

Re: pam_ldap and password management and rsh/ssh without password

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2005-06/0032.html>

From: Polly Squires (psquires_at_kewlhair.com)

Date: 06/28/05

Date: 27 Jun 2005 20:41:15 -0700

Jason King wrote:

> *Polly Squires wrote:*

> > *The System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* says that if you enable *pam_ldap* that *rsh/ssh* and authentication that doesn't require a password will fail. So it seems my choices are to fall back to *pam_unix_account* which ignores the fact that accounts may be expired (via *ldap*). This doesn't make sense to me. (Why isn't there a *pam_ldap_account* ?)

> >

> > *I am not hiding expiry information from my proxy...why is this a problem?*

> >

> > *At any rate, I'm sure that there are people out there who are using ldap for password management that have a working solution with ldap/rsh/ssh and password aging. What are people doing?*

> >

>

> *Funny you should mention that, I just mentioned something about this on the opensolaris-rfe list -- basically what's happening is that it's using an LDAP control that's returned as part of an ldap bind operation to obtain password expiration information, which means of course that pam_ldap has to actually be able to bind to the ldap server as the user (which it cannot do when using public key auth or rhosts since it never actually gets the password), so it returns a failure.*

>

> *You might be able to get away with manually maintaining the shadowAccount attributes (though I haven't tried this). The disadvantage to this is that then the clients are managing the password policy instead of letting the ldap server do it (i.e. each client would have to check the shadowLastChange, etc. attributes and enforce action appropriately). If you're doing only UNIX authentication, this might work, if you also want to have other things authenticate against the same ldap server to authenticate users, then you might start to run into issues (as they would also have to know to check those attributes to make sure an account isn't expired, or if they need to change their*

comp.security.unix: Re: pam_ldap and password management and rsh/ssh without password

> *password*).

I kind of figured it did a bind for account management , although I was hoping that it only used the bind for authentication verification.

I can't believe there isn't anyone else with a working solution already. Especially with audits pushing for password aging and increased security(while still having some automated processes to make your business run).

I don't have a problem falling back to pam_unix but what's really the most effective way of updating the shadow entries? A custom passwd command?

Does anyone know if PADL pam_ldap handles this more gracefully?

I'm really drawing for straws here.

--Polly