Lab A3 – User, Group, and Permission Management on Red Hat Enterprise Linux

Ayoub Zouargui
Master 1 – Networks and Embedded Systems
University of Algiers 1 (2025–2026)
https://github.com/AyoubSecurity

Objective

The objective of this lab is to practice user and group management on Red Hat Enterprise Linux. The lab demonstrates how Linux enforces access control through explicit permissions, ownership, and group membership, which are essential concepts in system administration and security.

Lab Environment

Operating System: Red Hat Enterprise Linux

Machine: Single RHEL administrative workstation (virtual machine)

Access Level: Local user with sudo privileges

Scenario

The system administrator must manage multiple users with different roles. Administrative users and application users must be separated, and access to shared directories must be controlled using Linux permissions following the principle of least privilege.

Step-by-Step Procedure

1. Verify Current User and Privileges

The following commands were executed to confirm the current user identity and group memberships:

```
whoami
id
```

2. Create User Groups

Two groups were created to represent administrative and application roles:

```
sudo groupadd admins
sudo groupadd developers
```

Group creation was verified using:

```
getent group admins
getent group developers
```

3. Create User Accounts

Two user accounts were created with home directories and Bash as the default shell:

```
sudo useradd -m -s /bin/bash ayoub.admin
sudo useradd -m -s /bin/bash devuser1
```

4. Set User Passwords

Passwords were assigned to the newly created users:

```
sudo passwd ayoub.admin
sudo passwd devuser1
```

5. Assign Users to Groups

Users were assigned to their respective groups:

```
sudo usermod -aG admins ayoub.admin
sudo usermod -aG developers devuser1
```

Membership was verified using:

```
id ayoub.admin
id devuser1
```

6. Review Linux Account Databases

The system account files were inspected in read-only mode:

```
cat /etc/passwd | tail -5
sudo cat /etc/shadow | tail -5
cat /etc/group | tail -5
```

7. Create a Shared Project Directory

A shared directory was created for application users:

```
sudo mkdir /srv/project
sudo chown :developers /srv/project
sudo chmod 2770 /srv/project
```

The `setgid` bit ensures that new files inherit the group ownership.

8. Permission Testing

The developer user tested write access:

```
su - devuser1
cd /srv/project
touch testfile.txt
exit
```

The administrator user tested access and was correctly denied due to lack of group membership:

```
su - ayoub.admin
cd /srv/project
```

Security Observation

Administrative users do not bypass filesystem permissions. Access is granted only through ownership, group membership, access control lists, or root privileges. This behavior enforces strict and predictable security boundaries.

Skills Acquired

Linux user and group administration

Permission and ownership configuration

Practical application of least-privilege principles

Understanding of Linux access control mechanisms

Conclusion

This lab demonstrates how Linux enforces access control through explicit configuration. Proper user and permission management is essential for maintaining secure and manageable enterprise systems.