User Privilege Administration

User Privilege Administration (Exercise)

1. Commands and Paths
2. Create|Modify|Delete users (useradd|usermod|userdel)
3. Create|Modify|Delete groups (groupadd|groupmod|groupdel)
4. Privileged Command Execution Management (sudo)

User Privilege Administration

/etc/passwd

/etc/shadow

```
shahadat@mars:~$ 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
```

```
shahadat@mars:~$ sudo cat /etc/shadow
[sudo] password for shahadat:
root:!:19370:0:99999:7:::
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
```

```
shahadat:$6$08REO9Up$XobwOS8ELQwwzVZvHbMGVlQ.QpdJBz5.MTA6q63o2LpklgZ0hAdOdIv1D5xIbnddqNiHPxQlYFNyNQacfxSQh0:19393:0:99999:7:::
cups-pk-helper:*:19371:0:99999:7:::
mysql:!:19371:0:99999:7:::
ftp:*:19371:0:99999:7:::
sshd:*:19371:0:99999:7:::
testuser:$6$oQotMVzZ$qlUQjbGWELX7Gnftjea8HTIO0dA9Xr7v7vMUJkKivhbwLRArUh1N0ejUOpElD/9Dc9RTIWhq/Y4Fi9Bo9QZ/8.:19397:0:99999:7:::
```

User Privilege Administration

/etc/passwd

```
shahadat@mars:~$ 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
```

- **Columns are separated by ":"**

1st Column
User's login Name field

2nd Column
User's password field. X means password is stored in /etc/shadow

3rd Column
User's login ID

4th Column
User's Primary Group ID

5th Column
Description Field, also known as GECOS field

6th Column
User's Home Directory

7th Column
User's login Shell OR command that will execute after successful login

User Privilege Administration

/etc/shadow

```
shahadat:$6$08REO9Up$XobwOS8ELQwwzVZvHbMGVlQ.QpdJBz5.MTA6q63o2LpklgZ0hAdOdIv1D5xIbnddqNiHPxQlYFNyNQacfxSQh0:19393:0:99999:7:::
cups-pk-helper:*:19371:0:99999:7:::
mysql:!:19371:0:99999:7:::
ftp:*:19371:0:99999:7:::
sshd:*:19371:0:99999:7:::
testuser:$6$oQotMVzZ$qlUQjbGWELX7Gnftjea8HTIO0dA9Xr7v7vMUJkKivhbwLRArUh1N0ejUOpElD/9Dc9RTIWhq/Y4Fi9Bo9QZ/8.:19397:0:99999:7:::
```

Columns are separated by ":"

1st Column
User's login Name field

2nd Column
User's password field. Password is stored as encrypted hash with few additional information

3rd Column
Last password change (last changed) : The date of the last password change, expressed as the number of days since Jan 1, 1970 (Unix time). The value 0 has a special meaning, which is that the user should change her password the next time she will log in the system. An empty field means that password aging features are disabled.

4th Column
Minimum : The minimum number of days required between password changes i.e., the number of days left before the user is allowed to change her password again. An empty field and value 0 mean that there are no minimum password age.

5th Column
Maximum : The maximum number of days the password is valid, after that user is forced to change her password again.

6th Column
Warn : The number of days before password is to expire that user is warned that his/her password must be changed

User Privilege Administration

/etc/shadow

7th Column
Inactive : The number of days after password expires that account is disabled.

8th Column
Expire : The date of expiration of the account, expressed as the number of days since Jan 1, 1970.

Details of Password Field

```
$6$oQotMVzZ$qlUQjbGWELX7Gnftjea8HTIO0dA9Xr7v7vMUJkKivhbwLRArUh1N0ejUOpElD/9Dc9RTIWhq/Y4Fi9Bo9QZ/8.
```

Separated by $ sign

1st Column
Algorithm used for hashing (6 Means SHA512Crypt)

2nd Column
Salt value

3rd Column
Actual hash that has been calculated