Lab 2 : Managing User and Group Accounts

Objectives:

- Manage groups, including creating, modifying, and deleting group accounts
- Learn how to create group administrators
- Manage users, including creating, modifying, and deleting user accounts
- Develop security policy for user/group access control

Part1. Managing Group Accounts

STEP 1. Open a terminal window.

Answer: Click **Applications** in the menu bar, then **Utilities**, then **Terminal**.

STEP 2. Display the current user's ID and group membership.

Answer: Enter the following:

```
id
```

STEP 3. Display the group membership of the root account.

Answer: Enter the following:

```
groups root
```

STEP 4. Run the correct command to determine the user owner and group owner of the **/etc/group** file.

Answer: Enter the following:

```
ls -l /etc/group
```

STEP 5. Display the group account information for the games group.

Answer: Enter the following:

```
grep games /etc/group
```

STEP 6. Display the group password information for the games group.

Answer: Enter the following:

```
grep games /etc/gshadow
```

STEP 7. Run the **su -** following command to switch to the root account (and provide the root password when

prompted).

Answer: Enter the following:

```
su -
```

STEP 8. Create a new group named test.

Answer: Enter the following:

```
groupadd test
```

STEP 9. Display the group account information for the test group.

Answer: Enter the following:

```
grep test /etc/group
```

STEP 10. Change the group name of the test group to newtest.

Answer: Enter the following:

```
groupmod -n newtest test
```

STEP 11. Add the student account as a secondary member of the newtest group without overriding this

user’s current group membership.

Answer: Enter the following:

```
usermod -G newtest -a student
```

Part B: Managing Group Administrators

Scenario: In this lab you will be asked to provide a “goal” rather than be told specifically which steps to take. It is up to you to achieve the end result based on what you have learned regarding this topic. Create a new group named **eng** and add the student user to this group. Make the student user a group administrator. To test this, add the bin user to the **eng** group while logged in as the student user and then verify this new group membership.

Answer:

STEP 1. Open a terminal window by clicking **Applications** in the menu bar, then **Utilities**, then **Terminal**.

STEP 2. Switch to the root account by entering the following:

```
su -
```

STEP 3. Create the eng group by entering the following:

```
groupadd eng
```

STEP 4. Add student to the eng group by entering the following:

```
usermod -G eng -a student
```

STEP 5. Make student a group administrator by entering the following:

```
gpasswd -A student eng
```

STEP 6. Use the following command to return to the student account:

```
exit
```

STEP 7. Execute the following command to add the bin user to the eng group:

```
gpasswd -a bin eng
```

STEP 8. Verify the new group membership by entering the following:

```
groups bin
```

Part C : Managing User Accounts

These labs should be performed on the Ubuntu operating system that you installed in Lab 1, “Distributions and Key Components.”

STEP 1. Open a terminal window.

Answer: Click **Applications** in the menu bar, then **Utilities**, then **Terminal**.

STEP 2. Execute the correct command to display user account information (including the login shell and home directory) for the bin account.

Answer: Enter the following:

```
grep bin /etc/passwd
```

STEP 3. Execute the correct command to display user password information (including the encrypted password and password aging) for the bin account.

Answer: Enter the following:

```
grep bin /etc/shadow
```

STEP 4. The command in step 3 should have failed. Execute the correct **su** command to change your account, so the command from step 3 will be successful when executed.

Answer: Enter the following:

```
su -
```

STEP 5. Create a new user named jake and explicitly use options to create the home directory **/home/jake** for this user.

Answer: Enter the following:

```
useradd -d /home/jake -m jake
```

STEP 6. Set a password for the jake user to a password of your choosing.

Answer: Enter the following:

```
passwd jake
```

Then, when prompted, enter password of your choice.

STEP 7. Run the correct command to display the default values used when a new account is created.

Answer: Enter the following:

```
useradd -D
```

STEP 8. Using the **less** command, display the file that contains the password aging defaults.

Answer: Enter the following:

```
less /etc/login.defs
```

STEP 9. Using the **less** command, display the file that contains the default login shell.

Answer: Enter the following:

```
less /etc/login.defs
```

STEP 10. Delete the jake user and his home directory, using a single command.

Answer: Enter the following:

```
userdel -r jake
```

Part D : Securing User Accounts

This lab focuses on developing and enforcing a security policy for user and group account management in Linux. The policy is designed to enforce **least privilege**, **accountability**, and **secure practices** for password management, authentication, and account monitoring.

Security Policy

i) User Account Management

- Each user must have a **unique account**; no shared accounts.
- Accounts created **only by administrators** after approval.
- Home directories must have permissions set to **700**.
- Password requirements:
  - Minimum **12 characters**.
  - Must include **uppercase, lowercase, numbers, and symbols**.
  - Expire every **90 days**.
  - Cannot reuse the **last 5 passwords**.

ii) Group Account Management

- Users are members of **only required groups**.
- Only admins belong to **sudo/wheel groups**.
- **Direct root access** is not allowed; use sudo.
- Group memberships are reviewed **quarterly**.

iii) Password & Authentication Controls

- **PAM** must enforce authentication policies.
- **MFA required** for admin users.
- Accounts locked after **5 failed login attempts**.
- Password aging enforced via chage.

iv) File & Directory Permissions

- /etc/passwd → 644
- /etc/shadow → 640 (root-only)
- Sensitive files must not be **world-readable**.
- Default **umask = 027**.

v) Account Monitoring & Auditing

- Enable logging of login attempts (/var/log/secure).
- Use last, lastlog, and faillog to review activity.
- Use **auditd** to track account changes.
- Disable **inactive accounts immediately**.

vi) Special Accounts

- **Service accounts** cannot be used for interactive login.
- **Root SSH login disabled** (PermitRootLogin no).
- **Guest accounts prohibited**.

Enforcing the Security Policy

Follow the steps below to enforce this security policy on your Linux system.

Step 1: Create a User and Group

1. Create a new group:

```
sudo groupadd securitylab
```

2. Create a new user:

```
sudo useradd -m -s /bin/bash -G securitylab student1
```

3. Set a password:

```
sudo passwd student1
```

Step 2: Configure Password Aging

1. Set password to expire every 90 days:

```
sudo chage -M 90 student1
```

2. Warn user 14 days before expiration:

```
sudo chage -W 14 student1
```

Step 3: Enforce Account Lockout After Failed Logins

1. Edit PAM configuration:
    - **Debian/Ubuntu** → /etc/pam.d/common-auth
    - **RHEL/CentOS** → /etc/pam.d/system-auth
2. Add:

```
auth required pam_tally2.so deny=5 unlock_time=600 onerr=fail audit
```

3. Test by attempting multiple failed logins and take screenshots for your lab submission.

Step 4: Disable Root SSH Access

1. Edit SSH config:

    ```
    sudo nano /etc/ssh/sshd_config
    ```

2. Set:

    ```
    PermitRootLogin no
    ```

3. Restart SSH service:

```
sudo systemctl restart sshd
```

Step 5: Monitor Accounts

1. View login history:

```
last
```

2. Check failed login attempts:

```
faillog -a
```

3. Audit account modifications:

```
sudo ausearch -m USER_ACCT
```

Submission Instructions

- Save your documentation (screenshots + command outputs) as a **Word file**.
- Export the Word file as a **PDF**.
- Use the following filename format:
- Lab1-FirstName-Lastname-StdNo.PDF
- Upload your PDF to the **Learning Hub** before the deadline (Sep 21st at 11:59).
