1. To check if your application uses LINUX-PAM or not use the following command in your terminal:

*$*ldd /bin/su

Text

Description automatically generated

As we can see in line 2 of the output there exists an lipbpam.so file which confirms the query.

1. The configuration of LINUX- PAM is in the directory /etc/pam.d/. Open the terminal of your Linux Operating system and go to the pam directory by typing the command:

*$*cd /etc/pam.d/

This is the directory that contains other services that supports PAM. One can

Text

Description automatically generated  
if you don’t find sshd as a service that supports PAM, you have to install the sshd server.

SSH(or secure shell) is an encrypted networking tool designed to allow different type of computers/users to login securely to various computers remotely over a network. You need to install the openssh-server package which you can do by running the following command in your terminal.

*$*sudo  apt-get   install openssh-server

It will install all the files and then you can reenter the pam directory and check for the services and see sshd has been added.

Text

Description automatically generated

1. VIM is a text editor that opens plain text documents for the user to see, and edit.

*$*vim sshd

Text

Description automatically generated

If you want to exit the vim editor and are unable to do so press the Esc key and colon (:) at the same time that puts you in the insert mode. After the colon type q and press enter. Here q stands for quit.

You can scroll down and see all the modules that were described earlier with terms like required, include, requisite etc. What are those?

They are called as the PAM Control Flags. Let us get into their details before diving into much more concepts of PAM services.

**PAM Control Flags**

1. **Required:**Must pass to result success. It is the necessity that one can’t do without.
2. **Requisite:** Must pass otherwise no further modules are run.
3. **Sufficient:** It is ignored if fails. If this module is passed no further flags will be checked.
4. **Optional:** It is often ignored. It is only used when there is only one module in interface.
5. **Include:** It fetches all the lines from the other files.

Now the general rule to write the main configuration is as follows service type control-flag module module-arguments

1. **SERVICE:**This is the name of the application. Suppose the name of your application is NUCUTA.
2. **TYPE:** This is the type of module used. Suppose here the module used is authentication module.
3. **CONTROL-FLAG:**This is the type of control flag used, one among the five types as describe before.
4. **MODULE:** The absolute filename or the relative pathname of the PAM.
5. **MODULE-ARGUMENTS:**It is the separate list of tokens to control module behavior.

Suppose you want to disable root user access to any kind of system via SSH, you need to restrict access to sshd service. Moreover, the login services are to be controlled access.

There are several modules that restrict the access and gives privileges but we can use the module **/lib/security/pam\_listfile.so**which is extremely flexible and has many functionalities and privileges.

1. Open and edit the file/application in the vim editor for the target service by entering into the **/etc/pam.d/**directory first.

The following rule is to be added in both the files:

auth required pam\_listfile.so\onerr=succeed item=user sense=deny file=/etc/ssh/deniedusers

Where auth is the authentication module, required is the control flag, the pam\_listfile.so module gives the deny privileges to the files, onerr=succeed is the module argument, item=user is another module argument that specifies file listings and the contents it must be checked for, sense=deny is another module argument that will if item is found in a file and file=/etc/ssh/deniedusers that specifies a type of file that only contains one item per line.

1. Next create another file **/etc/ssh/deniedusers**and add root as the name in it. It can be done by following the command:

*$*sudo vim /etc/ssh/deniedusers

1. Then save the changes after adding root name to it and close the file.
2. Use the chmod commond to change the access mode of the file. The syntax for the chmod command is

chmod   [reference][operator][mode]  file

Here the references are used to specify a list of letters that indicates whom to give permission.

For example, here you can write the command:

*$*sudo   chmod   600  /etc/ssh/deniedusers

You specify the users that are denied access to your file in the /etc/ssh/deniedusers file and set access mode for the file using the chmod command.

From now on while trying to access the file due to this rule PAM will deny all the users listed in the /etc/ssh/deniedusers  file any access to the file.

**Conclusion**

PAM provides dynamic authentication support for applications and services in a Linux Operating System. This guide states a number of flags that can be used to determine the outcome of the result of a module. It’s convenient, and reliable. for users than the traditional password, and username authentication mechanism, and thus PAM is often used in many secured systems.