**PAM - Plugable Authentication Module**

**pinfo**  - complete book with commands and examples

**man cmd\_name** - Manual about any command

passwd - stores user related information

shadow - stores password related info of the user

group - stores group related information

gshadow - stores password related info of the group

**USER**

useradd user\_name --- Add new user

cat /etc/passwd --- check users

passwd user\_name ---Set pass for user

passwd -d user\_name --- Delete Pass for user

chage -l user\_name --- Details of user

su - user\_name --- get into user mode

cat /etc/passwd --- get user info

cat /etc/shadow --- get password related info

id user\_name --- specific user related info

userdel -r user\_name --- Delete user with home directory

**GROUP**

groupadd group\_name --- Add new group

cat /etc/group --- group related info

cat /etc/gshadow --- group password related info

gpasswd group\_name --- Set group password

groupdel group\_name --- delete group

gpasswd -d user\_name --- delete user under that group password

cat /etc/login.defs --- this is where details are stored

**PERMISSIONS**

- Symbolic Method

- Numeric Method

**- Symbolic Method**

Read : r

Write : w

Execute : x

User Owner : u

Group Owner : g

Others : o

All : a

Assign : +

Remove : -

Overwrite : =

**Example :**

-rw-r--r--. 1 root root 1.8K Apr 19 04:20 initial-setup-ks.cfg

First 3 : User owner

Second 3 : Group Owner

Last 3 : Other

**Give Permission Commands**

chmod u+rw file/dir

chmod g-rw file/dir

chmod o=rw file/dir

**- Numeric Method**

This method will always override default permissions

Read : 4

Write : 2

Execute : 1

Full : 7

No : 0

chmod 670 file/dir

To see the permissions in numeric way : **stat file\_name**

**OWNERSHIP**

**User Owner**

chown user\_name file/dir

**Group Owner**

chgrp user\_name file/dir

**Membership**

1. Primary

useradd -g grp\_name user\_name

1. Secondary

useradd -G grp\_name user\_name --- In case of new user

usermod -G grp\_name user\_name --- In case of existing user

**ACL**

Access Control List

**User**

setfacl -m u:user\_name:rwx file/dir --- set permission to specific user

--- (-m) modify

**Group**

setfacl -m g:group\_name:rwx file/dir

**To check the ACL**

getfacl file/dir

**How to add multiple user ?**

- newusers