**Section-1 Advance User Management**

**Lesson-01: Create delete and modify local user accounts**

how can we change the password for the user

# passwd atif

Lets figure out how to lock the user we can use the usermod utility for that

# usermod -L atif

# cat /etc/shadow | grep atif

note the exclamation mark before the $ mark this show that user is locked

Unlocking the user

# usermod -U atif

notice the exclamation mark is disappeared

now how can we change the user id for an specific user

# usermod -u 1011 atif

how can we change the user home directory when creating a user

# useradd -u 1020 -d /home/john1 john

Adding a user to wheel group

# usermod -G wheel john

now to check that it has been assigned or not

# groups john

So coming to removing the user

# userdel -r john

**Lesson-02: Change password and set password aging**

For looking into a password policy for specific user we will use chage -l

# chage -l john

So for example we have new contractor and we need to expire his password after 30 days from today we will be adding a 30 day duration to that user, so how can we do that

For simplicity we will be getting a system date we will use a date command.

# date -d '+30days' +%F

now for changing the expiration date of the user

# chage -E copy-the-user-date john

for looking for changes we will use

# chage -l john

Now that we have assign the password expiration policy for the user how can we modify it, for that we will be using -M flag.

# chage -M 30 john (for confirmation chage -l john)

So how can we remove the account expires policy for user john

# chage -E -1 john (-1 flag will change the account expires to never for confirmation chage -l)

How can we force the user to change the password on next login

# chage -d 0 john (for confirmation chage -l john)

How do we change account to inactive state after certain amount of days i.e 30 days

# chage -l 30 john (this will set the account to change the password after 30 days)

how can we change the Number of warning days before the password expires

# chage -W 3 john

**Lesson-03: Create, delete and modify local groups**

To get the user information to which group it belongs to

# getent group john

We will be creating two groups

# groupadd class1

# groupadd class2

Now if we look into /etc/group file

# cat /etc/group | grep class1 (we see that class1 group is there)

So now we add a user by useradd command,

# useradd student

and if we take a look at user student to which group it belongs to

# groups student (and thats gonna show student primary group and supplementary group)

So lets change our primary group from student to class1

# usermod -g class1 student

Now we will be checking student user that which group it belongs to

# groups student

So how to assign a user to more supplementary or multiple groups

# usermod -aG class2 student

Small “a” shows that you want to append an group to student user

# id student (it will show us the detailed information about the user and what groups it belongs to along with id's)

So how can we change the group name

# groupmod -n class5 class1

# groups student | it has been renamed here

So how can we change the group id.

# groupmod -g 1010 class5

# getent group class5

So how can we specify permission to a group, lets make a directory.

# mkdir work

Change the permission of the work folder

# chmod g+w work

For assigning and group ownership

# chown root:class1 work

To remove a group

# groupdel class2

**Lesson-04: Set-GID on directories**

First of all we will creating two groups

# cd /home/

# mkdir groups

# mkdir {group1,group2}

# groupadd group1

# groupadd group2

Now we will change the group ownership of the folder with chown utility

# chown :group1 group1

# chown :group2 group2

Also we will assign write permission for group1 and group2

# chgrp g+w group1 group2

#ll

Next we will creating a user kevin and set a password to it

# useradd kevin

# passwd kevin

# id kevin

So lets add user kevin to two supplementry groups

# usermod -aG group1 kevin

# usermod -aG group2 kevin

so for checking that group has been assigned to user

# id kevin

it will show us that user has been assigned to supplement groups, so now we will be opening another ssh for kevin user to demonstrate this

rambo # cd /home/groups

rambo # cd group1

rambo # touch file1

what happen is file1 is created with user login group as the group owner, well that creates a problem for other user that are belong to the group1 and are using this directory for storing member files for group1. This means that no one inside the group1 will have the permission to view these files, so what do we need to do, well it is simple, for this we will be using chmod utility here, we will do

# chmod g+s group1

here s shows the set-gid, now we will create a file

# touch file2

**Lesson-05: Authentication using Realmd**

We have to update our centos 7 linux distritubtion

# yum update -y

# yum install realmd -y

for our local environment I have made a change in /etc/hosts file.

192.168.18.106 ad.linuxnoobcast.com

So to discover a realm in our environment we will do

# realmd discover ad.linuxnoobcast.com

We will install the required packages for the realmd

# yum install active-directory sssd oddjob oddjob-mkhomedir adcli samba-common-tools -y

Next we will join the realm

# realm join ad.linuxnoobcast.com

it will ask for the administrator password of the realm

So for confirmation we will be using realm utility

# realm discover ad.linuxnoobcast.local

Next we will be enabling kerberos authentication. We have to make sure that all the kerberos options is uncomment and set from no to yes.

# vi /etc/ssh/sshd\_config

Now we will restart the sshd service.

# systemctl restart sshd

now we will be testing this with username test as it is created in our active directory server

# cat /etc/passwd | grep test

Login to centos base linux virtual machine

In our case we will use this virutal machine ip address.

# ssh -l test@linuxnoobcast.local [the ip address that we are connecting to]