Bugs & Wish list

LDAP auth does not really connect to LDAP in order to authenticate (only does it on the first login) | Tiki
Wiki CMS Groupware :: Development
LDAP auth does not really connect to LDAP in order to authenticate (only does it on the first login)

Status
    ⊗ Closed

Subject
    LDAP auth does not really connect to LDAP in order to authenticate (only does it on the first login)

Version
    2.x

Category
- Error
- Regression

Feature
    External Authentication (LDAP, AD, PAM, CAS, etc)

Submitted by
    sacra

Volunteered to solve
    Philippe Cloutier

Lastmod by
    Philippe Cloutier

Rating
    ★ ★ ★ ★ ★ (0) ❓

Description
    Hello all.

    Almost by chance I noticed a behavior which seems wrong regarding the LDAP authentication on
    TikiWiki 2.0. I'm not sure if it was already present in 1.9.11 but I don't think so. We migrated last
    week.

    Regarding the TW configuration:

    - authentication method is "Tiki+PEAR::Auth"
    - users cannot register and cannot change password
    - "Create user if not in Tiki?" is on
    - "Create user if not in Auth?" is off
    - "Just use Tiki auth for admin?" is on
    - The LDAP auth configuration paramters are correct, the auth itself works well, as it worked in
    1.9.11. When TW connects to the LDAP server (OpenLDAP 2.1.30) the authentication works as
    expected.

    This means that a Tiki account is created when LDAP users login for the first time. As expected, in
    presence of such a user, TW connects to LDAP, authenticates, creates Tiki account and logs the user
    in (I have some doubts in this last item though). However, when users log in again after this, I would
    expect that authentication is still delegated completely to the LDAP and is not done through Tiki.
    Instead, I have confirmed by looking at my LDAP logs that when TW finds a Tiki account, it
    authenticates the user through Tiki and never connects to the LDAP. This is not the expected
    behavior, because it means that passwords are being stored on the TW database and actually used

for authentication. As a consequence, when a user changes his password on the LDAP, this is not "seen" by TW.

I'm pretty sure this is not the intended behavior also because if I go to Admin Users, both the "edit user" and the "add user" boxes show the following:

"No password is required
Tikiwiki is configured to delegate the password managment to LDAP through PEAR Auth."

And actually, the "edit user" box also says "Warning: changing the username will require the user to change his password" which is a contradiction since the password should be managed by LDAP and my TW is configured to disallow users from being able to change their passwords.

Paulo

Solution
    This should be fixed in Tiki 4. Please reopen if you can reproduce in Tiki 5 or later.

Importance
    6
Priority
    30
Demonstrate Bug (Tiki 19+)
    ## Please demonstrate your bug on show2.tiki.org

    Version: trunk ▼
Demonstrate Bug (older Tiki versions)
    ## Please demonstrate your bug on show.tikiwiki.org

    Version: 18.x ▼
Ticket ID
    1990
Created
    Wednesday 27 August, 2008 15:38:55 GMT-0000
    by Unknown
LastModif
    Friday 08 October, 2010 18:56:32 GMT-0000

Comments

Fallback 12 May 09 14:25 GMT-0000

I installed TW 3.0 and here it is the same.
The problem is, that u can spam the database with users which don't exist.
And the real users get a "invalid password" message if they don't exist in the auth, which is confusing.

Attachments

filename	created	hits	comment	version	filetype

No attachments for this item

The original document is available at
https://dev.tiki.org/item1990-LDAP-auth-does-not-really-connect-to-LDAP-in-order-to-authenticate-only-does-it-on-the-first-login