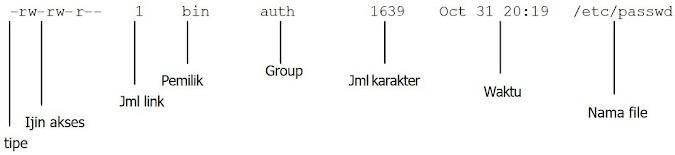
Sistem File

**Nama: Rizqi Bagus Andrean**

**Kelas: TI-1D**

**Absen: 25**

Pokok Bahasan:

• Sistem File

Tujuan Belajar:

Setelah mempelajari materi dalam bab ini, mahasiswa diharapkan mampu:

• Memahami atribut file dan ijin akses

• Memahami perintah untuk mengubah ijin akses suatu file • Menggunakan perintah-perintah untuk mengubah ijin akses

Dasar Teori:

1. ATRIBUT FILE

File mempunyai beberapa atribut, antara lain :

• Tipe file : menentukan tipe dari file, yaitu :

• Ijin akses : menentukan hak user terhadap file ini. • Jumlah link : jumlah link untuk file ini.

• Pemilik (Owner) : menentukan siapa pemilik file ini • Group : menentukan group yang memiliki file ini

• Jumlah karakter : menentukan ukuran file dalam byte

• Waktu pembuatan : menentukan kapan file terakhir dimodifikasi • Nama file : menentukan nama file yang dimaksud

Contoh:

2. IJIN AKSES

Setiap obyek pada Linux harus mempunyai pemilik, yaitu nama pemakai Linux (account) yang terdaftar pada */etc/passwd*.

Ijin akses dibagi menjadi 3 peran yaitu :

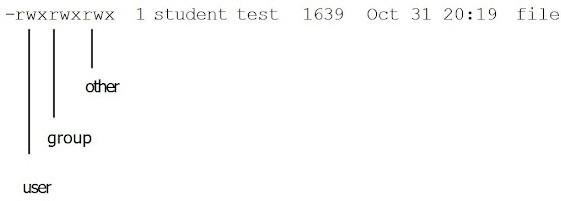
• Pemilik (Owner)

• Kelompok (Group) • Lainnya (Others)

Setiap peran dapat melakukan 3 bentuk operasi yaitu :

• Pada File

◦ R (Read) ➪ Ijin untukmembaca

◦ W (Write) ➪ Ijin untuk mengubah / membuat ◦ X (Execute) ➪ Ijin untuk menjalankan program

• Pada Direktori

◦ R (Read) ➪ Ijin untuk membaca daftar file dalam direktori ◦ W (Write) ➪ Ijin untuk mengubah/membuat file di direktori

◦ X (Execute) ➪ Ijin untuk masuk ke direktori (cd)

Pemilik File/Direktori dapat mengubah ijin akses sebagai berikut :

Format untuk mengubah ijin akses

chmod [ugoa] [= + -] [rwx] File(s)

chmod [ugoa] [= + -] [rwx] Dir(s) dimana

u = user (pemilik)

g = group (kelompok) o = others (lainnya)

a = all

Format lain dari chmod adalah menggunakan bilangan octal sebagai berikut

r w x

4 2 1 = 7

3. USER MASK

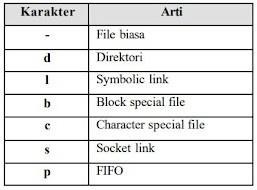
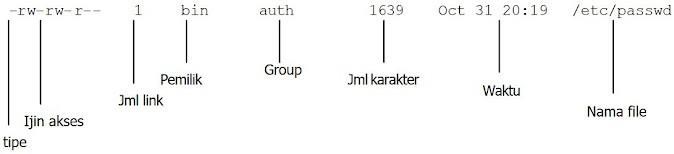
Untuk menentukan ijin akses awal pada saat file atau direktori dibuat digunakan perintah umask. Untuk menghitung nilai default melalui umask pada file, maka dapat dilakukan kalkulasi sebagai berikut :

Kreasi file (biasa) 6 6 6 Nilai umask 0 2 2

-6 4 4

Kreasi direktori 7 7 7 Nilai umask 0 2 2

-7 5 5

TUGAS PENDAHULUAN:

Jawablah pertanyaan- pertanyaan berikut ini:

1. Apa saja atribut file? Berikan contoh file dengan tipe file yang disebutkan pada dasar teori.

Atribut file adalah dimana sebuah file atau directori bisa eksis atau sebuah file mempunyai atribut yang berbeda antara sistem operasi satu dengan yang lainnya. Atribut file digunakan oleh sistem operasi untuk memisahkan tipe-tipe file. Setiap file di windows mempunyai atribut tersendiri sesuai dengan kepentingan file tersebut terhadap sistem. Misalnya, tipe file yang tidak boleh dihapus oleh user diberi attribut system, jadi ketika file manager (windows explorer) akan menampilkannya, file beratribut sistem tersebut tidak akan ditampilkan.

• Tipe file : menentukan tipe dari file, yaitu :

• Ijin akses : menentukan hak user terhadap file ini. • Jumlah link : jumlah link untuk file ini.

• Pemilik (Owner) : menentukan siapa pemilik file ini • Group : menentukan group yang memiliki file ini

• Jumlah karakter : menentukan ukuran file dalam byte

• Waktu pembuatan : menentukan kapan file terakhir dimodifikasi • Nama file : menentukan nama file yang dimaksud

Contoh:

Contoh file dengan tipe file yang disebutkan pada dasar teori:

• -rwr--=Tipe file biasa

• drw--=Tipefiledirektori

• Irw-- =Tipe file symbolic link • brw--=Tipefile block

2. Apa yang dimaksud ijin akses? Bagaimana contoh penggunaan perintah chmod untuk mengubah ijin akses.

Ijin akses bisa dibilang sebuah hak yang diberikan pada seluruh User atau file untuk melakukan sesuatu akses. Jadi hak akses ini dapat diatur sedemikian rupa supaya file atau

direktori itu hanya bisa di read, atau write, dan execute. Selain itu kita juga bisa mengatur bagaimana hak akses dari setiap user pada suatu file, atau direktori. Hal yang harus dikuasai dalam konfigurasi Hak Akses pada Linux:

1. Mengetahui Fungsi CHMOD

2. Mengetahui Fungsi setiap atribut tambahan dalam perintah CHMOD 3. Dapat mengatur hak akses bagi setiap user

4. Dapat mengatur hak akses bagi setiap group

5. Dapat merencanakan hak akses yang diaplikasikan di kehidupan sehari-hari atau Industri

Sesuai dengan semua yang harus kita kuasai kita harus memahami fungsi dari perintah "CHMOD" dan atribut tambahan pada perintah CHMOD tersebut. Chmod merupakan salah satu perintah pada Linux yang berfungsi untuk mengurangi atau memberikan izin ( Hak Akses ) pada suatu file atau direktori dan User serta Group.

Format untuk mengubah ijin akses

chmod [ugoa] [= + -] [rwx] File(s)

chmod [ugoa] [= + -] [rwx] Dir(s) dimana

u = user (pemilik)

g = group (kelompok) o = others (lainnya)

a = all

Format lain dari chmod adalah menggunakan bilangan octal sebagai berikut r w x

4 2 1 = 7

3. Berilah contoh penggunaan perintah umask untuk mengubah ijin akses.

User mask adalah kemampuan sistem operasi berbasis Linux untuk menambahkan pengaturan hak akses default untuk file-file baru (termasuk folder). Untuk tujuan edukasional, berikut adalah nilai-nilai oktal yang dapat digunakan untuk mengatur hak akses atas file:

0 – Read, Write, Execute (rwx) 1 – Read and Write (rw-)

2 – Read and Execute (r-x) 3 – Read only (r -)

4 – Write andExecute (wx) 5 – Writeonly (-w-)

6 – Execute only (- x)

7 – No permissions (—)

Untuk menghitung nilai defaultmelalui umask pada file, maka dapat dilakukan kalkulasi sebagai berikut :

Kreasi file (biasa) 6 6 6 Nilai umask 0 2 2

-6 4 4

Kreasi direktori 7 7 7 Nilai umask 0 2 2

-7 5 5

PERCOBAAN:

1. Login sebagai user.

2. Bukalah Console Terminal dan lakukan percobaan-percobaan di bawah ini kemudian analisa hasil percobaan.

3. Selesaikan soal-soal latihan

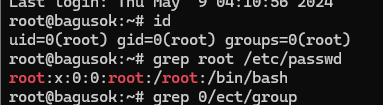
Percobaan 1 : Ijin Akses

1. Melihat identitas diri melalui etc/passwd atau etc/group, informasi apa yang ditampilkan?

$ id

$ grep <user> /etc/passwd

$ grep [Nomor group id]/etc/group



Analisa: Percobaan ini untuk mengetahui id dari pengguna dan mencetak atau memberikan informasi tentang nomor id pada group dan user.

2. Memeriksa direktori home

$ ls -ld /home/<user>

Analisa: Percobaan ini digunakan untuk mengetahui direktori user yang kita gunakan.



3. Mengubah Ijin akses (chmod). Perhatikan ijin akses setiap perubahan !

$ touch f1 f2 f3

$ ls -l

$ chmod u+x f1

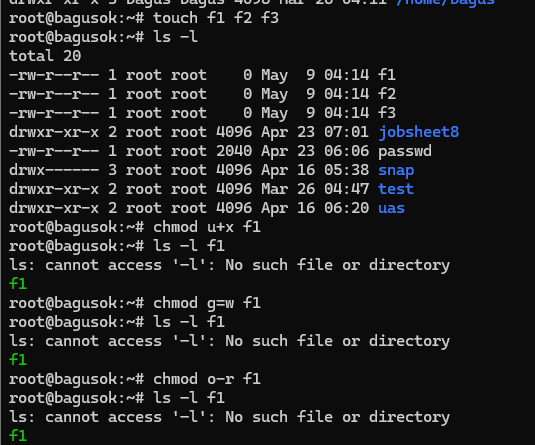
$ ls –l f1

$ chmod g=w f1

$ ls –l f1

$ chmod o-r f1

$ ls –l f1



$ chmod a=x f2

$ ls –l f2

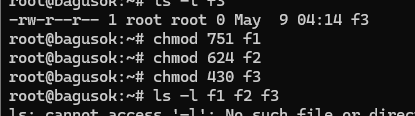
$ chmod u+x,g-r,o=w f3

$ ls –l f3

$ chmod 751 f1

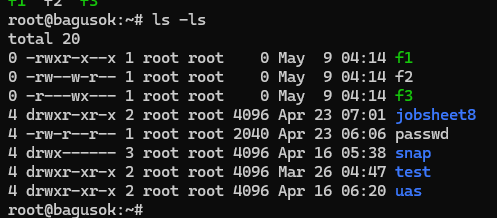
$ chmod 624 f2

$ chmod 430 f3



$ ls –l f1 f2 f3

Analisa: Percobaan ini digunakan

 untuk mengubah ijin akses dengan perintah chmod u+x f1 Maka hasilnya -rwx-w-r-1 untuk emngubah ijin akses kita lakukan perintah chmod g=w f1 maka hasilnya akan seperti ini -rwx-w 1.

4. Mengganti kepemilikan digunakan perintah chown. Masuk ke root untuk mengganti kepemilikan tersebut.

$ su root

$ echo Hallo > f1

$ ls –l f1



$ chown <user-baru> f1 contoh : chown student1 f1 $ ls –l f1



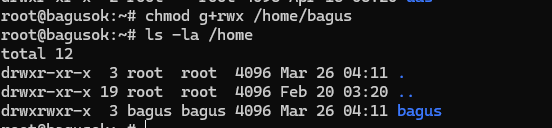
Analisa: Percobaan ini disini saya mengubah kepemilikan dengan perintah chown, untuk mengubah kepemilikan kita harus menambahkan user baru dengan contoh useradd students disitu terdapat kepemilikan file f1 yaitu students, dengan mengganti kepemilikan kita ketik perintah chown students f1 maka hasilnya yang tadinya kepemilikan file f1 adalah students setelah diganti kepemilikannya menjadi student1.

5. Ubahlah ijin akses home directory <user> (student) pada root sehingga <user-baru> (student1) pada satu group dapat mengakses home direktory <user>. Hal ini dimaksudkan agar file f1 yang sudah diubah kepemilikannya dapat diakses <user-baru>. Perubahan ijin akses home directory <user> hanya dapat dilakukan pada root.

$ chmod g+rwx /home/<user> contoh : chmod g+rwx /home/student

$ ls –l /home

$ exit



Analisa: Percobaan ini mengubah ijin akses home directory.

6. Sekarang cobalah untuk subtitute user ke <user-baru> (student1). Cobalah untuk mengakses file f1

$ su <user-baru>

$ ls –l f1

$ cat f1

$ exit

Analisa: Percobaan ini yaitu mensubtitusi user ke user baru, dan mengakses file f1.

7. Mengubah group dengan perintah $ chgrp

$ grep root /etc/group

$ grep other /etc/group



$ su

$ chgrp root f1

$ ls –l f1



$ chgrp <group-baru> f3





$ ls –l f3

$ exit

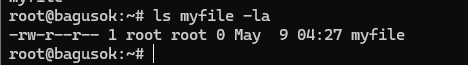
Analisa: Percobaan ini dengan perintah chgrp maka akan mengubah group. Sebelumnya dengan menambahkan addgroup terlebih dahulu.

Percobaan 2 : User Mask

1. Menentukan ijin akses awal pada saat file atau direktori dibuat

$ touch myfile

$ ls -l myfile



Analisa: Percobaan ini yaitu bertujuan untuk menetukan ijin akses awal pada saat direktori dibuat.

2. Melihat nilai umask

$ umask

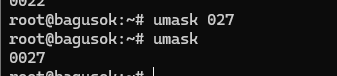


Analisa: Percobaan ini digunakan ntuk melihat nilai umask dengan perintah $umask.

3. Modifikasi nilai umask

$ umask 027

$ umask



$ touch file\_baru

$ mkdir mydir

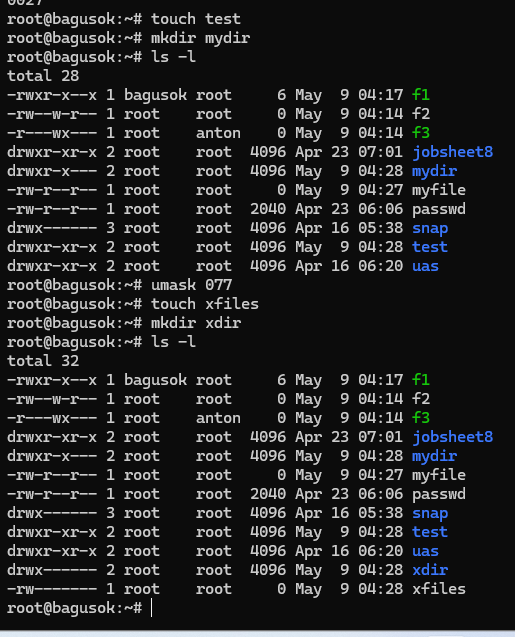
$ ls -l

$ umask 077

$ touch xfiles

$ mkdir xdir

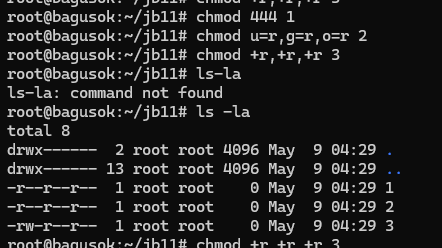
$ ls -l



Analisa: Percobaan ini bertujuan untuk memodifikasi nilai umask pada directory.

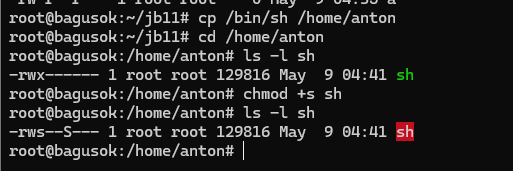
LATIHAN:

1. Lakukan tiga cara berbeda untuk setting ijin akses ke file atau direktori menjadi r--r--r--. Buatlah sebuah file dan lihat apakah yang anda lakukan benar.



Analisa : Saya membuat file dengan nama kadek dengan menggunakan perintah $touch. Ketika file ini saya lihat dengan menggunakan perintah ls -l maka terdapat informasi rw yang artinya file tersebut memberikan izin kepada saya untuk membaca (read) dan mengubahnya (write), untuk mengubah ijin akses file tersebut agar hanya dapat memberikan ijin read, saya menggunakan perintah pada gambar kedua.

2. Buatlah suatu kelompok. Copy-kan /bin/sh ke home directory. Ketik "chmod +s sh". Cek ijin akses sh pada daftar direktori. Sekarang tanyakan ke teman satu kelompok anda untuk mengubah ke home directory anda dan menjalankan program ./sh dan menjalankan id command. Apa yang terjadi. Untuk keluar dari shell tekan exit.



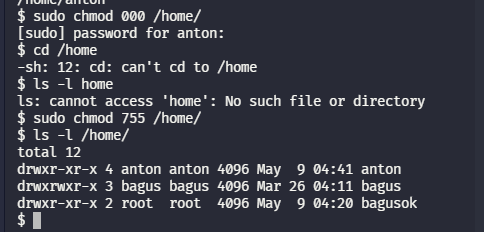
Analisa : Perintah chmod +s sh adalah perintah untuk mengubah file sh yang tadinya executable file menjadi socket link yang dapat dilihat perbedaannya saat kita lakukan ls -l sh maka nama file tersebut telah diberi tanda merah atau tanda yang berbeda dengan tanda sebelumnya. Selain itu perintah diatas juga menetukan hak izin akses untuk pengguna lain yang menggunakan file ini. Setelah itu saya lanjutkan dengan menjalankan perintah seperti ./ sh.

3. Hapus shdari home directory (atau setidaknya kerjakan perintah chmod –s sh)



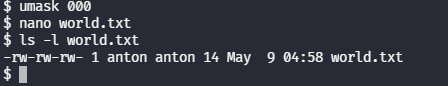
Analisa : Perintah chmod -s sh ini dapat menghapus atau mengembalikan bentuk file yang telah diubah menjadi socket link ke mode file sebelmnya. Dimana kita mencabut hak izin akses kepada pengguna lain untuk file ini.

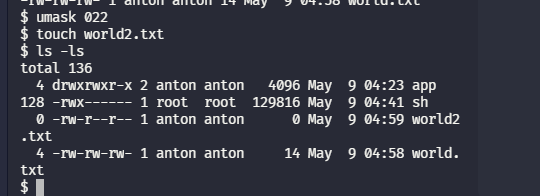
4. Modifikasi ijin akses ke home directory anda sehingga sangat privat. Cek apakah teman anda tidak dapat mengakses directory anda. Kemudian kembalikan ijin akses ke semula.



Analisa : Perintah chmod 000 tersebut merupakan perintah untuk menghapus / menghentikkan semua izin akses yang ada pada home baik itu izin untuk membaca, melihat dan lain-lain yang berhubungan dengan proses pengaksesan file atau directory. Untuk membuktikannya dapat dilakukan dengan perintah ls atau langsung dengan grafik pada home maka akan muncul bahwa data tidak dapat dibuka atau tidak memiliki izin. Sedangkan cara untuk mengembalikan pengaturannya seperti semula dapat dilakukan dengan perintah chmod 755.

5. Ketikkan umask 000 dan kemudian buatlah file yang bernama world.txt yang berisi beberapa kata "hello world". Lihat ijin akses pada file. Apa yang terjadi? Sekarang ketikkan umask 022dan buatlah file bernama world2.txt. Apakah perintah tersebut lebih berguna



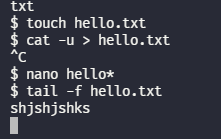


?

Analisa : $ mask 000 pada perintah diatas berfungsi untuk mengatur izin akses file yang akan

dibuat setelahnya dengan format pemberian izin akses untuk dapat membaca dan menulis atau melakukan perubahan yang ditandai dengan format -rw -r –r--, karena 2 adalah blangan octal dari read(r) yang apabila dijalankan menjadi seperti berikut:

6. Buatlah file yang bernama "hello.txt" pada home directory menggunakan perintah cat -u >hello.txt. Tanyakan ke teman Anda untuk masuk ke home directory Anda dan menjalankan tail -f hello.txt. Sekarang ketikkan beberapa baris dalam hello.txt. Apa yang terjadi pada layer teman Anda ?



Analisa : Kedua perintah diatas merupakan perintah untuk standar input dan output. Misalnya perintah cat -u > hello.txt ini merupakan perintah membelokan standar output ke file hello.txt dan untuk berhenti dapat dilakukan dengan menekan Ctrl + C.

Kesimpulan:

• Sebuah file dapat kita manajemen atau dapat kita atur sesuai dengan tingkat keamanan yang ingin kita tentukan pada file.

• Untuk proses ini dapat kita lakukan dengan menggunakan manajemen system file dimana sebuah file atau directory dapat kita tentukan hak izin aksenya, guna untuk menjaga data

yang kita miliki.

• Atribut file adalah dimana sebuah file atau directori bisa eksis atau sebuah file mempunyai atribut yang berbeda antara sistem operasi satu dengan yang lainnya. Atribut file digunakan

oleh sistem operasi untuk memisahkan tipe-tipe file. Setiap file di windows mempunyai atribut tersendiri sesuai dengan kepentingan file tersebut terhadap sistem. Misalnya, tipe file yang tidak boleh dihapus oleh user diberi attribut system, jadi ketika file manager (windows explorer) akan menampilkannya, file beratribut sistem tersebut tidak akan ditampilkan.

• Ijin akses bisa dibilang sebuah hak yang diberikan pada seluruh User atau file untuk melakukan sesuatu akses. Jadi Hak akses ini dapat diatur sedemikian rupa supaya file atau

direktori itu hanya bisa di read, atau write, dan execute. Selain itu kita juga bisa mengatur bagaimana hak akses dari setiap user pada suatu file, atau direktori.

• User mask adalah kemampuan sistem operasi berbasis Linux untuk menambahkan pengaturan hak akses default untuk file-file baru (termasuk folder).