Practical 9C : User Administration and Security

Practice 1: Creating Users

Scenario: You need to set up user accounts for the new employees setting strong password policy on each of the accounts.

Deliverable: A system with users lim, lee, lora, bryan, peter and eddy with password expiration every thirty days.

Instructions:

1. Login to the RedHat Client VM as a ordinary account (student or rhel6).

2. Open a Terminal window on the RedHat Client VM.

3. Connect to RedHat Server as student and escalate your privileges to root with **su –** command (below example, login to RedHat client as student):

```
[student@client ~]$ ssh server
Password: redhat
[student@server ~]# su -
Password: redhat
[root@server ~]#
```

   In order for **ssh server** to work, you must edit the **/etc/hosts** file to include a line that maps the server IP address (eg. 10.0.0.3) to server.

   Note: if the ssh command does not work, exit RedHat Client VM and log in to the Red Hat Server VM directly as root to continue with the practice.

4. Use **useradd** command to add accounts for the following six users to your system: lim, lee, lora, byran, peter, and eddy. For the password, use redhat

   Repeat by creating users lee, lora, byran, peter and eddy with the same password redhat. You will be prompted that the password is BAD but you can still go ahead and use redhat as password.

```
[student@server ~]$ useradd lim
[student@server ~]# passwd lim
Password: redhat
[root@server ~]#
```

   Note that this sets a password of password for each user.

5. Use **chage** command to change all six earlier created users to have their password expire every thirty days.

   Change all six earlier created users to have their password expire every thirty days.

```
[root@server ~]# for USER in lim lee lora bryan peter
eddy
> do
> chage -M 30 $USER
> done
```

6. Of course, the use of password as a password for these users is insecure. Configure the user accounts to prompt the six users to have their passwords changes the next time they login.

   If we change the date that the password was last changed to be more than thirty days ago, the user will be prompted to change on the next login.

```
[root@server ~]# for USER in lim lee lora bryan peter
eddy
> do
> chage -d 2020-01-01 $USER
> done
```

7. Test one of the users by using **ssh** to log back in to the localhost. You should be prompted to change your password.

```
[root@server ~]# ssh lim@127.0.0.1
lam@localhost's password: password
You are required to change your password immediately
(password aged)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user lam
(current) UNIX password: password
New UNIX password: a new password
Passwd: all authentication tokens updated successfully.
Connection to localhost closed.
[root@server ~]# ssh lim@127.0.0.1
lam@localhost's password: a new password
Last login: . . .
[lam@server ~]# exit
[root@server ~]#
```

8. From the RedHat Client, remote login to the Server using any account. Create a text file **myusers** in the home directory containing these 2 lines (you can copy and paste them):

   Alice:password:500:500:Alice:/home/alice:/bin/bash
   Bob:dooow0rd:501:501:Bob:/home/bob:/bin/bash

Use the **newusers** command to create the 2 user accounts via the script file myusers. Check the /etc/passwd file to verify the accounts.

```
student@client ~]$ ssh server
Password: redhat
[student@server ~]$ nano myusers
<copy and paste the 2 lines above into myusers>
[student@server ~]$ su -
Password: redhat
[root@server ~]# newusers /home/student/myusers
```

9. When done, close your **ssh** session (if applicable) and terminal windows.

Practice 2: Creating Departmental Groups

Scenario: You need to set up group for different departments in your company. You also need to place the user accounts in those departments.

Deliverable: A system with users lim and lee in the sales group;
lora and bryan in the hr group;
peter and eddy in the web group,
and the student in the sales, hr, and web groups.

System setup: This sequence presumes that you earlier created the users named lim, lee, lora, bryan, peter and eddy.

Instructions:

1. If necessary, connect to the server as student and switch to root by command su –

```
[student@client ~]# ssh server
Password: student
[student@server ~]# su -
```

Note: if the ssh command does not work, exit RedHat Client VM and log in to the Red Hat Server VM directly as root to continue with the practice.

2. Add the following groups to the system:
    - Sales (GID:601)
    - Hr (GID:602)
    - Web (GID:603)

```
[root@server ~]# groupadd -g 601 sales
```

```
Repeat for hr and web
```

3. Add lim and lee to the sales auxiliary group, lora and bryan to the hr auxiliary group. Add peter and eddy to the web auxiliary group. Add student to all of these auxiliary groups.

   You can use usermod –G to do this:

```
[root@server ~]$ usermod -G sales lim
[root@server ~]$ usermod -G sales lee
[root@server ~]$ usermod -G hr lora
[root@server ~]$ usermod -G hr bryan
[root@server ~]$ usermod -G web peter
[root@server ~]$ usermod -G web eddy
[root@server ~]$ usermod -G sales,hr,web student
```

4. Verify that each user is a member of the correct groups by logging in as each user and using the **id** command.

```
[root@server ~]# for USER in lim lee lora bryan peter
eddy student
> do
> id $USER
> done
```

5. When done, close your **ssh** session (if applicable) and terminal windows.

[THE END]