LAB TIME

Try Try Try ... Success

1. From control, open an SSH session to servera as student.

```
[student@control ~]$ ssh student@servera
...output omitted...
[student@servera ~]$
```

2. On servera, explore locking and unlocking user accounts as student.

   2.1. As student, lock the operator1 account using administrative rights.

   ```
   [student@servera ~]$ sudo usermod -L operator1
   [sudo] password for student: student
   ```

   2.2. Attempt to log in as operator1. This should fail.

   ```
   [student@servera ~]$ su - operator1
   Password: redhat
   su: Authentication failure
   ```

   2.3. Unlock the operator1 account.

   ```
   [student@servera ~]$ sudo usermod -U operator1
   ```

   2.4. Attempt to log in as operator1 again. This should succeed.

   ```
   [student@servera ~]$ su - operator1
   Password: redhat
   ...output omitted...
   [operator1@servera ~]$
   ```

   2.5. Exit out of the operator1 user's shell to return to the student user's shell.

   ```
   [operator1@servera ~]$ exit
   logout
   ```

3. Change the password policy for operator1 to require a new password every 90 days. Confirm that the password age is successfully set.

   3.1. Set the maximum age of the operator1 user's password to 90 days.

   ```
   [student@servera ~]$ sudo chage -M 90 operator1
   ```

   3.2. Verify that the operator1 user's password expires 90 days after it is changed.

   ```
   [student@servera ~]$ sudo chage -l operator1
   Last password change : Jan 25, 2019
   Password expires : Apr 25, 2019
   Password inactive : never
   Account expires : never
   Minimum number of days between password change : 0
   Maximum number of days between password change : 90
   Number of days of warning before password expires : 7
   ```

4. Force a password change on the first login for the operator1 account.

   ```
   [student@servera ~]$ sudo chage -d 0 operator1
   ```

5. Log in as operator1 and change the password to forsooth123. After setting the password, return to the student user's shell.

   5.1. Log in as operator1 and change the password to forsooth123 when prompted.

   ```
   [student@servera ~]$ su - operator1
   Password: redhat
   You are required to change your password immediately (administrator
   enforced)
   Current password: redhat
   New password: forsooth123
   Retype new password: forsooth123
   ...output omitted...
   [operator1@servera ~]$
   ```

   5.2. Exit the operator1 user's shell to return to the student user's shell.

   ```
   [operator1@servera ~]$ exit
   logout
   ```

6. Set the operator1 account to expire 180 days from the current day. Hint: The date -d "+180 days" gives you the date and time 180 days from the current date and time.

    6.1. Determine a date 180 days in the future. Use the format %F with the date command to get the exact value.

    ```
    [student@servera ~]$ date -d "+180 days" +%F
    2019-07-24
    ```

    You may get a different value to use in the following step based on the current date and time in your system.

    6.2. Set the account to expire on the date displayed in the preceding step.

    ```
    [student@servera ~]$ sudo chage -E 2019-07-24 operator1
    ```

    6.3. Verify that the account expiry date is successfully set.

    ```
    [student@servera ~]$ sudo chage -l operator1
    Last password change : Jan 25, 2019
    Password expires : Apr 25, 2019
    Password inactive : never
    Account expires : Jul 24, 2019
    Minimum number of days between password change : 0
    Maximum number of days between password change : 90
    Number of days of warning before password expires : 7
    ```

7. Set the passwords to expire 180 days from the current date for all users. Use administrative rights to edit the configuration file.

    7.1. Set **PASS_MAX_DAYS** to 180 in **/etc/login.defs**. Use administrative rights when opening the file with the text editor. You can use the sudo vim /etc/login.defs command to perform this step.

    ```
    ...output omitted...
    # Password aging controls:
    #
    # PASS_MAX_DAYS Maximum number of days a password may be
    # used.
    # PASS_MIN_DAYS Minimum number of days allowed between
    # password changes.
    # PASS_MIN_LEN Minimum acceptable password length.
    # PASS_WARN_AGE Number of days warning given before a
    # password expires.
    #
    # PASS_MAX_DAYS 180
    # PASS_MIN_DAYS 0
    ```

```
# PASS_MIN_LEN 5
# PASS_WARN_AGE 7
...output omitted...
```

7.2. Log off from servera.

```
[student@servera ~]$ exit
logout
```

Connection to servera closed.

```
[student@workstation ~]$
```

FINISH