



Lab 36.1: PAM Configuration

One of the more common **PAM** configurations is to deny login access after a certain number of failed attempts. This is done with the `pam_tally2` module. In this exercise we are going to deny login through `ssh` after three failed login attempts.

1. Edit `/etc/pam.d/ssh` and configure it to deny login after three failed attempts. Hint: add the following two lines to the file:

```
auth required pam_tally2.so deny=3 onerr=fail
account required pam_tally2.so
```

2. Try to login three times as a particular user (who has an account) while mistyping the password.
3. Try to login as the same user with the correct password.
4. Check to see how many failed logins there are for the user.
5. Reset the failed login counter.
6. Check again to see how many failed logins there are.
7. Try to login again with the correct password.

Solution 36.1

1. Add the following two lines to `/etc/pam.d/sshd`:

```
auth required pam_tally2.so deny=3 onerr=fail
account required pam_tally2.so
```

2. `$ ssh student@localhost`

```
Password:
Password:
Password:
Permission denied (publickey,keyboard-interactive).
```

3. `$ ssh student@localhost`

```
Password:
Account locked due to 3 failed logins
```

4. `$ sudo pam_tally2`

```
Login      Failures Latest failure   From
student          3    11/01/14 20:41:12 localhost
```

5. `$ sudo pam_tally2 -u student -r`

```
Login      Failures Latest failure   From
student          3    11/01/14 20:41:12 localhost
```

6. `$ sudo pam_tally2 -u student -r`

```
Login      Failures Latest failure   From
student          0
```

7. `$ ssh student@localhost`

```
Password:
Last failed login: Sat Nov  1 20:41:14 CDT 2014 from localhost on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Sat Nov  1 20:28:38 2014 from localhost
Have a lot of fun...
```