

# Linux User & Access Management

## Scenario Overview

In the final phase of Project Phoenix, I was assigned the role of **Keeper of the Keys**, responsible for controlling system access. This lab focused on **secure user onboarding, group management, password configuration, and account lockdown**, simulating real-world identity and access management (IAM) responsibilities.

---

## Access Control Objectives

- Onboard a new senior developer securely
  - Ensure proper home directory creation
  - Assign secure authentication credentials
  - Grant correct group access without privilege escalation
  - Immediately revoke access for a departing contractor while preserving audit data
- 

## Step 1: Create a New User Account (Brenda Smith)

### Requirement

- Username format: `first_initial.last_name`
- Username: `b.smith`

### Command Used

```
sudo useradd b.smith
```

```
labex:project/ $ sudo useradd b.smith
labex:project/ $ grep "b.smith" /etc/passwd
b.smith:x:5002:5004::/home/b.smith:/bin/sh
labex:project/ $ id b.smith
uid=5002(b.smith) gid=5004(b.smith) groups=5004(b.smith)
labex:project/ $
```

## Step 2: Create a Home Directory for the New User

To ensure a secure personal workspace, the user was recreated with a home directory.

### Command Used

```
sudo userdel b.smith
sudo useradd -m -d /home/b.smith b.smith
```

### Result

- Home directory created at `/home/b.smith`
- Ownership automatically assigned to `b.smith`

```
labex:project/ $ man useradd
labex:project/ $ userdel b.smith
userdel: Permission denied.
userdel: cannot lock /etc/passwd; try again later.
labex:project/ $ sudo userdel b.smith
labex:project/ $ id b.smith
id: 'b.smith': no such user
```

```
labex:project/ $ man useradd
labex:project/ $ userdel b.smith
userdel: Permission denied.
userdel: cannot lock /etc/passwd; try again later.
labex:project/ $ sudo userdel b.smith
labex:project/ $ id b.smith
id: 'b.smith': no such user
```

---

### Step 3: Assign an Initial Password

The account was unlocked by setting an initial password.

#### Command Used

```
sudo passwd b.smith
```

(Password set during interactive prompt)

```
labex:project/ $ sudo passwd b.smith
New password:
Retype new password:
passwd: password updated successfully
labex:project/ $ sudo grep "^b.smith:" /etc/shadow
b.smith:$y$j9T$dLSXe8ucdbgcumVXhWN82.$B7vfpbjTAvVnJycxlwHy2F4oFWtZc8XM4ZjAnFk9y9D:20462:0:99999:7:::
```

---

### Step 4: Add User to the **developers** Group

Brenda required access to Project Phoenix resources without removing existing group memberships.

#### Command Used

```
sudo usermod -aG developers b.smith
```

#### Verification (Optional)

```
groups b.smith
```

```
labex:project/ $ groups b.smith
b.smith : b.smith
labex:project/ $ usermod -aG developers b.smith
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
labex:project/ $ sudo usermod -aG developers b.smith
labex:project/ $ groups b.smith
b.smith : b.smith developers
labex:project/ $
```

---

## Step 5: Lock a Departing Contractor's Account

John Doe (`j.doe`) was identified as a security risk. His account was locked **without deleting user data**, preserving files for compliance and audit purposes.

### Command Used

```
sudo usermod -L j.doe
```

### Result

- Account disabled
- Home directory and files preserved
- Login access fully revoked

```
labex:project/ $ id j.doe
uid=5001(j.doe) gid=5001(j.doe) groups=5001(j.doe)
labex:project/ $ sudo usermod -L j.doe
labex:project/ $ sudo grep "^j.doe:" /etc/shadow
j.doe:!:20462:0:99999:7:::
labex:project/ $ sudo usermod -U j.doe
usermod: unlocking the user's password would result in a passwordless account.
You should set a password with usermod -p to unlock this user's password.
labex:project/ $ sudo grep "^j.doe:" /etc/shadow
j.doe:!:20462:0:99999:7:::
labex:project/ $
```

---

## Skills Demonstrated

- Linux user account creation (`useradd`)
- Home directory management
- Password administration (`passwd`)
- Group membership control (`usermod`)
- Account lockdown for security incidents
- Identity & Access Management (IAM) best practices
- Compliance-aware security decisions