

1. Use which cmd to check the where are its executable files

- a. Which pwd
- b. Which passwd
- c. Which su
- d. Which mount
- e. Which gpasswd

```
[siddharrth@linux ~]$ which pwd
/usr/bin/pwd
[siddharrth@linux ~]$ which passwd
/usr/bin/passwd
[siddharrth@linux ~]$ which su
/usr/bin/su
[siddharrth@linux ~]$ which mount
/usr/bin/mount
[siddharrth@linux ~]$ which gpasswd
/usr/bin/gpasswd
```

2. List all the files having special permission 4 – setuid

- a. Find /usr/bin -type f -perm -4000

```
[siddharrth@linux ~]$ find /usr/bin -type f -perm -4000
/usr/bin/fusermount3
/usr/bin/fusermount
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/mount
/usr/bin/su
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper
/usr/bin/at
/usr/bin/passwd
```

- b. Use **find** to get all files with spl perm 2- setgid from /usr/bin

```
[siddharrth@linux ~]$ find /usr/bin -type f -perm -2000
/usr/bin/write
/usr/bin/locate
```

3. List all the directories having special permission 2 – setgid from / directory (use find / -type d -perm -2000)

```
Permission denied
find: '/usr/share/polkit-1/rules.d': Permission denied
find: '/usr/share/empty.sshd': Permission denied
find: '/usr/libexec/initscripts/legacy-actions/audit': Permission denied
find: '/home/siddharrth/CEO/VP_Sales/Sale_lead1': Permission denied
find: '/home/siddharrth/CEO/VP_Engineering/Tech_Lead': Permission denied
find: '/home/sid': Permission denied
find: '/home/kevin': Permission denied
find: '/home/Marie': Permission denied
find: '/home/laura': Permission denied
find: '/home/einstein': Permission denied
find: '/home/bob': Permission denied
find: '/home/adrian': Permission denied
find: '/home/Robin': Permission denied
find: '/home/Ronaldo': Permission denied
find: '/home/Messi': Permission denied
find: '/home/Dravid': Permission denied
find: '/home/Neymar': Permission denied
find: '/home/dhoni': Permission denied
find: '/home/raina': Permission denied
find: '/home/virat': Permission denied
find: '/home/faf': Permission denied
find: '/home/sachin': Permission denied
find: '/home/sourav': Permission denied
find: '/cricket/kings': Permission denied
find: '/cricket/challengers': Permission denied
```

4. Run `ls -l /usr/bin/gpasswd` and observe the permission (-rws-r-x-r-x)
- a. Run the same for `passwd` and `sudo` and `chmod` and observe.

```
[siddharrth@linux ~]$ sudo passwd
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[siddharrth@linux ~]$
```

- b. Run `ls -l /usr/bin/locate` and observe the permission (-rwx--s--x)

```
[siddharrth@linux ~]$ ls -l /usr/bin/locate
-rwx--s--x. 1 root slocate 41032 Aug 10 2021 /usr/bin/locate
```

- c. Run `ls -l /usr/bin/write` and observe the permission (-rwxr-sr-x)

```
[siddharrth@linux ~]$ ls -l /usr/bin/write
-rwxr-sr-x. 1 root tty 23968 Aug 22 13:18 /usr/bin/write
```

- d. Run `ls -ld /tmp` and observe the permission (`drwxrwxrwt`)

```
drwxrwxrwt. 2 siddharrth siddharrth 34 Nov 6 12:50 VMwareDnD
```

5. Set up a directory, owned by the group `sports`. (`setGID -4`)

- a. Members of the `sports` group should be able to create files in this directory.

```
drwxr-sr-x. 2 siddharrth siddharrth 6 Nov 7 00:06 sports
```

- b. All files created in this directory should be group-owned by the `sports` group.

- i. Use (`chmod g+s dir/filename`) and also using octal values (`chmod 2775 dir/filename`)

```
drwxrwsr-x. 2 siddharrth siddharrth 6 Nov 7 00:06 sports
```

- c. Users should be able to delete only their own user-owned files.

```
drwxrwsr-t. 2 siddharrth siddharrth 6 Nov 7 00:06 sports
```

- d. Check if this works.

```
[sachin@linux siddharrth]$ rmdir sports/
rmdir: failed to remove 'sports/': Permission denied
```

- e. Try removing the permissions also and checking(`chmod g-s dir.filename`)

```
[dhoni@linux siddharrth]$ rmdir sports/
rmdir: failed to remove 'sports/': Permission denied
```

6. Create files and try setting and removing `setuid` permissions (`setUID -2`) and chk using `ls -l filename`

- a. `Chmod u+s filename`

```
drwsr-xr-x. 2 siddharrth siddharrth 6 Nov 7 00:24 splfile
```

- b. `Chmod u-s filename`

```
drwxr-xr-x. 2 siddharrth siddharrth 6 Nov 7 00:24 splfile
```

- c. `Chmod 4764 filename`

```
drwsrw-r--. 2 siddharrth siddharrth 6 Nov 7 00:24 splfile
```

- d. `Chmod 0764 filename`

```
drwsrw-r--. 2 siddharrth siddharrth 6 Nov 7 00:24 splfile
```

7. Become root user and create a shared full permission dir

- a. Become user `kevin` and create files and dirs.

```
[root@linux ~]# mkdir Newfolder
[root@linux Newfolder]# touch file{1..3}
[root@linux Newfolder]# ll
total 0
-rw-r--r--. 1 root root 0 Nov 8 10:48 file1
-rw-r--r--. 1 root root 0 Nov 8 10:48 file2
-rw-r--r--. 1 root root 0 Nov 8 10:48 file3
[root@linux Newfolder]#
```

- b. Login as another user and delete the files created by `kevin`

```
[root@linux Newfolder]# su raina
[raina@linux Newfolder]$ ll
total 0
-rw-r--r--. 1 root root 0 Nov  8 10:48 file1
-rw-r--r--. 1 root root 0 Nov  8 10:48 file2
-rw-r--r--. 1 root root 0 Nov  8 10:48 file3
[raina@linux Newfolder]$ rm file1
rm: remove write-protected regular empty file 'file1'? yes
[raina@linux Newfolder]$ ll
total 0
-rw-r--r--. 1 root root 0 Nov  8 10:48 file2
-rw-r--r--. 1 root root 0 Nov  8 10:48 file3
```

- c. Now set sticky bit to the shared dir (chmod +t dirname) / chmod 1777 dirname)

```
[root@linux ~]# chmod +t Newfolder/
[root@linux ~]# ls -ld Newfolder/
drwxrwxrwt. 2 root root 32 Nov  8 10:58 Newfolder/
```

- d. Again, as kevin create dirs and files inside shared folder

```
[raina@linux Newfolder]$ mkdir sub1
[raina@linux Newfolder]$ touch file{8..10}
[raina@linux Newfolder]$ ls
file10  file2  file3  file8  file9  sub1
```

- e. Login as another user and delete the files created by kevin f. Observe the changes.

```
[root@linux Newfolder]# su dhoni
bash-5.1$ rm file9
rm: remove write-protected regular empty file 'file9'? yes
rm: cannot remove 'file9': Operation not permitted
bash-5.1$
```