

Re: question about pam_tally and the faillog

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2008-03/msg00149.html>

- *From:* "Bill Tangren" <bjt@xxxxxxxxxxxxxxx>
 - *Date:* Thu, 20 Mar 2008 07:17:15 -0400 (EDT)
-

I am running a number of RHEL ES 4.5 systems, fully updated.

The problem I am having is baffling me. I am using pam_tally so that three consecutive unsuccessful logins will lock out the user, until an hourly cron script unlocks the account. It has worked fine for a number of years.

Anyone?

I've noticed the same problem with other accounts. suing to root tallies a failed login, even though the su was successful.

The problem is this:

If I log in as user bjt, and I SUCCESSFULLY su - to user bdna_user, the faillog records this as a failed login attempt, even though nothing untoward appears in the logs, that I can find. In essence, I can log in as bjt, su - to bdna_user three times, and cause bdna_user's account to be locked out, so that if bdna_user attempts to log in, their access will be denied. Below is the logs where I do just that.

```
Mar 18 09:40:35 doggett sshd(pam_unix)[14176]: session opened for user bjt
by (uid=0)
Mar 18 09:40:49 doggett su(pam_unix)[14201]: session opened for user
bdna_user by bjt(uid=500)
Mar 18 09:41:27 doggett su(pam_unix)[14201]: session closed for user
bdna_user
Mar 18 09:41:36 doggett su(pam_unix)[14226]: session opened for user
bdna_user by bjt(uid=500)
Mar 18 09:41:38 doggett su(pam_unix)[14226]: session closed for user
bdna_user
Mar 18 09:41:44 doggett su(pam_unix)[14250]: session opened for user
```

Re: question about pam_tally and the faillog

```
bdna_user by bjt(uid=500)
Mar 18 09:41:48 doggett su(pam_unix)[14250]: session closed for user
bdna_user
Mar 18 09:42:03 doggett sshd(pam_unix)[14176]: session closed for user bjt
Mar 18 09:42:07 doggett sshd(pam_unix)[14150]: session closed for user
bdna_user
Mar 18 09:42:23 doggett pam_tally[14278]: user bdna_user (1029) tally 4,
deny 3
```

```
[root@doggett ~]# pam_tally
User bdna_user (1029) has 4
[root@doggett ~]#
```

This is what is in /etc/pam.d/system-auth:

```
auth required /lib/security/$ISA/pam_tally.so onerr=succeed
no_magic_root
account required /lib/security/$ISA/pam_tally.so deny=3
no_magic_root reset
```

NOTE: I have systems where "onerr=fail" is set, and it makes no difference.

My question is, why is it doing this?

—
Bill Tangren
U.S. Naval Observatory

Si hoc legere scis nimium eruditionis habes

—
redhat-list mailing list
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>

—
Bill Tangren
U.S. Naval Observatory

Si hoc legere scis nimium eruditionis habes

—
redhat-list mailing list
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>

Re: question about pam_tally and the faillog