Name : Mohammed Tousif
Roll : CB.EN.P2CYS22008

SECURE CODING - V
USERS & GROUPS

User Information

/etc/passwd

/etc/passwd file used to keep track of every user that can access the system

```
tousif@TousifVM:~$ 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:/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
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
```

Password Information

sudo cat /etc/shadow

/etc/shadow file contains the password information.

```
tousif@TousifVM:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
tousif@TousifVM:~$ sudo cat /etc/shadow
[sudo] password for tousif:
root:!:19255:0:99999:7:::
daemon:*:19213:0:99999:7:::
bin:*:19213:0:99999:7:::
sys:*:19213:0:99999:7:::
sync:*:19213:0:99999:7:::
games:*:19213:0:99999:7:::
man:*:19213:0:99999:7:::
lp:*:19213:0:99999:7:::
mail:*:19213:0:99999:7:::
news:*:19213:0:99999:7:::
uucp:*:19213:0:99999:7:::
proxy:*:19213:0:99999:7:::
www-data:*:19213:0:99999:7:::
backup:*:19213:0:99999:7:::
list:*:19213:0:99999:7:::
irc:*:19213:0:99999:7:::
gnats:*:19213:0:99999:7:::
nobody:*:19213:0:99999:7:::
systemd-network:*:19213:0:99999:7:::
```

ls -l /etc/passwd /etc/shadow
cat /etc/shadow
sudo cat /etc/shadow
id

```
tousif@TousifVM:~$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root   2822 Sep 20 22:53 /etc/passwd
-rw-r----- 1 root shadow 1430 Sep 20 22:53 /etc/shadow
tousif@TousifVM:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
tousif@TousifVM:~$ id
uid=1000(tousif) gid=1000(tousif) groups=1000(tousif),4(adm),24(cdrom),27(sudo),30(dip),46(plugd
ev),122(lpadmin),134(lxd),135(sambashare)
tousif@TousifVM:~$
```

Permission is denied

Adding a new user
sudo adduser <username>

```
tousif@TousifVM:~$ sudo adduser dupuser
Adding user `dupuser' ...
Adding new group `dupuser' (1001) ...
Adding new user `dupuser' (1001) with group `dupuser' ...
Creating home directory `/home/dupuser' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for dupuser
Enter the new value, or press ENTER for the default
        Full Name []: Duplicate User
        Room Number []: 13
        Work Phone []: 123456789
        Home Phone []: 987654321
        Other []: none
Is the information correct? [Y/n] y
tousif@TousifVM:~$
```

Switch user
su dupuser
Change password
passwd

```
tousif@TousifVM:~$ su dupuser
Password:
dupuser@TousifVM:/home/tousif$ id
uid=1001(dupuser) gid=1001(dupuser) groups=1001(dupuser)
dupuser@TousifVM:/home/tousif$ passwd
Changing password for dupuser.
Current password:
New password:
Retype new password:
passwd: password updated successfully
dupuser@TousifVM:/home/tousif$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root   2909 Oct 11 12:11 /etc/passwd
-rw-r----- 1 root shadow 1531 Oct 11 12:14 /etc/shadow
dupuser@TousifVM:/home/tousif$
```

Groups
cat /etc/group
Group details are available in /etc/group.

```
dupuser@TousifVM:/home/tousif$ cat /etc/group | tail
colord:x:129:
geoclue:x:130:
pulse:x:131:
pulse-access:x:132:
gdm:x:133:
lxd:x:134:tousif
tousif:x:1000:
sambashare:x:135:tousif
plocate:x:136:
dupuser:x:1001:
dupuser@TousifVM:/home/tousif$
```

Change permissions
chmod 640 file
Binary to decimal - 110 | 100 | 000 = 6 | 4 | 0.
rw- | r-- | ---

```
tousif@TousifVM:~/Documents$ ls -l file1.txt
-rw-rw-r-- 1 tousif tousif 77 Oct  9 10:49 file1.txt
tousif@TousifVM:~/Documents$ chmod 000 file1.txt
tousif@TousifVM:~/Documents$ ls -l file1.txt
---------- 1 tousif tousif 77 Oct  9 10:49 file1.txt
tousif@TousifVM:~/Documents$ chmod 664 file1.txt
tousif@TousifVM:~/Documents$ ls -l file1.txt
-rw-rw-r-- 1 tousif tousif 77 Oct  9 10:49 file1.txt
tousif@TousifVM:~/Documents$
```

Permissions of directories
ls -l dirname
The first bit (d) represents the directory bit.

```
tousif@TousifVM:~$ ls -l
total 40
drwxr-xr-x 2 tousif tousif 4096 Oct 11 10:16 Desktop
drwxr-xr-x 2 tousif tousif 4096 Oct 10 22:05 Documents
drwxr-xr-x 2 tousif tousif 4096 Sep 21 09:11 Downloads
drwxr-xr-x 2 tousif tousif 4096 Sep 21 09:11 Music
drwxr-xr-x 2 tousif tousif 4096 Sep 21 09:11 Pictures
drwxr-xr-x 2 tousif tousif 4096 Sep 21 09:11 Public
drwxrwxr-x 2 tousif tousif 4096 Oct  9 18:14 sclab
drwx------ 4 tousif tousif 4096 Sep 21 14:57 snap
drwxr-xr-x 2 tousif tousif 4096 Sep 21 09:11 Templates
drwxr-xr-x 2 tousif tousif 4096 Sep 21 09:11 Videos
tousif@TousifVM:~$
```

Default permissions

umask
touch file1 && ls -l file1
umask 0077
touch file2 && ls -l file2
umask 0002

Default permissions are 110 | 110 | 110

```
tousif@TousifVM:~/Documents$ umask
0002
tousif@TousifVM:~/Documents$ touch file3 && ls -l file3
-rw-rw-r-- 1 tousif tousif 0 Oct 11 12:27 file3
tousif@TousifVM:~/Documents$ umask 0077
tousif@TousifVM:~/Documents$ touch file4 && ls -l file4
-rw------- 1 tousif tousif 0 Oct 11 12:28 file4
tousif@TousifVM:~/Documents$ umask 0002
tousif@TousifVM:~/Documents$
```

Change ownership

sudo chown user file

```
tousif@TousifVM:~/Documents$ ls -l file4
-rw------- 1 tousif tousif 0 Oct 11 12:28 file4
tousif@TousifVM:~/Documents$ chown dupuser file4
chown: changing ownership of 'file4': Operation not permitted
tousif@TousifVM:~/Documents$ sudo chown dupuser file4
[sudo] password for tousif:
tousif@TousifVM:~/Documents$ ls -l file4
-rw------- 1 dupuser tousif 0 Oct 11 12:28 file4
tousif@TousifVM:~/Documents$
```

Full Access Control List

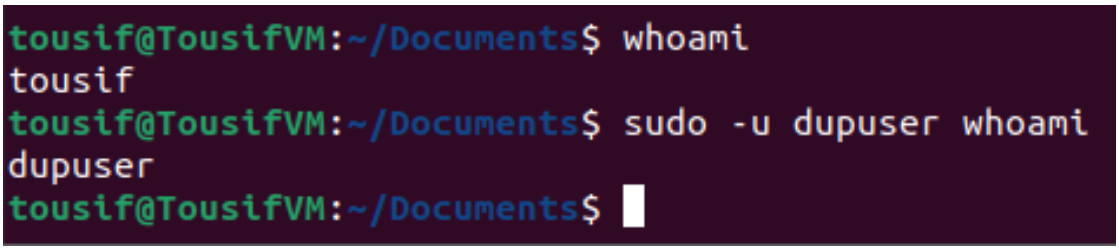
getfacl file
setfacl -m user:user:r file

getfacl displays the file name , owner , group and the Access Control List.

```
tousif@TousifVM:~/Documents$ ls -l file4
-rw------- 1 tousif tousif 0 Oct 11 12:28 file4
tousif@TousifVM:~/Documents$ getfacl file4
# file: file4
# owner: tousif
# group: tousif
user::rw-
group::---
other::---

tousif@TousifVM:~/Documents$ setfacl -m user:dupuser:r file4
tousif@TousifVM:~/Documents$ getfacl file4
# file: file4
# owner: tousif
# group: tousif
user::rw-
user:dupuser:r--
group::---
mask::r--
other::---

tousif@TousifVM:~/Documents$
```

Sudo - run command as another user

sudo -u user whoami



SuperUser privileges

sudo head /etc/shadow

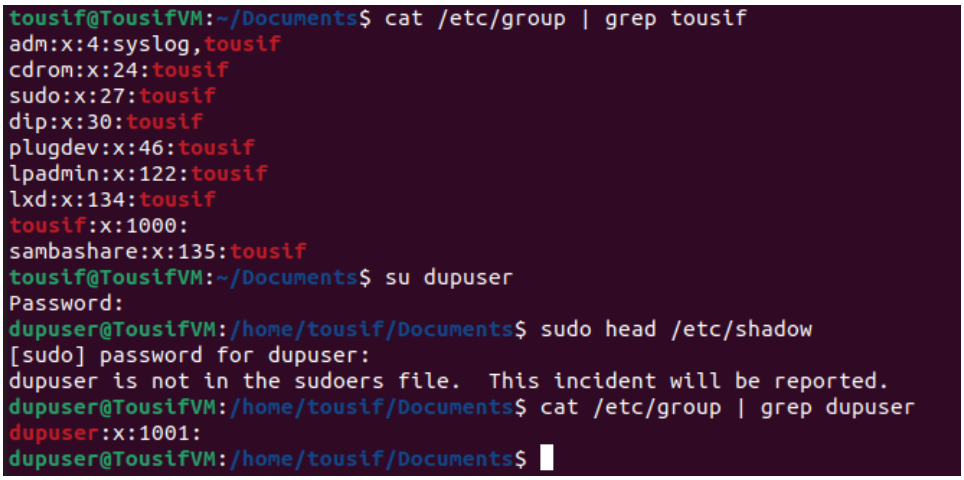
```
tousif@TousifVM:~/Documents$ head /etc/shadow
head: cannot open '/etc/shadow' for reading: Permission denied
tousif@TousifVM:~/Documents$ sudo head /etc/shadow
root:!:19255:0:99999:7:::
daemon:*:19213:0:99999:7:::
bin:*:19213:0:99999:7:::
sys:*:19213:0:99999:7:::
sync:*:19213:0:99999:7:::
games:*:19213:0:99999:7:::
man:*:19213:0:99999:7:::
lp:*:19213:0:99999:7:::
mail:*:19213:0:99999:7:::
news:*:19213:0:99999:7:::
tousif@TousifVM:~/Documents$
```

Sudo configuration file

sudo cat /etc/sudoers
sudo group is allowed to run anu command as super user.

```
tousif@TousifVM:~/Documents$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
tousif@TousifVM:~/Documents$ sudo cat /etc/sudoers | tail

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
tousif@TousifVM:~/Documents$
```

cat /etc/group | grep user
su user
sudo head /etc/shadow


tousif@TousifVM:~/Documents$ cat /etc/group | grep tousif
adm:x:4:syslog,tousif
cdrom:x:24:tousif
sudo:x:27:tousif
dip:x:30:tousif
plugdev:x:46:tousif
lpadmin:x:122:tousif
lxd:x:134:tousif
tousif:x:1000:
sambashare:x:135:tousif
tousif@TousifVM:~/Documents$ su dupuser
Password:
dupuser@TousifVM:/home/tousif/Documents$ sudo head /etc/shadow
[sudo] password for dupuser:
dupuser is not in the sudoers file. This incident will be reported.
dupuser@TousifVM:/home/tousif/Documents$ cat /etc/group | grep dupuser
dupuser:x:1001:
dupuser@TousifVM:/home/tousif/Documents$