Laporan Sementara
Operating System
Pengaturan Akses User di Linux

Nama: Gagas Amukti Nandaka
Kelas: 1 D4 Teknik Informatika B
NRP: 3120600032

PROGRAM STUDI TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2021

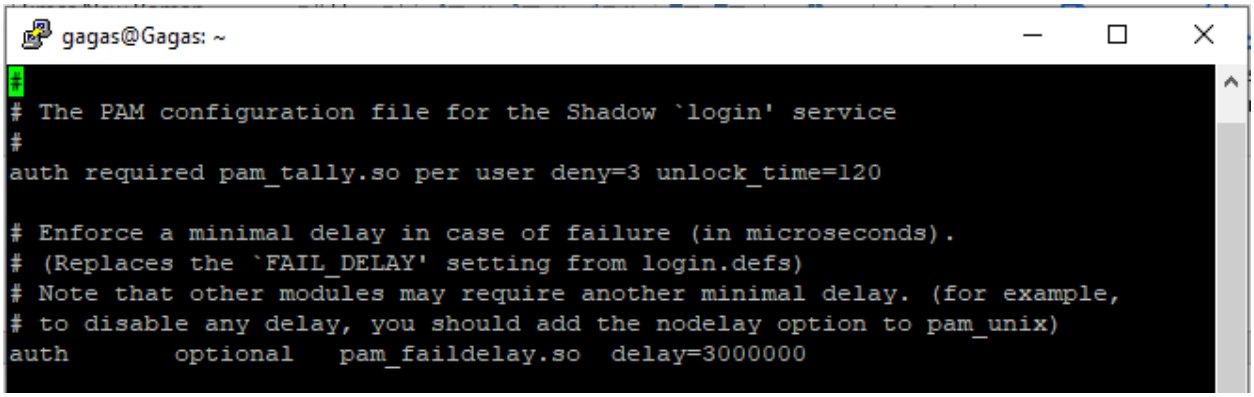
Percobaan 1 :

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

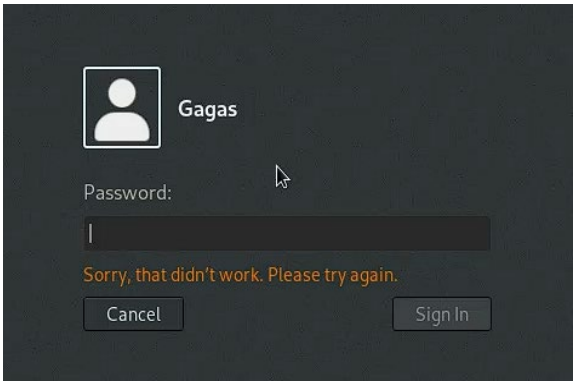


auth required pam_tally.so per user deny=3 unlock_time=120

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

Percobaan ke 2 salah



Percobaan ke 3 salah langsung tidak memperolehkan mengisi 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

```
 GNU nano 3.2                /etc/security/time.conf                 Modified

# this is an example configuration file for the pam_time module. Its syntax
# was initially based heavily on that of the shadow package (shadow-960129).
#
# the syntax of the lines is as follows:
#
#       services;ttys;users;times
#       login;*;testt;sasu0800-1800
#login;*;testt;sasu0800-1800
login;*;testt;sasu0800-1800
# white space is ignored and lines maybe extended with '\\n' (escaped
```

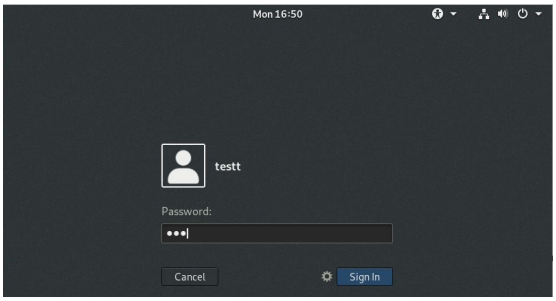
Karena tidak yakin saya coba beri yang ber # dan yang tidak

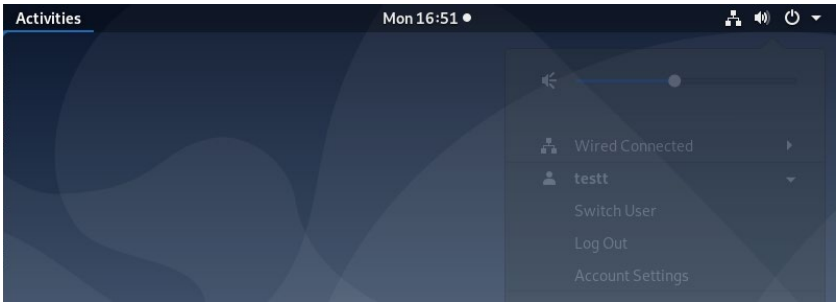
Kemudian tambahkan baris berikut pada file /etc/pam.d/login

```
 GNU nano 3.2                  /etc/pam.d/login                      Modified

#
# The PAM configuration file for the Shadow `login' service
#
#auth required pam_tally.so per user deny=3 unlock_time=120

# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the `FAIL_DELAY' setting from login.defs)
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
auth       optional   pam_faildelay.so  delay=3000000
account         required        pam_time.so
account         required        pam_nologin.so
# account         required        pam_time.so
# account         required        pam_nologin.so
# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth       required   pam_issue.so issue=/etc/issue
```

Skenario :

Setelah dilakukan percobaan berikut adalah hasil capture dimana Budi tidak diizinkan login karena hari ini adalah hari senin*





Praktikum gagal karena masih memperbolehkan login di hari senin walaupun semua percobaan sudah saya lakukan dengan benar

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 :

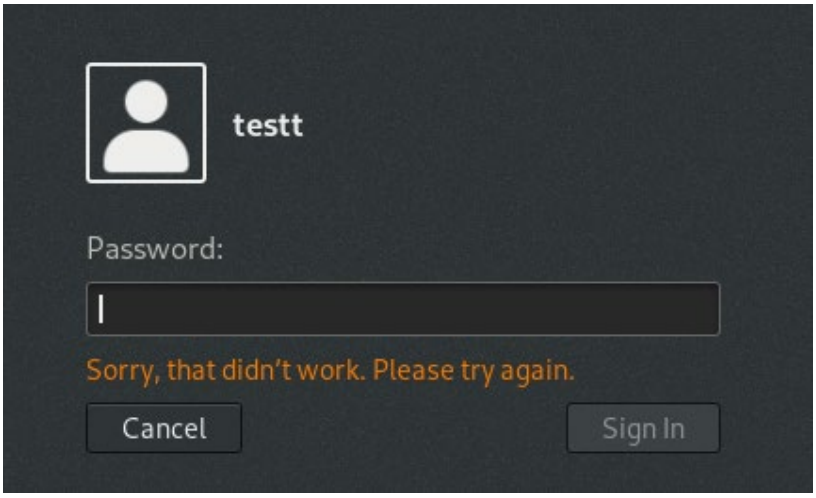
Untuk user budi dibatasi maksimum login kedalam sistem 2 kali.

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

```
  GNU nano 3.2              /etc/security/limits.conf              Modified

#         - chroot - change root to directory (Debian-specific)
#
#<domain>      <type>  <item>         <value>
#

#*               soft    core            0
#root            hard    core            100000
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4
#testt           -       maxsyslogins    2

# End of file
```

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

```
  GNU nano 3.2                  /etc/pam.d/login                    Modified


# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without this it is possible
# that a module could execute code in the wrong domain.
# When the module is present, "required" would be sufficient (When SELinux
# is disabled, this returns success.)
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinu$

# Sets the loginuid process attribute
session    required     pam_loginuid.so
session    required   pam_limits.so
#session    required   pam_limits.so

# SELinux needs to intervene at login time to ensure that the process
```



Percobaan gagal karena sudah 2 kali gagal masih bisa memasukan password lagi dan masih bisa login Kembali

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.

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

```
root@Gagas:/home/gagas# sudo apt-get install libpam-cracklib
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libpam-cracklib
0 upgraded, 1 newly installed, 0 to remove and 8 not upgraded.
Need to get 88.2 kB of archives.
After this operation, 119 kB of additional disk space will be used.
Get:1 http://kebo.pens.ac.id/debian buster/main amd64 libpam-cracklib amd64 1.3.
1-5 [88.2 kB]
Fetched 88.2 kB in 0s (178 kB/s)
Selecting previously unselected package libpam-cracklib:amd64.
(Reading database ... 137378 files and directories currently installed.)
Preparing to unpack .../libpam-cracklib_1.3.1-5_amd64.deb ...
Unpacking libpam-cracklib:amd64 (1.3.1-5) ...
Setting up libpam-cracklib:amd64 (1.3.1-5) ...
Processing triggers for man-db (2.8.5-2) ...
root@Gagas:/home/gagas#
```

setelah itu tembahkan baris berikut pada /etc/pam.d/passwd dengan cara :

Vi /etc/pam.d/common-password :

```
st_pass sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
password        required pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=0 minlen=8
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
```

https://www.youtube.com/watch?v=dwLCjZVEtpE