Lab 33.1: Working with User Accounts

1. Examine /etc/passwd and /etc/shadow, comparing the fields in each file, especially for the normal user account. What is the same and what is different?

2. Create a `user1` account using **useradd**.

3. Login as `user1` using **ssh**. You can just do this with:

   `$ ssh user1@localhost`

   It should fail because you need a password for `user1`; it was never established.

4. Set the password for `user1` to `user1pw` and then try to login again as `user1`.

5. Look at the new records which were created in the /etc/passwd, /etc/group and the /etc/shadow files.

6. Look at the /etc/default/useradd file and see what the current defaults are set to. Also look at the /etc/login.defs file.

7. Create a user account for `user2` which will use the **Korn** shell (**ksh**) as its default shell. (if you dont have **/bin/ksh** install it or use the **C** shell at **/bin/csh**.) Set the password to `user2pw`.

8. Look at /etc/shadow. What is the current expiration date for the `user1` account?

9. Use **chage** to set the account expiration date of `user1` to December 1, 2013.

   Look at /etc/shadow to see what the new expiration date is.

10. Use **usermod** to lock the `user1` account.

    Look at /etc/shadow and see what has changed about `user1`'s password. Reset the password to `userp1` on the account to complete this exercise.

Solution 33.1

1. `$ sudo grep student /etc/passwd /etc/shadow`

   ```
   /etc/passwd:student:x:1000:100:LF Student:/home/student:/bin/bash
   /etc/shadow:student:$6$jtoFVPICHhba$iGFFUU8ctrtOGoistJ4/3ODrNLi1FS66qnn0VbS6Mvm
     luKI08SgbzT5.IcOHo5j/SOdCagZmF2RgzTvzLb11H0:16028:0:99999:7:::
   ```

   (You can use any normal user name in the place of `student`.) About the only thing that matches is the user name field.

2. `$ sudo useradd user1`

3. `$ ssh user1@localhost`

   ```
   user1@localhost's password:
   ```

   Note you may have to first start up the **sshd** service as in:

   `$ sudo service sshd restart`

   or

   `$ sudo systemctl restart sshd.service`

4. `$ sudo passwd user1`

   ```
   Changing password for user user1.
   New password:
   ```

5. `$ sudo grep user1 /etc/passwd /etc/shadow`

   ```
   /etc/passwd:user1:x:1001:100::/home/user1:/bin/bash
   /etc/shadow:user1:$6$OBE1mPMw$CIc7urbQ9ZSnyiniVOeJxKqLFu8fz4whfEexVem2
     TFpucuwRN1CCHZ19XGhj4qVujslRIS.P4aCXd/y1U4utv.:16372:0:99999:7:::
   ```

6. On either **RHEL 7** or **openSUSE 13.1** systems for example:

   ```
   $ cat /etc/default/useradd
   # useradd defaults file
   GROUP=100
   HOME=/home
   INACTIVE=-1
   EXPIRE=
   SHELL=/bin/bash
   SKEL=/etc/skel
   CREATE_MAIL_SPOOL=yes
   $ cat /etc/login.defs

   ....
   ```

   We don't reproduce the second file as it is rather longer, but examine it on your system.

7. `$ sudo useradd -s /bin/ksh user2`
   `$ sudo passwd user2`

   ```
   Changing password for user user2.
   New password:
   ```

8. `$ sudo grep user1 /etc/shadow`

   ```
   user1:$6$OBE1mPMw$CIc7urbQ9ZSnyiniVOeJxKqLFu8fz4whfEexVem2TFpucuwRN1CCHZ
     19XGhj4qVujslRIS.P4aCXd/y1U4utv.:16372:0:99999:7:::
   ```

   There should be no expiration date.

9. `$ sudo chage -E 2013-12-1 user1`
   `$ sudo sudo grep user1 /etc/shadow`

   ```
   user1:$6$OBE1mPMw$CIc7urbQ9ZSnyiniVOeJxKqLFu8fz4whfEexVem2TFpucuwRN1CCHZ
   19XGhj4qVujslRIS.P4aCXd/y1U4utv.:16372:0:99999:7::16040:
   ```

10. `$ sudo usermod -L user1`

    `$ sudo passwd user1`