OPEN SOURCE OS (LINUX)
برمجة مفتوحة المصدر

LECTURE 3

BY SCHOLAR PHD. EDRIS HUSSAIN MOHAMMED

DEPARTMENT OF INFORMATION SYSTEMS

EDRUIS.HESSAN@GMAIL.COM

2025

Lecture 3:

- Users
- Groups
- Permissions
- Permissions Management

Introduction

- Linux uses groups to help you manage users, set permissions on those users.
- Normally Linux computers have two user accounts—

  1. root account, which is the super user that can access everything on the PC, make system changes, and administer other users.
  2. normal users

User Accounts Files

– /etc/passwd This file contains the user account

information for the system.

– /etc/shadow This file contains encrypted passwords for the user accounts.

– /etc/group This file contains the list of groups.

– /etc/gshadow each line in this file represents a record for a single group.

The Superuser (root)

- By default, one account has elevated privileges to issue any command, access any file, and perform every function, it is the Superuser, which is called root
- root User ID is 0 and group number is 0
- Why root account should be limited?

– Inexperienced users can cause serious harm

– Use of root for non-privileged tasks unnecessary and can be open to attack

– Security and privacy violations – root can look at anyone’s files

- Recommended Settings for root:
    - ❖Disable root account locally and remotely
    - ❖If not then disable or limit what root can do remotely
    - ❖Ensure a strong password

Superuser Privileges

- What usually works best is short periods of superuser privilege, only when necessary
- Obtain privileges, complete task, relinquish privileges
- Most common ways are su and sudo
- Some Linux distributions such as Ubuntu disable the root account by default
- Must rely on sudo to obtain privilege.

su

- Short for substitute or switch user
- Syntax: su [options]
- After issuing command, prompted for that root’s password
- A new shell opened with the superuser privileges
- Once done issuing commands, must type exit

sudo

- Allows user to issue a single command as root
- Syntax:

    sudo command

- In Ubuntu the root account is disabled by default.
- In Ubuntu the user created during installation will have certain administrative privileges, since it will be member of sudo group by default so it can run commands with superuser privileges
- The files and folders created with sudo will be owned by root

Creating and Managing User and Groups

- Creating a User

    Syntax: adduser username

    example: adduser azad

- You will be asked for certain information which you can keep empty except full name (use same username in this course) and provide password. (recommended to use 12345)
- Whenever a new user is created a group with same name will be created automatically.

Deleting a User

Syntax: userdel –r username

example: userdel –r azad

- Use the –r option in the command line to remove the home directory when you delete the user.

Creating/Deleting a Group

- To create a group use groupadd like below

  Syntax:

  groupadd options groupname
- Options:

–g Specifies a GID for the new group.

–p Specifies a password for the group.

–r Specifies that the group being created is a system group

example: groupadd groupc

- To delete a group use groupdel like below

  Syntax: groupdel group_name

  example: groupdel test2

Add/Remove a User to/from a Group

- To add an existing user account to a group on your system, use the usermod command,

  sudo usermod -a -G groupname username
- For example, to add the user azad to the group groupc , use
- the following command:

  sudo usermod -a -G groupc azad
- To view the groups the current user account is assigned to, run the groups command. You'll see a list of groups.
- groups
- To remove a user from a group, use the gpasswd command with the -d option as follows.

The end