Service Access Control

Per user restriction

Ferry Boender

1. About this document

On standard Unix systems it’s common for a user account to have access to just about all the services which exist on the server. When a new user account is created, it will have a homedir, FTP access, SSH access, POP and mail capabilities, etc. More open services means more security risks. It is therefor very important to only give access to services which are required for a user. This document describes how this can be accomplished through the use of PAM.

PAM, which is short for Pluggable Authentication Modules, allows a system administrator to use modules in order to secure his system. Modules exist for all kinds of authentication methods, for instance: password-based, username-based, origin-based, etc. In theory it would be possible to write PAM modules for fingerprinting, voice and retinal-scan identification. Perhaps they already exist. (I didn’t bother looking into it, I’m lazy and proud of it.)

This document describes only one nice ’trick’ which can be accomplished using PAM. Much more interesting things can be done using PAM. If you’d like to know more about these, check out the Additional Readings section, which contains links to other PAM documents.

2. What we want

We (or at least, I) want to have one directory in my server’s /etc/ dir, which contains a number of files (one for each service). Each of these files contain a list of usernames which are allowed access to the service. For example:

```
[todsah@sharky]/etc/service-access$ ls
ftp pop ssh su

[todsah@sharky]/etc/service-access$ cat ftp
root
todsah
annaangel
aromog
```

This means, the users root, todsah, etc are allowed access to the ftp server. They still need to enter their normal authentication like a password or whatever.

3. Which services are supported?

All services/programs that support PAM should in theory work with these service-access thingies. I'm sure it works with:

- Proftpd (see chapter 4.3, Specific services)
- Sshd (OpenSSH)
- Telnet
- Console logins
- Ipop3d

Some services require some additional configuration. This will be discussed later.

4. How we're gonna do it

To accomplish this, we'll need to fiddle around with the PAM configuration. But first of all, lets create the service-access dir.

4.1. Service access files

Create a directory somewhere. It doesn't matter where, because we can all change where PAM will look for the files inside the PAM configuration. You can also name the dir anything you want. In this example, well create a dir in /etc/ named service-access.

After creating the directory, fill it with text files using your favorite text editor. The text files may be named anyway you want to, but it's best to use the same name as the service or the program which is providing the service. The text file should contain the names of the users which may use the service. When we look at the ftp service-access file, named ftp this is what's contained in it:

```
root
todsah
annaangel
aromog
```

You may create such a file for each service.

4.2. Modifying PAM configuration

Now we tell PAM to check for a username in the service-access files, in addition to the default authorization checking. This can be done by changing the PAM configuration file for a service. The PAM configuration files are usually contained within the /etc/pam.d directory.

Edit a pam configuration file and add the following line:

```
auth required pam_listfile.so item=user sense=allow file=/etc/service-access/ftp onerr=fail
```

(make sure you modify the *file=* option so it points to the correct file)

You can do this for all services which support PAM.

4.3. Specific services

Some services (daemons) require some configuration changes before PAM authentication will work properly.

4.3.1. ProFTPd

To enable PAM in ProFTPd, you'll have to add the following line to your configuration (which usually is `/etc/proftpd.conf`):

```
AuthPAMAuthoritative on
```

5. Additional reading

The following world wide web links may provide interesting additional readings about PAM and other service access related reading material:

- PAM Modules/Applications available or in progress... (http://www.kernel.org/pub/linux/libs/pam/modules.html)
- The Linux-PAM System Administrators' Guide (http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html)

6. Copyright / Author

Author:

Ferry Boender
De Cotelaer 28
3772 BP
Barneveld
The Netherlands
`<f (DOT) boender (AT) electricmonk (DOT) nl>`

6.1. Document changes

This document has undergone the following changes:

Revision History

Revision 0.4 24 June 2003 Revised by: FB
Rewrote document in Docbook SGML
Revision 0.3 20 June 2003 Revised by: FB
Added document history. Added additional reading links
Revision 0.2 05 May 2003 Revised by: FB
Added specific service information
Revision 0.1 10 May 2002 Revised by: FB
Initial release