



SELinux security module definition for pam ldap

<i>SELinux security module definition for pam ldap</i>	1
SELinux environment.....	1
SELinux Informations.....	1
Gentoo Informations.....	1
General informations about the PamLDAP module.....	1
Main scheme.....	2
Needs.....	2
SELinux Module.....	3
Module definition	3

Note: this work has been made during an internship (summer 2007) at the ENST Bretagne of Rennes, France, SERES team. Note that these patches are only draft that have not been approved by the hardened-gentoo community.

Bug's reference: #199561 - http://bugs.gentoo.org/show_bug.cgi?id=199561

SELinux environment

SELinux Informations

```
SELinux status:      enabled
SELinuxfs mount:    /selinux
Current mode:        permissive
Mode from config file:  permissive
Policy version:      21
Policy from config file:  strict
```

Gentoo Informations

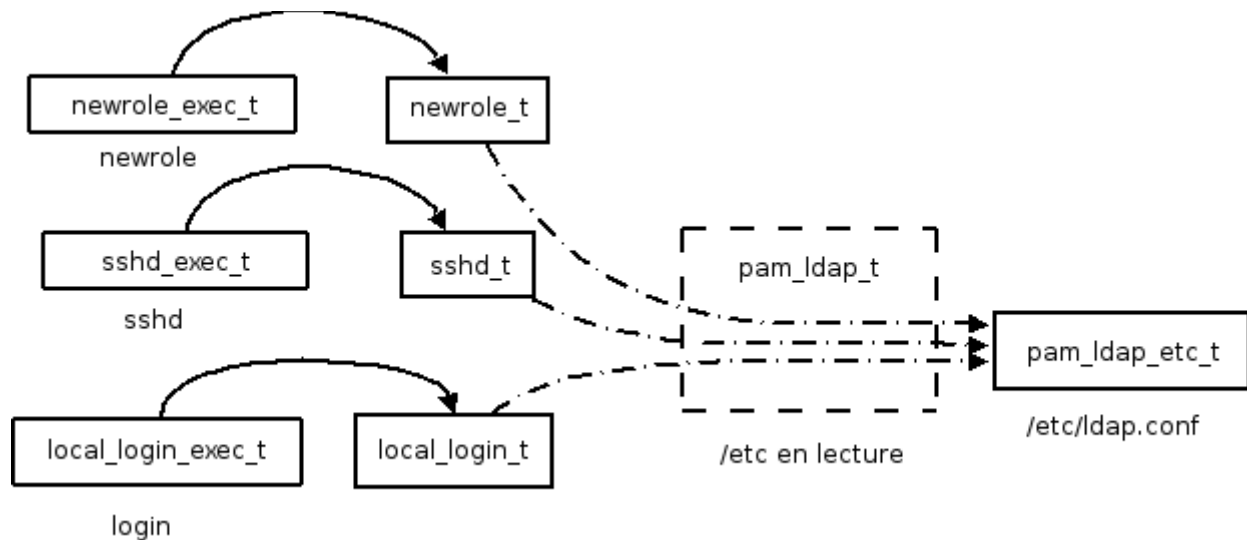
Linux 2.6.20-hardened-r5

General informations about the PamLDAP module

The main aspect of this module consists in defining a new domain for the confinement of this PAM module. I have created this module as when I used the *PamLDAP* extension for remote authentications, I discovered that it used sensitive information for LDAP connexions. The module aims to protect these datas.

Main scheme

The following figure describes the new *PamLDAP* module.



Needs

Needs analysis is required for this module, as no one were proposed before. Besides, it helps use to identify legitimate processes for *PamLDAP* data accesses.

These processes where identify through the following way: deny access to every processes and analyze AVC messages.

Thus, the current SELinux module is adapted for standards uses but new processes can be added if required. For instance (see bellow) the login processes may not be authorized to use the *PamLDAP* module if accessed from the outside. The module reject this use as it was not required in my case. This is an example of modular development (boolean values) for new versions of this module.

The current allowed processes are described bellow:

- login: local accesses (local_login_t). However, remote_login_t processes are not allowed for the moment.
- ssh: remote connexion (sshd_t)
- newrole: SELinux role transitions (newrole_t)

For the *PamLDAP* module, sensitive informations are stored in the file `/etc/ldap.conf`. It contains ldap server connexion parameters, such as login and password. These informations need to be protected. Though DAC rights with a mode 640 protect them well, it is possible to enhance the protection with the SELinux module: even root processes will not be able to access to the information (before, this file was labelled *etc_t* and any process with root rights was able to access it).

SELinux Module

In order to provide the required security restrictions, the module consists in:

- defining a pam_ldap_t (meta-type) attribute
- associating existing SELinux type (authorized processes) with this typeattribute
- restricting accesses to /etc/ldap.conf only to pam_ldap_t.

Module definition

```
module pam_ldap 1.0 ;

require {
class file {read getattr lock ioctl } ;
class lnk_file { getattr read } ;
class dir { getattr search read lock ioctl } ;
type local_login_t ;
type sshd_t ;
type etc_t ;
type newrole_t ;
}

attribute pam_ldap_t ;
type pam_ldap_etc_t ;

typeattribute local_login_t pam_ldap_t ;
typeattribute sshd_t pam_ldap_t ;
typeattribute newrole_t pam_ldap_t ;

allow pam_ldap_t pam_ldap_etc_t:file {read getattr } ;
allow pam_ldap_t etc_t:dir { getattr search read lock ioctl } ;
allow pam_ldap_t etc_t:file { getattr read lock ioctl } ;
allow pam_ldap_t etc_t:lnk_file { getattr read } ;
```

```
pam_ldap.fc
/etc/ldap.conf -- system_u:object_r:pam_ldap_etc_t
```