System Administration

Session 3 CONTENT

- Users
- Groups
- Switching users
- sudo usage
- User Password Aging
- Files and Directories Ownership
- Files and Directories Permissions

Users types

Traditionally the root user was the responsible for running services, once a service is hacked the whole system is hacked.

Types of users:

- root user (has all privileges, can do anything)
- normal user (accounts for persons going to login on the OS)
- service user (as a more security layer can deal only with the service& can’t login to OS)

System deals with the user based on his UID

/etc/passwd

/etc/passwd file is a database for system users

loginame:x:uid:gid:comment:home-directory:login-shell

Included fields are:

- Login name
- Password (in very old distros)
- User Id (uid)
- Group Id (gid)
- Comment about the user (full name)
- Home Directory
- Login shell

Creating/Modifying users

You can use the following commands to create/modify users

```
useradd [options] username
usermod [options] username
```

The useradd command populates user home directories from the /etc/skel directory.

Deleting users

To delete a user account you can

1. Manually remove the user from
   - /etc/passwdfile
   - /etc/shadow file
   - /etc/group file
   - remove the user's home directory (/home/username)
   - mail spool file (/var/spool/mail/username)
2. Use the userdelcommand.

```
userdel[-r] username
```

Creating/Modifying Groups

You can use the following commands to create/modify groups

```
groupadd [options] groupname
groupmod [options] groupname
```

/etc/group file

groupname:x:gid:comma-separatedlist of group members

To **delete** a group we can use

```
groupdel groupname
```

/etc/sudoers file

The sudoers file is a file Linux and Unix administrators use to allocate system rights to system users. This allows the administrator to control who does what.

Linux is built with security in mind. When you want to run a command that requires root rights,

Linux checks your username against the sudoers file.

User Switching

You can switch between users by using

```
su [-] [username]
```

After switching into several users, it is a sever issue to know your current (effective) user

```
whoami command
id command
```

User Password Aging

The chage command sets up password aging

```
chage[options] username
```

Options

-m:	to change the min number of days between password changes
-M:	to change the max number of days between password changes
-E :	change the expiration date for the account
-W:	change the number of days to start warning before a password change will be required

Quiz

How can I create many users at once?

Ownership & Permissions

Every file and directory has both **user** and **group** ownership. A newly-created file will be owned by:

- The user who creates it
- That user's primary group

File ownership can be changed using

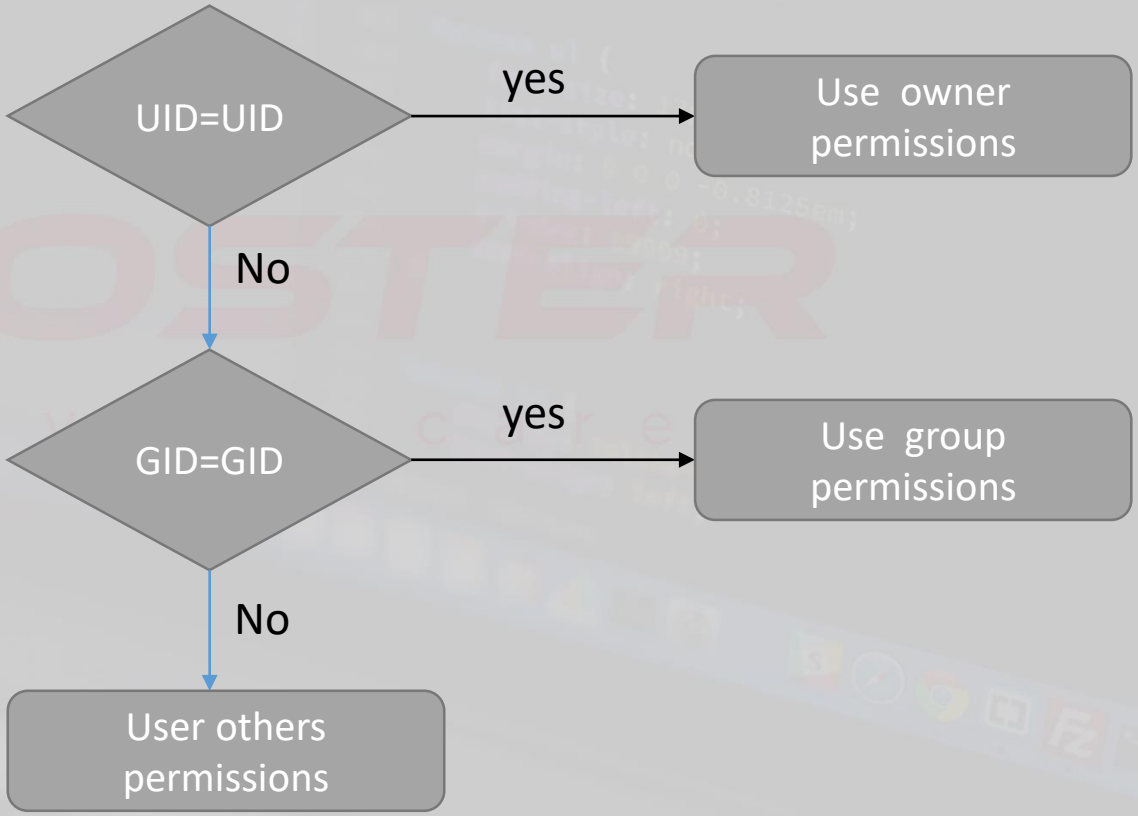
`chown command`

`chgrp command`

Ownership & Permissions

- User permissions override group permissions, which override other permissions.

- All permissions in Linux are set directly on each file or directory (not inherited)



Changing Permissions

```
chmod permissions filename/dir
```

1- Symbolic method:

- Who is u, g, o, a (for user, group, other, all)
- What is +, -, = (for add, remove, set exactly)
- Which is r, w, x (for read, write, executable)

2- Numeric method:

r=4, w=2, x=1

Questions?!

Thank YOU!

boost your career