LAB :: Password Policy in Linux

- In this LAB we will see how to set various types of password policy in Ubuntu system.
- OS Ubuntu 14.04

Login to your server

- Windows: use puTTY
- Mac and Linux: use your terminal
- Username `apnic` and password `training`
- Login to your server using the above username and password.
- Note that the password rules presented in this LAB will be enforced only when non-root users change passwords, but not the root.

Password Policy

We will use the below password policy for our LAB

- The Password should be minimum of 8 characters long.
- The Password should contain one UPPER case and one symbol letter.
- The Password should be changed within 30 calendar days.
- The system should inform the user before 7 days of password expiration.

Install the required module

We need to install `libpam-cracklib` pam module for this LAB.

```
sudo apt-get install libpam-cracklib
```

Set minimum password length

To set the minimum password length open the following file with vim editor.

```
sudo vim /etc/pam.d/common-password
```

search the below line in that file

```
password   requisite  pam_cracklib.so retry=3 minlen=8 difok=3
```

By default, the password length is set to 8 characters. Exit from the file.

Set password complexity (One Upper case and one symbol)

To set the password complexity open the following file with vim editor.

```
sudo vim /etc/pam.d/common-password
```

search the below line in that file

```
password   requisite  pam_cracklib.so retry=3 minlen=8 difok=3
```

add `ucredit=-1` for UPPER case letter and `ocredit=-1` for symbol letter at the end of this line.

```
password  requisite     pam_cracklib.so retry=3 minlen=8 difok=3 ucredit=-1 ocredit=-1
```

To test your work, try to change the password. The system will prevent you to change the password if you violate the password policy.

Password expiration and notification

To see the password expiration of a specific user, type the following command:

```
sudo chage -l sysadmin1
```

By default, a user password is set to never expire.

```
Last password change                                    : Apr 16, 2017
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
```

```
Minimum number of days between password change        : 0
Maximum number of days between password change        : 99999
Number of days of warning before password expires     : 7
```

To set any of this values, Type the following command and follow the interactive prompts:

```
sudo chage sysadmin1
```

To see your changes, type the following command again:

```
sudo chage -l sysadmin1
```

******END of LAB******