox systemd[1]: Finished postfix.service - Postfix Mail Transport Agent.
janesh@janesh-VirtualBox:/$ sudo su
root@janesh-VirtualBox:/# cd
root@janesh-VirtualBox:~# ls /var/log/
alternatives.log  btmp                  dmesg            hp         openvpn            syslog
apport.log        cloud-init.log        dpkg.log         installer  private            sysstat
apt               cloud-init-output.log faillog          journal    README             unattended-upgrades
auth.log          cups                  fontconfig.log   kern.log   speech-dispatcher  wtmp
boot.log          cups-browsed          gdm3             lastlog    sssd
bootstrap.log     dist-upgrade          gpu-manager.log  mail.log   sudo-access.log
root@janesh-VirtualBox:~#
```

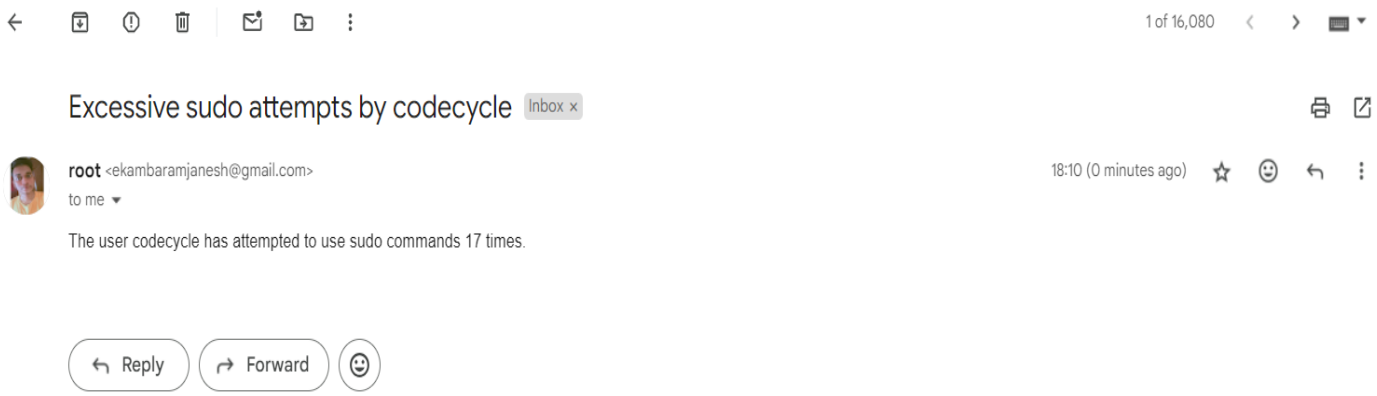
4) FILE TO WRITE LOGIC FOR MONITORING UNSUCCESSFUL SUDO ATTEMPTS (mailalerfile.sh)



5) SUDO ATTEMPTS BY ‘CODECYCLE’ USER :

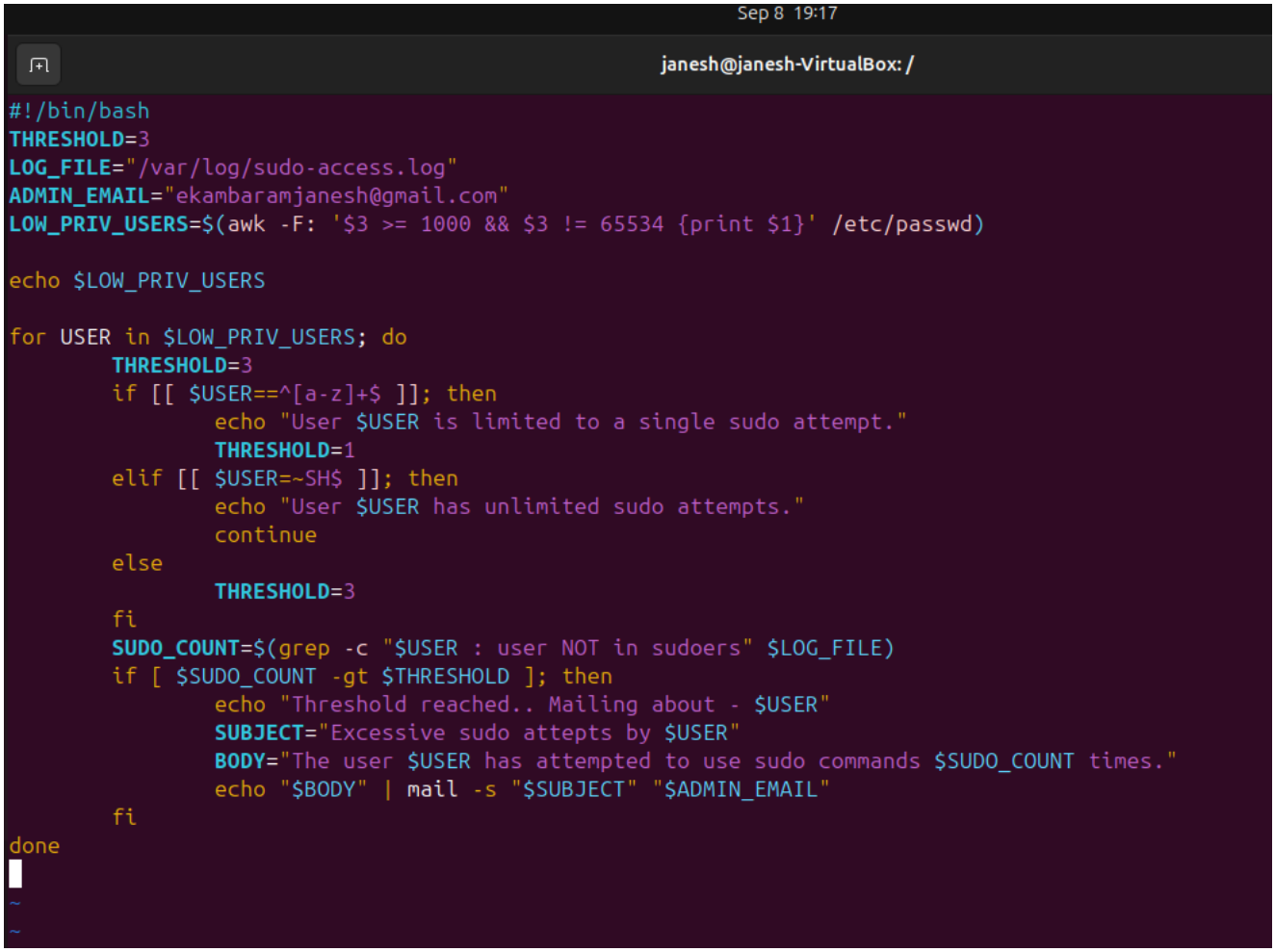


6) MAIL FOR ALERTING SUDO ATTEMPT:



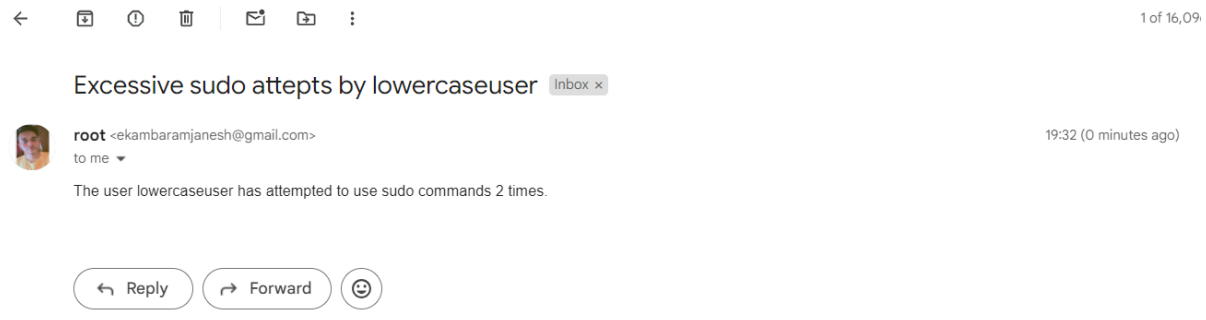
SECTION 3 :

1) bash file to allow all users with usernames ending with 'SH' to have unlimited sudo access attempts, while users not having any capital letters in their usernames are limited to a single attempt



```
janesh@janesh-VirtualBox:/$ sudo vim mailalertfile.sh
janesh@janesh-VirtualBox:/$ sudo su
root@janesh-VirtualBox:/# bash mailalertfile.sh
janesh codecycle lowercaseuser
User janesh is limited to a single sudo attempt.
User codecycle is limited to a single sudo attempt.
Threshold reached.. Mailing about - codecycle
User lowercaseuser is limited to a single sudo attempt.
root@janesh-VirtualBox:/# exit
exit
```

```
lowercaseuser@janesh-VirtualBox:/$ sudo ls
[sudo] password for lowercaseuser:
lowercaseuser is not in the sudoers file.
This incident has been reported to the administrator.
lowercaseuser@janesh-VirtualBox:/$ exit
exit
janesh@janesh-VirtualBox:/$ sudo su
root@janesh-VirtualBox:/# bash mailalertfile.sh
janesh codecycle lowercaseuser
User janesh is limited to a single sudo attempt.
User codecycle is limited to a single sudo attempt.
Threshold reached.. Mailing about - codecycle
User lowercaseuser is limited to a single sudo attempt.
root@janesh-VirtualBox:/# exit
exit
janesh@janesh-VirtualBox:/$ su lowercaseuser
Password:
lowercaseuser@janesh-VirtualBox:/$ sudo ls
[sudo] password for lowercaseuser:
lowercaseuser is not in the sudoers file.
This incident has been reported to the administrator.
lowercaseuser@janesh-VirtualBox:/$ exit
exit
janesh@janesh-VirtualBox:/$ sudo su
root@janesh-VirtualBox:/# bash mailalertfile.sh
janesh codecycle lowercaseuser
User janesh is limited to a single sudo attempt.
User codecycle is limited to a single sudo attempt.
Threshold reached.. Mailing about - codecycle
User lowercaseuser is limited to a single sudo attempt.
Threshold reached.. Mailing about - lowercaseuser
```



2) CRONTAB TO AUTOMATE THE PROCESS

```
  GNU nano 7.2                                  /tmp/crontab.2rfJ5c/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

0 0,4,8,12,16,20 * * * /mailalertfile.sh
```

```
janesh@janesh-VirtualBox:/$ crontab -e
crontab: installing new crontab
janesh@janesh-VirtualBox:/$ sudo service cron status
● cron.service - Regular background program processing daemon
     Loaded: loaded (/usr/lib/systemd/system/cron.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-09-08 15:31:34 IST; 4h 11min ago
       Docs: man:cron(8)
   Main PID: 952 (cron)
      Tasks: 1 (limit: 4615)
     Memory: 464.0K (peak: 2.3M)
        CPU: 578ms
     CGroup: /system.slice/cron.service
             └─952 /usr/sbin/cron -f -P

Sep 08 19:17:01 janesh-VirtualBox CRON[6674]: pam_unix(cron:session): session closed for user root
Sep 08 19:25:01 janesh-VirtualBox CRON[6698]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 19:25:01 janesh-VirtualBox CRON[6699]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Sep 08 19:25:01 janesh-VirtualBox CRON[6698]: pam_unix(cron:session): session closed for user root
Sep 08 19:30:01 janesh-VirtualBox CRON[6805]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 19:30:01 janesh-VirtualBox CRON[6806]: (root) CMD ([ -x /etc/init.d/anacron ] && if [ ! -d /run/systemd/system ]>
Sep 08 19:30:01 janesh-VirtualBox CRON[6805]: pam_unix(cron:session): session closed for user root
Sep 08 19:35:01 janesh-VirtualBox CRON[6913]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 19:35:01 janesh-VirtualBox CRON[6914]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Sep 08 19:35:01 janesh-VirtualBox CRON[6913]: pam_unix(cron:session): session closed for user root
...skipping...
```