

Pengaturan Akses User di Linux

Pada pertemuan ini kita akan membahas dua hal yang berhubungan dengan pengaturan akses di linux yaitu :

- Pengaturan Kompleksitas Pasword di Linux
- Pengaturan Akses Admin di Linux

Pengaturan Kompleksitas Pasword di Linux

Password merupakan salah satu elemen yang sangat penting karena dipergunakan oleh user sebagai kunci untuk melakukan autentifikasi ke dalam sistem.

Dalam sistem operasi linux pengaturan kompleksitas password diatur oleh module PAM (**Pluggable Authentication Module**) yang terletak pada folder */etc/pam.d/system-auth* (Red Hat dan turunannya) dan */etc/pam.d/common-password* (Debian dan turunannya).

Ada beberapa manfaat ketika menggunakan PAM, diantaranya :

- Meminimalkan kesalahan konfigurasi untuk sebuah aplikasi
- Memudahkan untuk maintenance suatu aplikasi sehingga salah konfigurasi tidak mengganggu aplikasi lain lain.
- Memungkinan adanya link simbolik antar file konfigurasi yang berbeda menjadi satu file.
- Memudahkan dan menghemat waktu konfigurasi.
- Memungkinkan untuk membatasi akses individu menggunakan proteksi file system
- Manajemen paket lebih sederhana karena setiap aplikasi baru dapat dilekatkan di */etc/pam.d/*

Konfigurasi untuk setiap service PAM yang ada di simpan pada satu file */etc/pam.conf*. Namun karena alasan pemeliharaan dan penggunaan, konfigurasi berbasis file ini tidak lagi digunakan. Untuk saat ini, konfigurasi untuk setiap service disimpan pada direktori */etc/pam.d/*

Berikut tampilan isi dari file konfigurasi PAM */etc/pam.conf* :

```
ahmad@debian:~$ sudo cat /etc/pam.conf
# -----#
# /etc/pam.conf                                     #
# -----#
#
# NOTE
# ----
#
# NOTE: Most program use a file under the /etc/pam.d/ directory to setup their
# PAM service modules. This file is used only if that directory does not exist.
# -----#
#
# Format:
# serv. module      ctrl      module [path]      ...[args..]      #
# name type        flag
# -----#
```

Setiap service atau program yang menggunakan PAM memiliki file konfigurasi sendiri yang disimpan dalam direktori /etc/pam.d/. Beberapa file konfigurasi yang ada dalam direktori /etc/pam.d/ berbeda untuk semua host.

Berikut tampilan beberapa file konfigurasi yang ada dalam direktori /etc/pam.d/ :

```
ahmad@debian:~$ sudo ls /etc/pam.d
atd          common-password      gdm3-autologin      polkit-1
chfn         common-session        gnome-screensaver   su
chpasswd     common-session-noninteractive login                sudo
chsh         cron                  newusers
common-account cups                  other
common-auth  gdm3                  passwd
```

Dalam debian, terdapat 5 konfigurasi default yang ada di dalam PAM, diantaranya adalah :

- o /etc/pam.d/common-auth
- o /etc/pam.d/common-account
- o /etc/pam.d/common-password
- o /etc/pam.d/common-session
- o /etc/pam.d/common-session-noninteractive

Percobaan 1 :

1. Membatasi Jumlah Kegagalan Login

Salah satu cara untuk menyusup ke dalam sistem adalah dengan mencoba kombinasi username dan password untuk login. Dengan menggunakan PAM kita dapat mengurangi resiko sistem disusupi oleh orang-orang luar. Untuk mengimplementasikannya, kita menggunakan modul pam_tally.so.

Contoh :

Tambahkan baris berikut ini ke file /etc/pam.d/login dengan cara Vi /etc/pam.d/login

```
auth required pam_tally.so per user deny=3 unlock_time=120
```

Ket:

Deny = 3, toleransi untuk kegagalan 3 kali Unlock_time = 120, akun akan di unlock setelah 120 s kemudian.

Skenario :

Lakukan login misal User budi, jika user budi telah 3 kali melakukan kesalahan password, akan muncul warning bahwa accountnya telah dikunci, sehingga harus menunggu selama 120 detik agar dapat melakukan login

```
Debian GNU/Linux 6.0 debian tty6
debian login: budi
Password:
Login incorrect
debian login: budi
Password:
Login incorrect
debian login: budi
Password:
Login incorrect
debian login: budi
Account locked due to 4 failed logins
Password: _
```

2. Membatasi waktu login

Dengan menggunakan PAM kita juga dapat membatasi waktu login untuk masing-masing user.

Contoh:

Misal user budi hanya dapat login pada hari sabtu minggu pada jam 08:00 – 18.00.

Pertama tambahkan baris berikut pada file /etc/security/time.conf

```
login;*;budi;SaSu0800-1800
```

Kemudian tambahkan baris berikut pada file /etc/pam.d/login

```
account      required      pam_time.so
account      required      pam_nologin.so
```

Skenario :

Setelah dilakukan percobaan berikut adalah hasil capture dimana Budi tidak diizinkan login karena hari ini adalah hari selasa.

```
debian login: budi
Password:
Permission denied
Debian GNU/Linux 6.0 debian tty6
debian login: ahmad
Password:
Last login: Tue Apr  3 17:38:53 WIT 2012 on tty6
Linux debian 2.6.32-5-686 #1 SMP Mon Jan 16 16:04:25 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ahmad@debian:~$ _
```

3. Membatasi resource untuk user atau group

Dengan menggunakan PAM kita juga dapat membatasi resource untuk user ataupun group. Dan juga kita bisa membatasi jumlah maksimum seorang user dapat login kedalam sistem.

Contoh :

Untuk user budi dibatasi maksimum login kedalam sistem 2 kali.

Caranya tambahkan baris berikut pada file /etc/security/limits.conf

```
budi - maxsyslogins 2
```

Kemudian tambahkan baris berikut kedalam file /etc/pam.d/login

```
session required pam_limits.so
```

Skenario :

Lakukan percobaan login dan lihat hasil jika salah login lebih dari 2 kali login ?

4. Keamanan Password menggunakan pam_cracklib

Dengan menggunakan pam_cracklib admin dapat memastikan agar setiap user memiliki password yang sesuai dengan ketentuan. Misalnya dengan mewajibkan setiap user memiliki password dengan panjang minimal 8 karakter, terdiri dari kombinasi angka, huruf atau simbol, dan ketentuan lainnya.

Contoh :

Sebelumnya pastikan anda telah menginstall modul libpam-cracklib. Jika anda belum menginstall, install libpam-cracklib dengan cara :

Aptitude install libpam-cracklib

setelah itu tambahkan baris berikut pada /etc/pam.d/passwd dengan cara :
Vi /etc/pam.d/common-password

```
#menambahkan baris untuk memastikan user memilih password baru dengan  
#panjang minimal 8 karakter minimal 1 digit, 1 uppercase letter, dan 1 karakter  
#lainnya  
password required pam_cracklib.so dcredit=-1 ucredit=-1 ocredit=-1 lcredit=0 min  
len=8
```

Pengaturan Akses Admin di Linux

Pada OS linux pada awal penginstallan kita sudah di sediakan user TERATAS atau user ROOT. User root adalah user yang memiliki hak paling tertinggi, dengan user ini semua bisa dilakukan. software yang tidak dapat di install oleh user lain dapat kita install dengan user ini, tapi terdapat bahaya kalau kita selalu menggunakan user ini, misal apa bila kalian menginstall suatu software atau tool yang berisi virus, maka virus itu memiliki hak akses tertinggi juga karena virus itu di izinkan terinstall di user tertinggi, virus tersebut dapat menyebar ke USER mana pun di komputer/perangkat anda .

Sebenarnya user root hanya boleh di gunakan ketika keadaan darurat saja, jadi kalau kita mau mengoperasikan OS linux yang tanpa keadaan darurat login saja menggunakan user biasa.

Di linux permission itu sangat penting, jika kita login dengan user biasa kita tidak akan bisa mengakses file atau folder yang permission nya root kecuali menggunakan sudo, itupun kalau user kita di masukkan ke group sudo. Misalnya jika kita deploy web dengan user root, jika seumpama situs tersebut terdapat celah yang bisa di buat upload shell, nanti otomatis kan shell tersebut mempunyai permission root, maka dari jarak jauh memungkinkan dilakukan akses file, untuk mengatasi hal tersebut di linux dikenal cara mengaktifkan user biasa sebagai administrator system.

Ada dua cara untuk mengaktifkan user biasa sebagai administrator system, yang pertama adalah menambahkan user tersebut ke dalam group sudo, dan yang kedua adalah menambahkan user tersebut ke dalam list sudo. Kedua cara tersebut akan saya bahas disini.

Percobaan 2 :

1. Pertama-tama buat user baru dengan nama test, dengan menggunakan user utama/root, saya akan menjalankan perintah penambahan user baru dengan cara di bawah:

```
adduser test
```

Ikuti langkah-langkah dan menyelesaikan penambahan user baru tersebut sesuai panduan system seperti yang ditunjukkan pada gambar di bawah:

```
himawan@himawan-HP-Mini-210-1014TU:~$ sudo adduser test
[sudo] password for himawan:
Adding user `test' ...
Adding new group `test' (1001) ...
Adding new user `test' (1001) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for test
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
himawan@himawan-HP-Mini-210-1014TU:~$
```

Tambahkan user yang kedua dengan nama akili melalui perintah:

```
adduser akili
```

```

himawan@himawan-HP-Mini-210-1014TU:~$ sudo adduser akili
[sudo] password for himawan:
Adding user 'akili' ...
Adding new group 'akili' (1002) ...
Adding new user 'akili' (1002) with group 'akili' ...
Creating home directory '/home/akili' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for akili
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
himawan@himawan-HP-Mini-210-1014TU:~$

```

2. Cara pertama untuk menambahkan user tersebut ke dalam group sudo, dengan menjalankan perintah:

```
vim /etc/group
```

Cari bagian group sudo, lalu tambahkan nama user akili di belakangnya, sebagai tanda bahwa user akili masuk ke dalam grup sudo seperti yang tampak pada gambar di bawah:

```

himawan@himawan-HP-Mini-210-1014TU: ~
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,himawan
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:himawan
floppy:x:25:
tape:x:26:
sudo:x:27:himawan
audio:x:29:pulse
dip:x:30:himawan

```

Menjadi

```

himawan@himawan-HP-Mini-210-1014TU: ~
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,himawan
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:himawan
floppy:x:25:
tape:x:26:
sudo:x:27:himawan,akili
audio:x:29:pulse
dip:x:30:himawan
"/etc/group" 66L, 931C

```

Setelah itu simpan. Kemudian saya akan masuk berganti user dari user himawan, ke user akili dengan perintah:

Untuk mencoba hasilnya lakukan login dengan user akili, masukkan password yang dibutuhkan.

```
su akili
```

Selanjutnya jalankan perintah atau aplikasi yang seharusnya hanya bisa dijalankan oleh root atau administrator system, salah satunya adalah perintah atau aplikasi untuk melakukan penambahan user baru dengan nama ubuntu seperti pada gambar di bawah:

```

akili@himawan-HP-Mini-210-1014TU:/home/himawan$ sudo adduser ubuntu
Adding user 'ubuntu' ...
Adding new group 'ubuntu' (1003) ...
Adding new user 'ubuntu' (1003) with group 'ubuntu' ...
Creating home directory '/home/ubuntu' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:

```

Jika anda berhasil menjalankan perintah yang seharusnya hanya bisa dilakukan oleh user administrator seperti yang tampak pada gambar di atas, maka anda telah berhasil mendelegasikan hak akses administrator dengan cara yang pertama.

3. Cara kedua membuat sudoers user, misalkan menambahkan user test agar bisa menjalankan perintah-perintah dengan hak akses administrator:
 - a. Jalankan perintah sbb :

Dengan menggunakan user akili yang sudah diberi hak akses sebagai administrator system, lakukan perintah sudo visudo sbb :

```
sudo visudo
```

```

# User privilege specification
root    ALL=(ALL:ALL) ALL

```

tambahkan user test dibawah user rootm sehingga menjadi seperti:

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
test    ALL=(ALL:ALL) ALL
```

Keluar dari aplikasi editor, dengan menekan tombol CTRL+x dan simpan file ke dalam /etc/sudoers. Konfigurasi di atas dimaksudkan untuk mendelegasikan user test ke dalam list pemakai sudo dengan hak akses administrator.

- b. Setelah berhasil, coba dengan menjalankan aplikasi yang hanya bisa dijalankan oleh administrator system dengan user test tersebut, salah satunya adalah melakukan manajemen aplikasi dengan hasil seperti di bawah:

```
test@hinawan-HP-Mini-210-1014TU:/home/hinawan$ sudo apt-get remove mc
[sudo] password for test:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libssh2-1 mc-data
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  mc
0 upgraded, 0 newly installed, 1 to remove and 28 not upgraded.
After this operation, 1.454 kB disk space will be freed.
Do you want to continue? [Y/n]
```

Jika konfigurasi berhasil, maka anda akan melihat keluaran output seperti diatas, yang bisa melakukan instalasi aplikasi menggunakan user biasa.

TUGAS PRAKTIKUM : LAKUKAN PERCOBAAN 1 dan PERCOBAAN 2