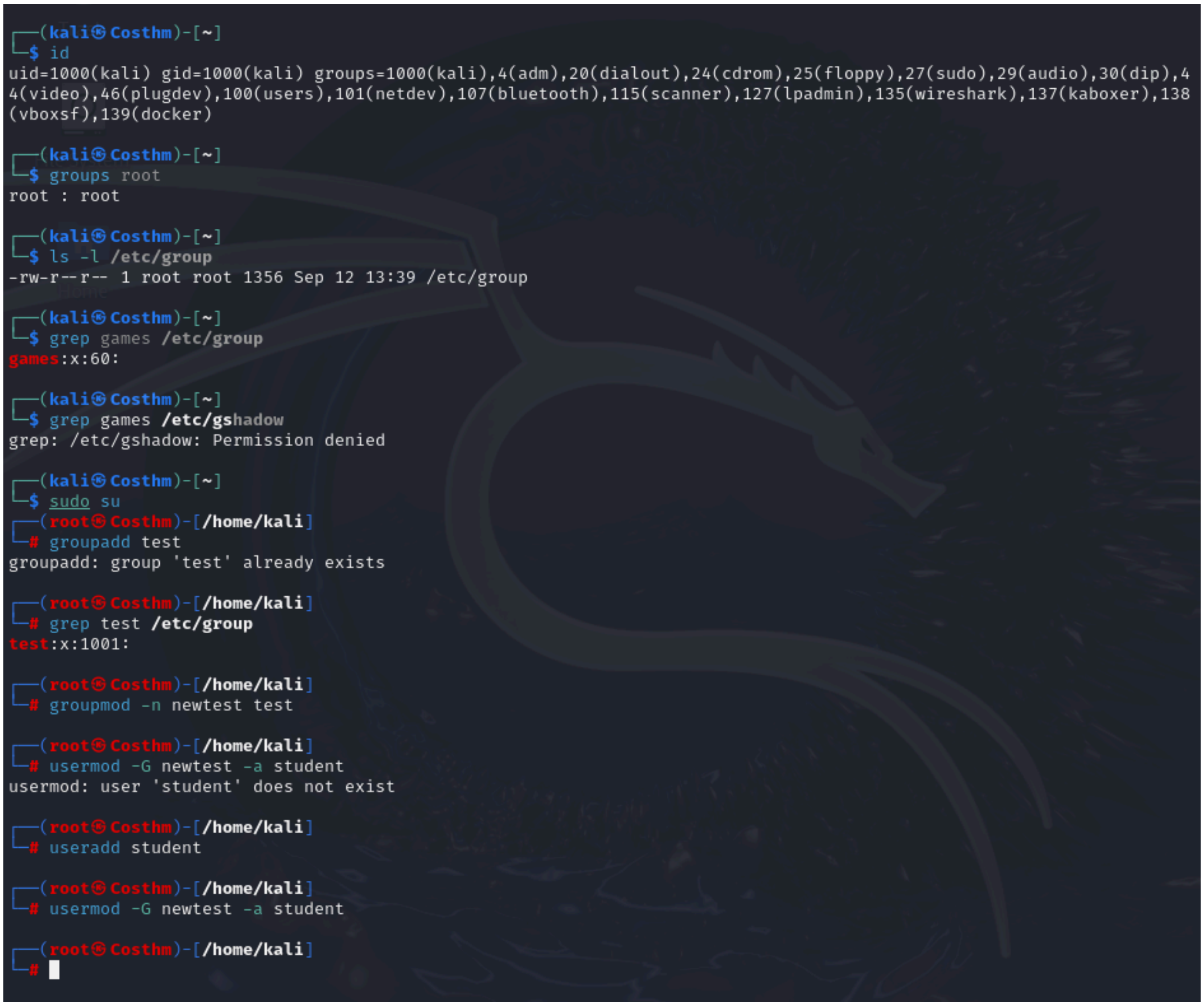
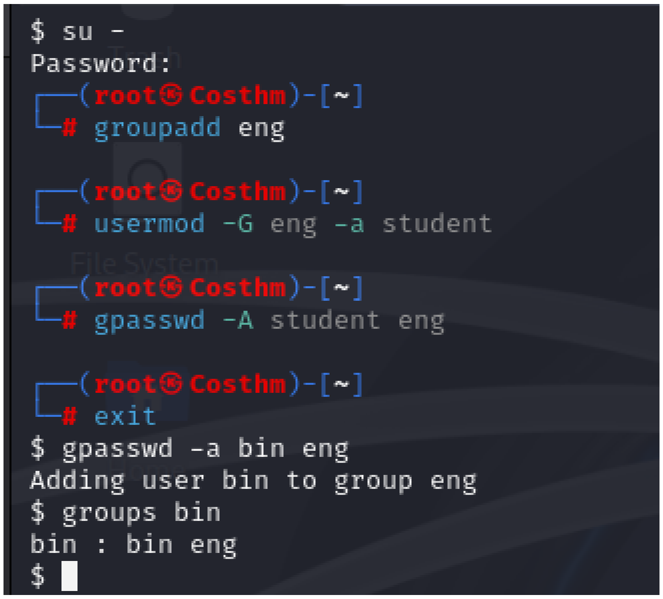
# Part A



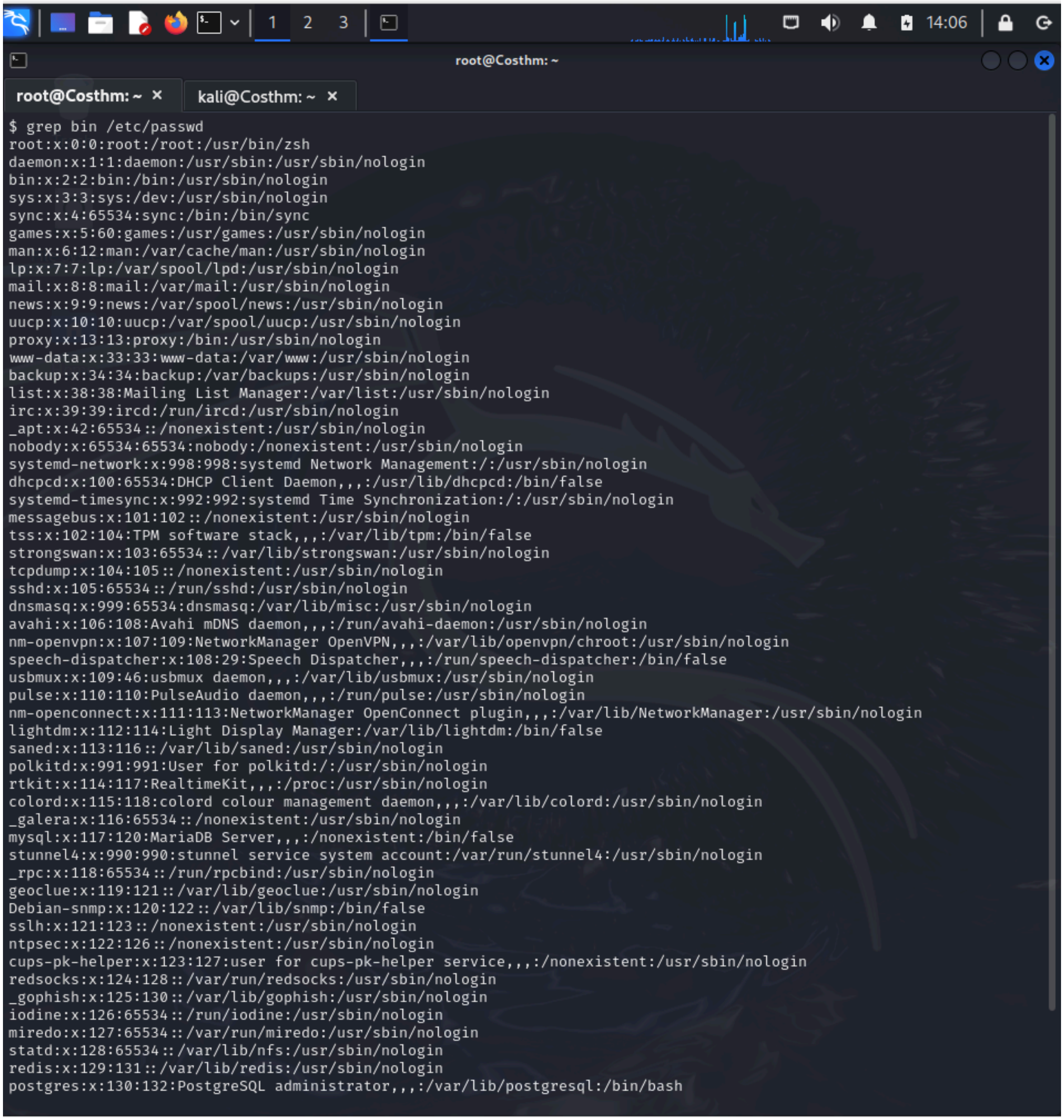
```
┌──(kali㉿Costhm)-[~]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),4
4(video),46(plugdev),100(users),101(netdev),107(bluetooth),115(scanner),127(lpadmin),135(wireshark),137(kaboxer),138
(vboxsf),139(docker)

┌──(kali㉿Costhm)-[~]
└─$ groups root
root : root

┌──(kali㉿Costhm)-[~]
└─$ ls -l /etc/group
-rw-r--r-- 1 root root 1356 Sep 12 13:39 /etc/group

┌──(kali㉿Costhm)-[~]
└─$ grep games /etc/group
games:x:60:

┌──(kali㉿Costhm)-[~]
└─$ grep games /etc/gshadow
grep: /etc/gshadow: Permission denied

┌──(kali㉿Costhm)-[~]
└─$ sudo su
┌──(root㉿Costhm)-[/home/kali]
└─# groupadd test
groupadd: group 'test' already exists

┌──(root㉿Costhm)-[/home/kali]
└─# grep test /etc/group
test:x:1001:

┌──(root㉿Costhm)-[/home/kali]
└─# groupmod -n newtest test

┌──(root㉿Costhm)-[/home/kali]
└─# usermod -G newtest -a student
usermod: user 'student' does not exist

┌──(root㉿Costhm)-[/home/kali]
└─# useradd student

┌──(root㉿Costhm)-[/home/kali]
└─# usermod -G newtest -a student

┌──(root㉿Costhm)-[/home/kali]
└─# 
```

# Part B

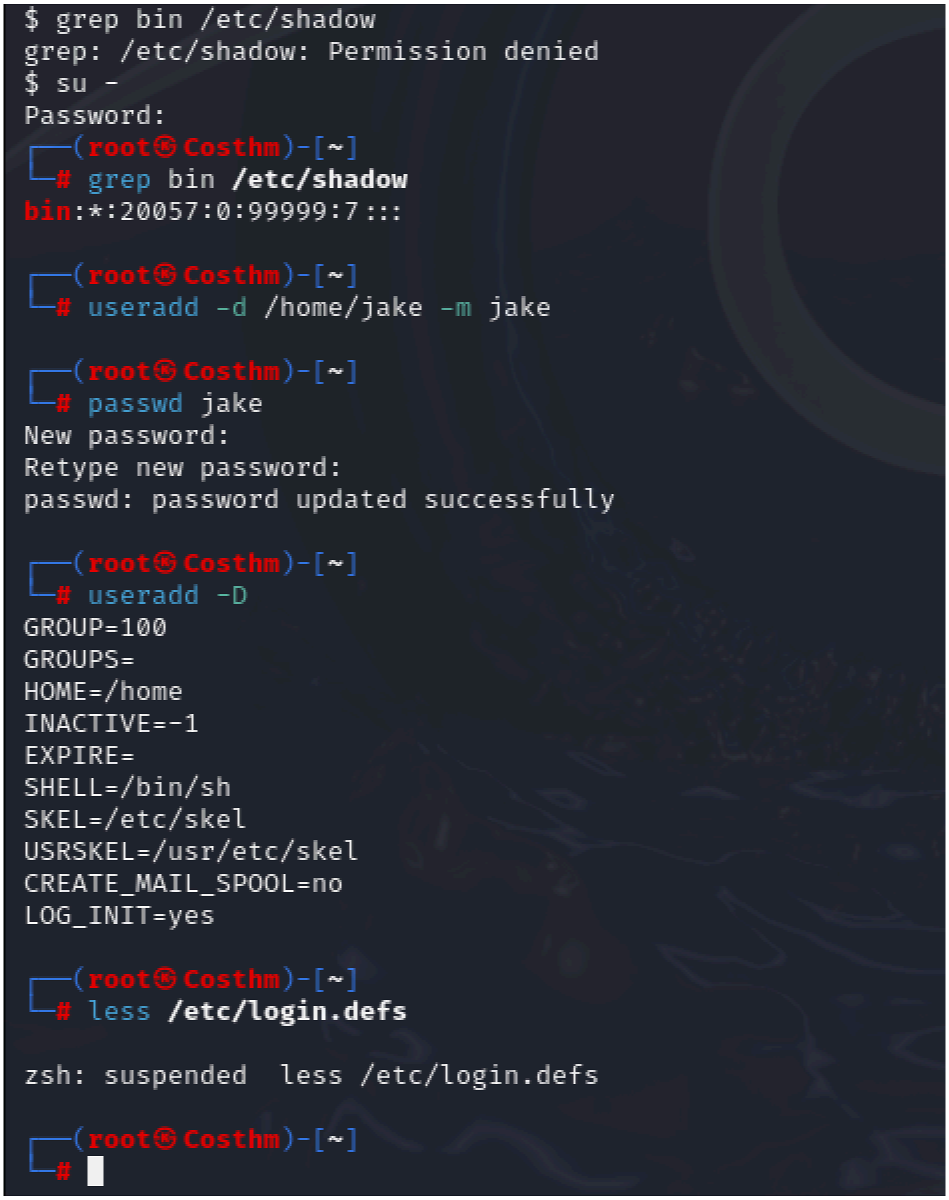


```
$ su -
Password:
┌──(root㉿Costhm)-[~]
└─# groupadd eng

┌──(root㉿Costhm)-[~]
└─# usermod -G eng -a student

┌──(root㉿Costhm)-[~]
└─# gpasswd -A student eng

┌──(root㉿Costhm)-[~]
└─# exit
$ gpasswd -a bin eng
Adding user bin to group eng
$ groups bin
bin : bin eng
$ █
```

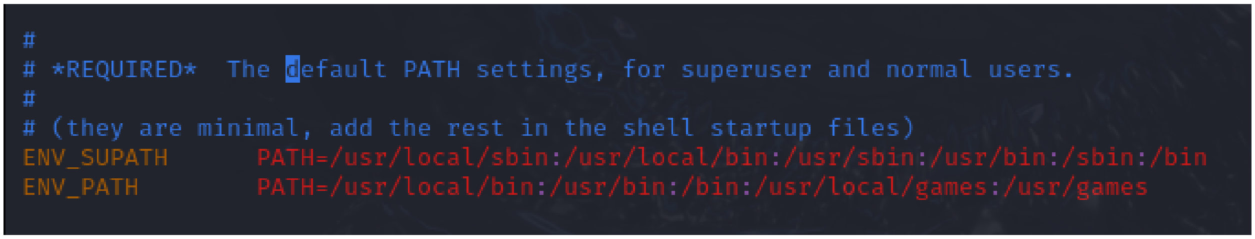
# Part C



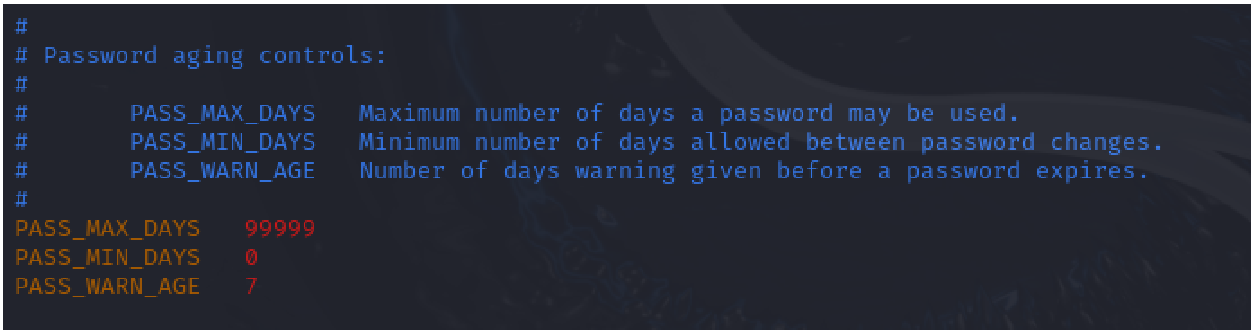
```
$ grep bin /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
pulse:x:110:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
nm-openconnect:x:111:113:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
lightdm:x:112:114:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
rtkit:x:114:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:115:118:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
_galera:x:116:65534::/nonexistent:/usr/sbin/nologin
mysql:x:117:120:MariaDB Server,,,:/nonexistent:/bin/false
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:118:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:119:121::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:120:122::/var/lib/snmp:/bin/false
sslh:x:121:123::/nonexistent:/usr/sbin/nologin
ntpsec:x:122:126::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:123:127:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
redsocks:x:124:128::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:125:130::/var/lib/gophish:/usr/sbin/nologin
iodine:x:126:65534::/run/iodine:/usr/sbin/nologin
miredo:x:127:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:128:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:129:131::/var/lib/redis:/usr/sbin/nologin
postgres:x:130:132:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```



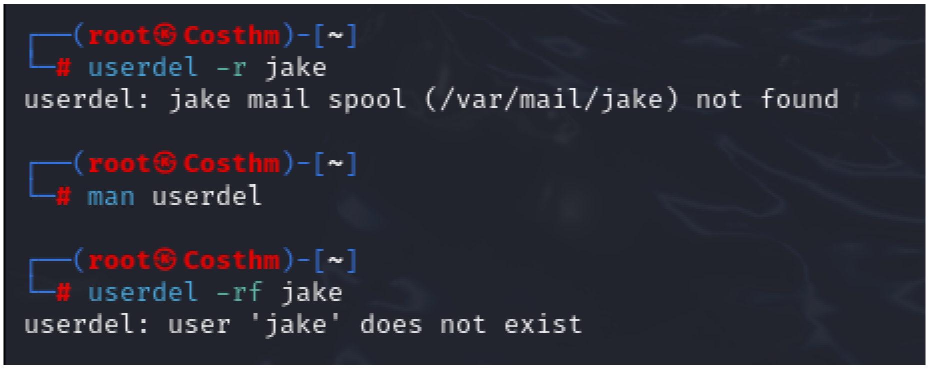
```
$ grep bin /etc/shadow
grep: /etc/shadow: Permission denied
$ su -
Password:
┌──(root㉿Costhm)-[~]
└─# grep bin /etc/shadow
bin:*:20057:0:99999:7:::

┌──(root㉿Costhm)-[~]
└─# useradd -d /home/jake -m jake

┌──(root㉿Costhm)-[~]
└─# passwd jake
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿Costhm)-[~]
└─# useradd -D
GROUP=100
GROUPS=
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
USRSKEL=/usr/etc/skel
CREATE_MAIL_SPOOL=no
LOG_INIT=yes

┌──(root㉿Costhm)-[~]
└─# less /etc/login.defs

zsh: suspended  less /etc/login.defs

┌──(root㉿Costhm)-[~]
└─# 
```



```
#
# *REQUIRED*  The default PATH settings, for superuser and normal users.
#
# (they are minimal, add the rest in the shell startup files)
ENV_SUPATH      PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
ENV_PATH        PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

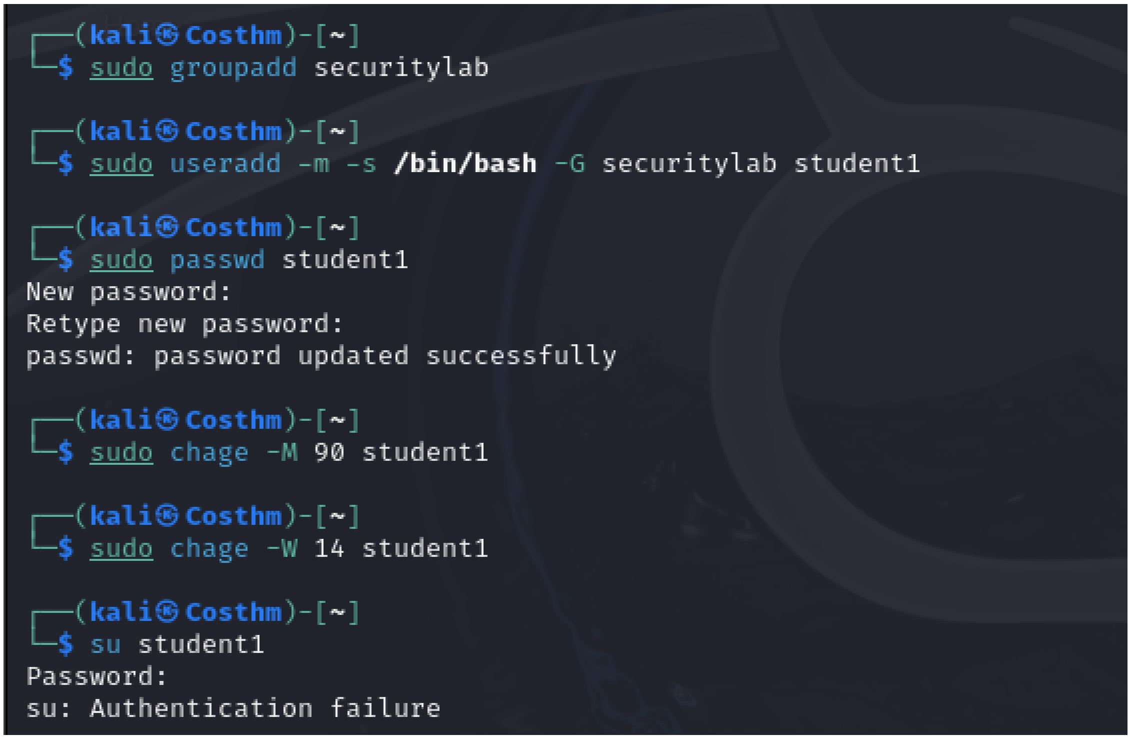


```
#
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

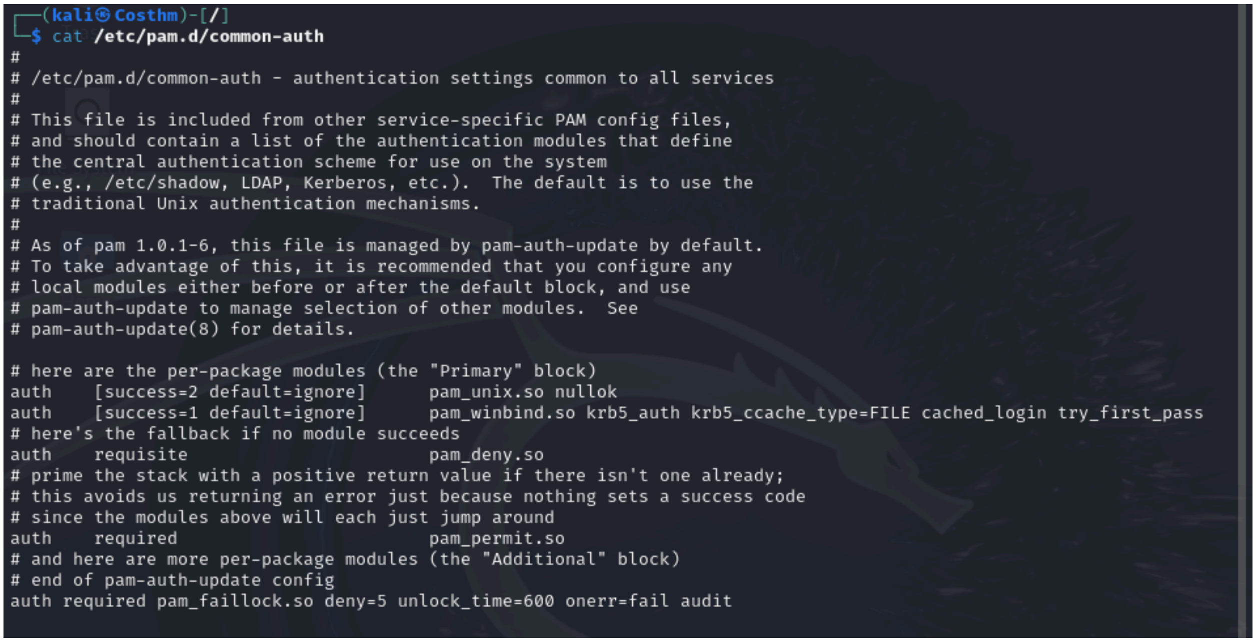


```
┌──(root㉿Costhm)-[~]
└─# userdel -r jake
userdel: jake mail spool (/var/mail/jake) not found

┌──(root㉿Costhm)-[~]
└─# man userdel

┌──(root㉿Costhm)-[~]
└─# userdel -rf jake
userdel: user 'jake' does not exist
```

# Part D

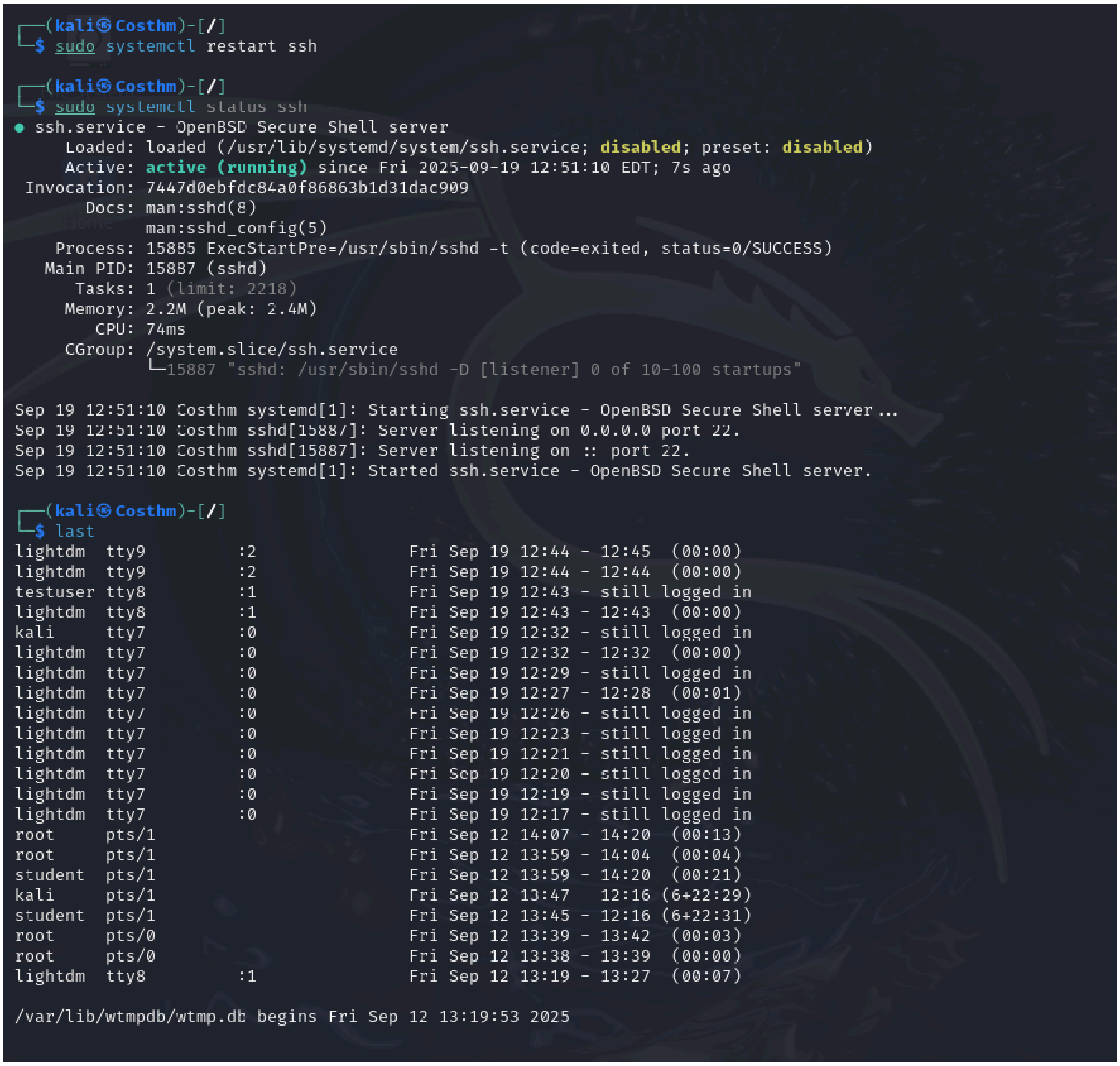


```
┌──(kali㉿Costhm)-[~]
└─$ sudo groupadd securitylab

┌──(kali㉿Costhm)-[~]
└─$ sudo useradd -m -s /bin/bash -G securitylab student1

┌──(kali㉿Costhm)-[~]
└─$ sudo passwd student1
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿Costhm)-[~]
└─$ sudo chage -M 90 student1

┌──(kali㉿Costhm)-[~]
└─$ sudo chage -W 14 student1

┌──(kali㉿Costhm)-[~]
└─$ su student1
Password:
su: Authentication failure
```

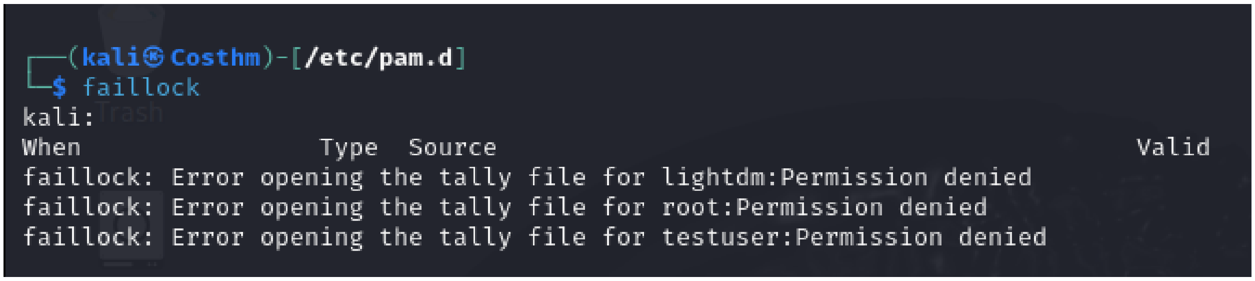


```
┌──(kali㉿Costhm)-[/]
└─$ cat /etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=2 default=ignore]      pam_unix.so nullok
auth    [success=1 default=ignore]      pam_winbind.so krb5_auth krb5_ccache_type=FILE cached_login try_first_pass
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
auth required pam_faillock.so deny=5 unlock_time=600 onerr=fail audit
```

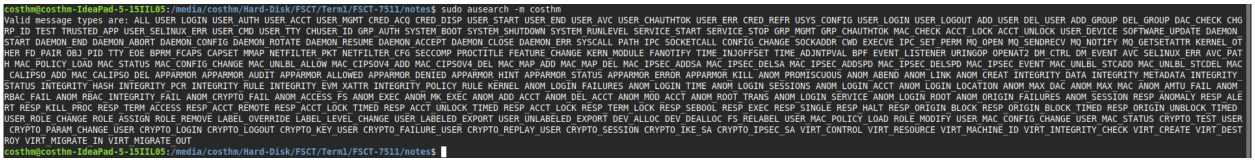
Pam_tally2 is deprecated, using faillock here instead
In theory, this setup should lock my account up for 600 seconds (10 minutes) if I fail to enter the password 5 times in a row, and it would be logged in the audit file `/var/log/auth.log`



```
┌──(kali㉿Costhm)-[/]
└─$ sudo systemctl restart ssh

┌──(kali㉿Costhm)-[/]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2025-09-19 12:51:10 EDT; 7s ago
 Invocation: 7447d0ebfdc84a0f86863b1d31dac909
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 15885 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 15887 (sshd)
      Tasks: 1 (limit: 2218)
     Memory: 2.2M (peak: 2.4M)
        CPU: 74ms
     CGroup: /system.slice/ssh.service
             └─15887 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 19 12:51:10 Costhm systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 19 12:51:10 Costhm sshd[15887]: Server listening on 0.0.0.0 port 22.
Sep 19 12:51:10 Costhm sshd[15887]: Server listening on :: port 22.
Sep 19 12:51:10 Costhm systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

┌──(kali㉿Costhm)-[/]
└─$ last
lightdm  tty9         :2                Fri Sep 19 12:44 - 12:45  (00:00)
lightdm  tty9         :2                Fri Sep 19 12:44 - 12:44  (00:00)
testuser tty8         :1                Fri Sep 19 12:43 - still logged in
lightdm  tty8         :1                Fri Sep 19 12:43 - 12:43  (00:00)
kali     tty7         :0                Fri Sep 19 12:32 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:32 - 12:32  (00:00)
lightdm  tty7         :0                Fri Sep 19 12:29 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:27 - 12:28  (00:01)
lightdm  tty7         :0                Fri Sep 19 12:26 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:23 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:21 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:20 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:19 - still logged in
lightdm  tty7         :0                Fri Sep 19 12:17 - still logged in
root     pts/1                          Fri Sep 12 14:07 - 14:20  (00:13)
root     pts/1                          Fri Sep 12 13:59 - 14:04  (00:04)
student  pts/1                          Fri Sep 12 13:59 - 14:20  (00:21)
kali     pts/1                          Fri Sep 12 13:47 - 12:16 (6+22:29)
student  pts/1                          Fri Sep 12 13:45 - 12:16 (6+22:31)
root     pts/0                          Fri Sep 12 13:39 - 13:42  (00:03)
root     pts/0                          Fri Sep 12 13:38 - 13:39  (00:00)
lightdm  tty8         :1                Fri Sep 12 13:19 - 13:27  (00:07)

/var/lib/wtmpdb/wtmp.db begins Fri Sep 12 13:19:53 2025
```



```
┌──(kali㉿Costhm)-[/etc/pam.d]
└─$ faillock
kali:
When                Type  Source                                           Valid
faillock: Error opening the tally file for lightdm:Permission denied
faillock: Error opening the tally file for root:Permission denied
faillock: Error opening the tally file for testuser:Permission denied
```



```
costhm@costhm-IdeaPad-5-15IIL05:/media/costhm/Hard-Disk/FSCT/Term1/FSCT-7511/notes$ sudo ausearch -m costhm
Valid message types are: ALL USER_LOGIN USER_AUTH USER_ACCT USER_MGMT CRED_ACQ CRED_DISP USER_START USER_END USER_AVC USER_CHAUTHTOK USER_ERR CRED_REFR USYS_CONFIG USER_LOGIN USER_LOGOUT ADD_USER DEL_USER ADD_GROUP DEL_GROUP DAC_CHECK CHG
RP_ID TEST TRUSTED_APP USER_SELINUX_ERR USER_CMD USER_TTY CHUSER_ID GRP_AUTH SYSTEM_BOOT SYSTEM_SHUTDOWN SYSTEM_RUNLEVEL SERVICE_START SERVICE_STOP GRP_MGMT GRP_CHAUTHTOK MAC_CHECK ACCT_LOCK ACCT_UNLOCK USER_DEVICE SOFTWARE_UPDATE DAEMON_
START DAEMON_END DAEMON_ABORT DAEMON_CONFIG DAEMON_ROTATE DAEMON_RESUME DAEMON_ACCEPT DAEMON_CLOSE DAEMON_ERR SYSCALL PATH IPC SOCKETCALL CONFIG_CHANGE SOCKADDR CWD EXECVE IPC_SET_PERM MQ_OPEN MQ_SENDRECV MQ_NOTIFY MQ_GETSETATTR KERNEL_OT
HER FD_PAIR OBJ_PID TTY EOE BPRM_FCAPS CAPSET MMAP NETFILTER_PKT NETFILTER_CFG SECCOMP PROCTITLE FEATURE_CHANGE KERN_MODULE FANOTIFY TIME_INJOFFSET TIME_ADJNTPVAL BPF EVENT_LISTENER URINGOP OPENAT2 DM_CTRL DM_EVENT AVC SELINUX_ERR AVC_PAT
H MAC_POLICY_LOAD MAC_STATUS MAC_CONFIG_CHANGE MAC_UNLBL_ALLOW MAC_CIPSOV4_ADD MAC_CIPSOV4_DEL MAC_MAP_ADD MAC_MAP_DEL MAC_IPSEC_ADDSA MAC_IPSEC_DELSA MAC_IPSEC_ADDSPD MAC_IPSEC_DELSPD MAC_IPSEC_EVENT MAC_UNLBL_STCADD MAC_UNLBL_STCDEL MAC
_CALIPSO_ADD MAC_CALIPSO_DEL APPARMOR APPARMOR_AUDIT APPARMOR_ALLOWED APPARMOR_DENIED APPARMOR_HINT APPARMOR_STATUS APPARMOR_ERROR APPARMOR_KILL ANOM_PROMISCUOUS ANOM_ABEND ANOM_LINK ANOM_CREAT INTEGRITY_DATA INTEGRITY_METADATA INTEGRITY_
STATUS INTEGRITY_HASH INTEGRITY_PCR INTEGRITY_RULE INTEGRITY_EVM_XATTR INTEGRITY_POLICY_RULE KERNEL ANOM_LOGIN_FAILURES ANOM_LOGIN_TIME ANOM_LOGIN_SESSIONS ANOM_LOGIN_ACCT ANOM_LOGIN_LOCATION ANOM_MAX_DAC ANOM_MAX_MAC ANOM_AMTU_FAIL ANOM_
RBAC_FAIL ANOM_RBAC_INTEGRITY_FAIL ANOM_CRYPTO_FAIL ANOM_ACCESS_FS ANOM_EXEC ANOM_MK_EXEC ANOM_ADD_ACCT ANOM_DEL_ACCT ANOM_MOD_ACCT ANOM_ROOT_TRANS ANOM_LOGIN_SERVICE ANOM_LOGIN_ROOT ANOM_ORIGIN_FAILURES ANOM_SESSION RESP_ANOMALY RESP_ALE
RT RESP_KILL_PROC RESP_TERM_ACCESS RESP_ACCT_REMOTE RESP_ACCT_LOCK_TIMED RESP_ACCT_UNLOCK_TIMED RESP_ACCT_LOCK RESP_TERM_LOCK RESP_SEBOOL RESP_EXEC RESP_SINGLE RESP_HALT RESP_ORIGIN_BLOCK RESP_ORIGIN_BLOCK_TIMED RESP_ORIGIN_UNBLOCK_TIMED 
USER_ROLE_CHANGE ROLE_ASSIGN ROLE_REMOVE LABEL_OVERRIDE LABEL_LEVEL_CHANGE USER_LABELED_EXPORT USER_UNLABELED_EXPORT DEV_ALLOC DEV_DEALLOC FS_RELABEL USER_MAC_POLICY_LOAD ROLE_MODIFY USER_MAC_CONFIG_CHANGE USER_MAC_STATUS CRYPTO_TEST_USER
 CRYPTO_PARAM_CHANGE_USER CRYPTO_LOGIN CRYPTO_LOGOUT CRYPTO_KEY_USER CRYPTO_FAILURE_USER CRYPTO_REPLAY_USER CRYPTO_SESSION CRYPTO_IKE_SA CRYPTO_IPSEC_SA VIRT_CONTROL VIRT_RESOURCE VIRT_MACHINE_ID VIRT_INTEGRITY_CHECK VIRT_CREATE VIRT_DEST
ROY VIRT_MIGRATE_IN VIRT_MIGRATE_OUT
costhm@costhm-IdeaPad-5-15IIL05:/media/costhm/Hard-Disk/FSCT/Term1/FSCT-7511/notes$ 
```