USER AND GROUPS

Rahul M Menon
CB.EN.P2CYS23015

User Information

```
[08/15/23]seed@VM:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
```

Every user information is listed here

Password Information

```
[08/15/23]seed@VM:~$ sudo cat /etc/shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
avahi-autoipd:*:18474:0:99999:7:::
usbmux:*:18474:0:99999:7:::
rtkit:*:18474:0:99999:7:::
dnsmasq:*:18474:0:99999:7:::
cups-pk-helper:*:18474:0:99999:7:::
speech-dispatcher:!:18474:0:99999:7:::
avahi:*:18474:0:99999:7:::
kernoops:*:18474:0:99999:7:::
```

Only root user can access shadow files hence sudo must be used.

$ls-1/etc/passwd/etc/shadow

```
[08/15/23]seed@VM:~$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root   2886 Nov 24  2020 /etc/passwd
-rw-r----- 1 root shadow 1514 Nov 24  2020 /etc/shadow
```

$id – userid, groupid and group info

```
[08/15/23]seed@VM:~$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(di
p),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
```

Add user

```
[08/15/23]seed@VM:~$ sudo adduser bob
Adding user `bob' ...
Adding new group `bob' (1001) ...
Adding new user `bob' (1001) with group `bob' ...
Creating home directory `/home/bob' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for bob
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
[08/15/23]seed@VM:~$
```

Su bob

```
[08/15/23]seed@VM:~$ su bob
Password:
bob@VM:/home/seed$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root   2926 Aug 15 13:05 /etc/passwd
-rw-r----- 1 root shadow 1644 Aug 15 13:08 /etc/shadow
bob@VM:/home/seed$ passwd
Changing password for bob.
Current password:
New password:
Retype new password:
Bad: new password is too simple
New password:
Retype new password:
Bad: new password is too simple
New password:
Retype new password:
passwd: password updated successfully
bob@VM:/home/seed$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root   2926 Aug 15 13:05 /etc/passwd
-rw-r----- 1 root shadow 1644 Aug 15 13:11 /etc/shadow
bob@VM:/home/seed$
```

```
bob@VM:/home/seed$ sudo cat /etc/shadow
[sudo] password for bob:
bob is not in the sudoers file.  This incident will be reported.
```

Group

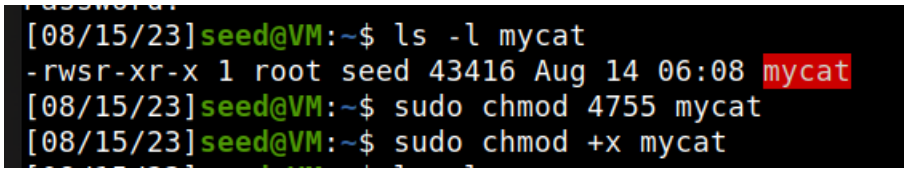
```
bob@VM:/home/seed$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,seed
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:seed
floppy:x:25:
tape:x:26:
sudo:x:27:seed
audio:x:29:pulse
dip:x:30:seed
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:telnetd
video:x:44:
sasl:x:45:
plugdev:x:46:seed
staff:x:50:
```

```
crontab:x:105:
messagebus:x:106:
input:x:107:
kvm:x:108:
render:x:109:
syslog:x:110:
tss:x:111:
bluetooth:x:112:
ssl-cert:x:113:
uuidd:x:114:
tcpdump:x:115:
avahi-autoipd:x:116:
rtkit:x:117:
ssh:x:118:
netdev:x:119:
lpadmin:x:120:seed
avahi:x:121:
scanner:x:122:saned
saned:x:123:
nm-openvpn:x:124:
whoopsie:x:125:
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
lxd:x:131:seed
seed:x:1000:
sambashare:x:132:seed
systemd-coredump:x:999:
vboxsf:x:133:
telnetd:x:134:
ftp:x:135:
docker:x:136:seed
bob:x:1001:
```

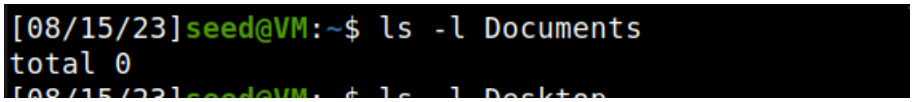
ls -l

```
bob@VM:/home/seed$ ls -l
total 76
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Desktop
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Documents
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Downloads
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Music
-rwsr-xr-x 1 root seed 43416 Aug 14 06:08 mycat
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Pictures
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Public
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Templates
drwxr-xr-x 2 seed seed  4096 Nov 24  2020 Videos
```

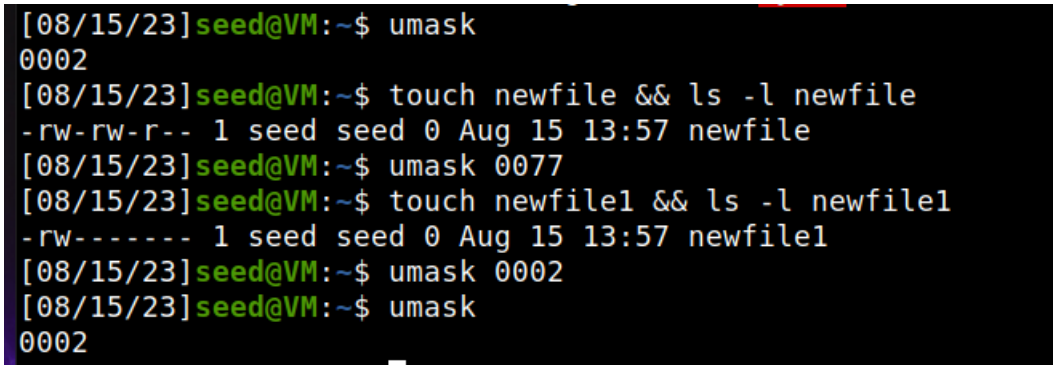
Ls -l mycat



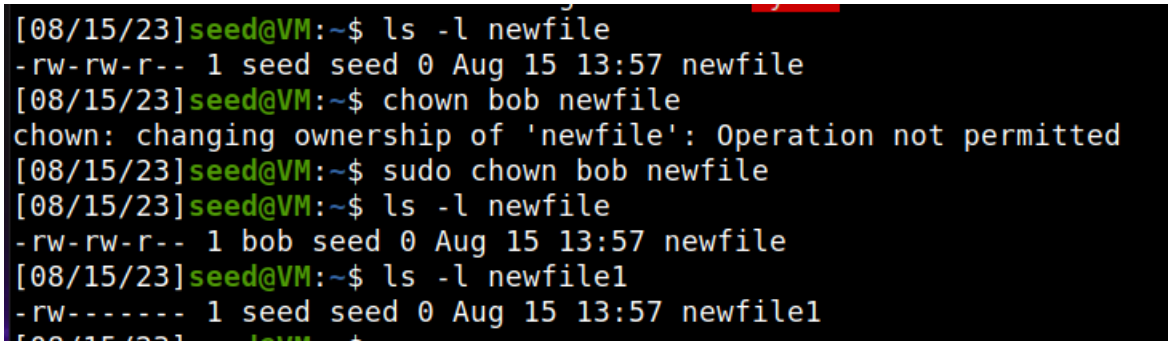
Permission on directories



Default Permissions



Change Ownership



Full Access Control list

```
[08/15/23]seed@VM:~$ getfacl newfile1
# file: newfile1
# owner: seed
# group: seed
user::rw-
group::---
other::---
```

```
[08/15/23]seed@VM:~$ sudo setfacl -m user:bob:r newfile1
[08/15/23]seed@VM:~$ getfacl newfile1
# file: newfile1
# owner: seed
# group: seed
user::rw-
user:bob:r--
group::---
mask::r--
other::---
```

Run command as another user

```
[08/15/23]seed@VM:~$ whoami
seed
[08/15/23]seed@VM:~$ sudo -u bob whoami
bob
```

Superuser Privileges

```
[08/15/23]seed@VM:~$ head /etc/shadow
head: cannot open '/etc/shadow' for reading: Permission denied
[08/15/23]seed@VM:~$ sudo head /etc/shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
```

Sudo Configuration File