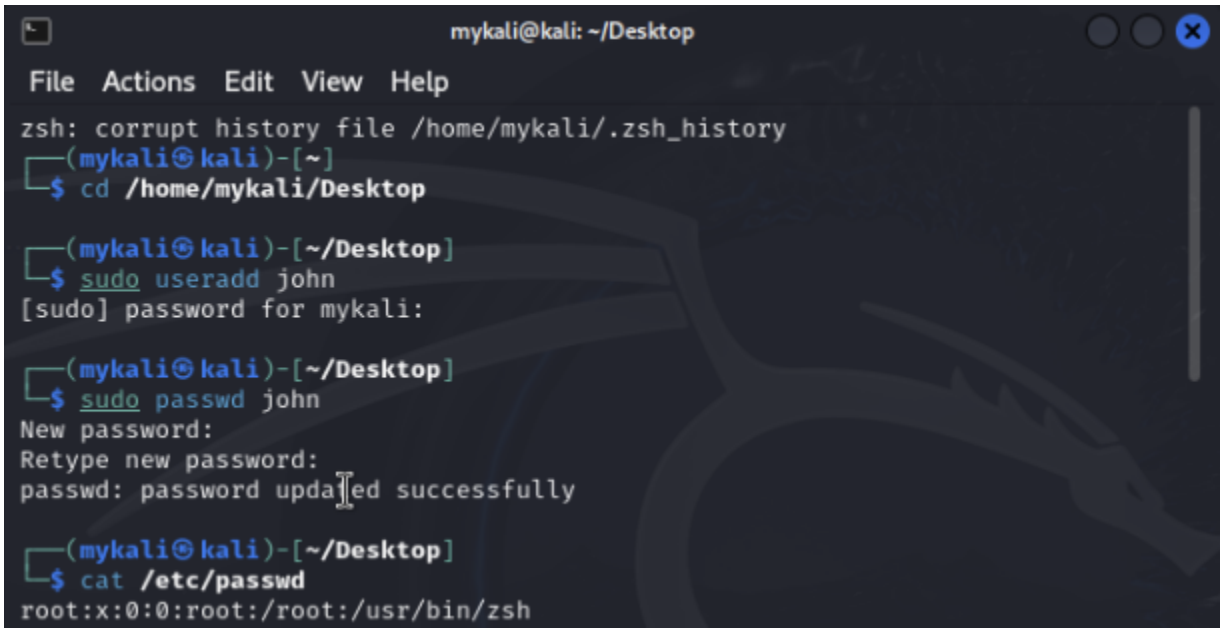
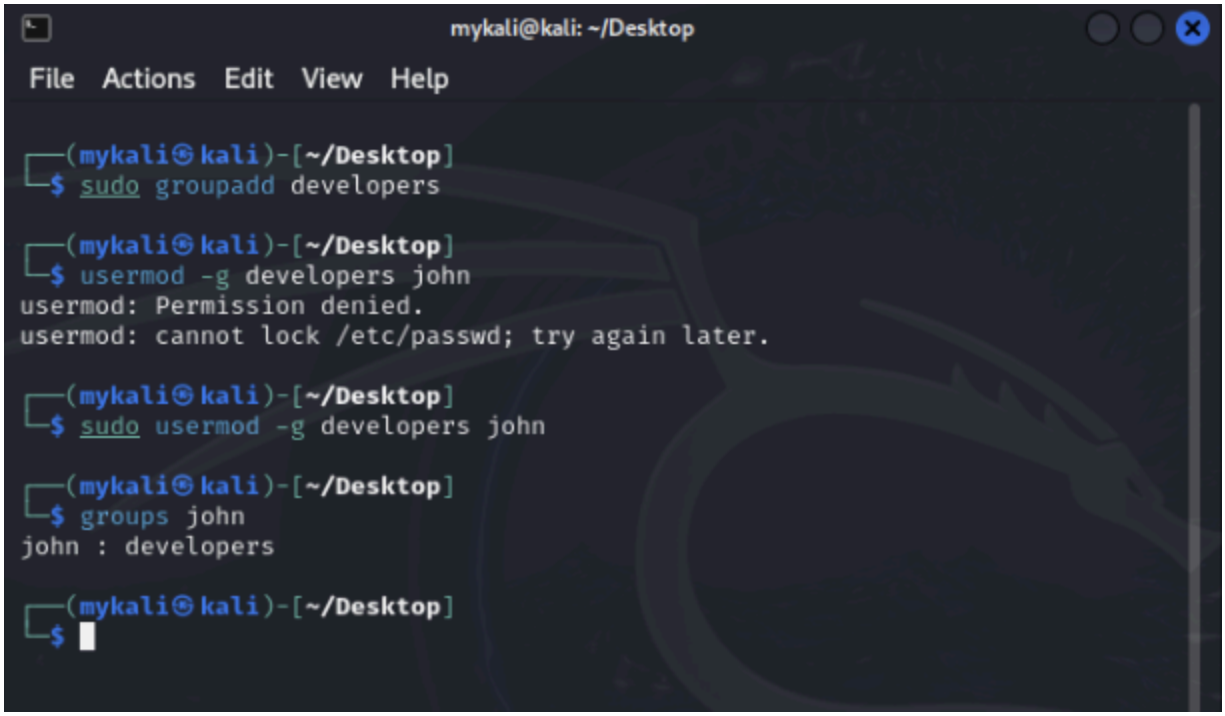
Objective 1: Create a New User

Task 1: Use the useradd command to create a new user
- sudo useradd john
Task 2: Set a password for the new user using passwd
- sudo passwd john
Task 3: Verify the new user by checking the /etc/passwd file
- cat /etc/passwd



Objective 2: Add a User to a Group

Task 1: Create a new group using groupadd
- sudo groupadd developers
Task 2: Add an existing user to the group using usermod
- sudo usermod -g developers john
Task 3: Verify that the user is added to the group by using the groups command
- groups john



Objective 3: Modify User Information

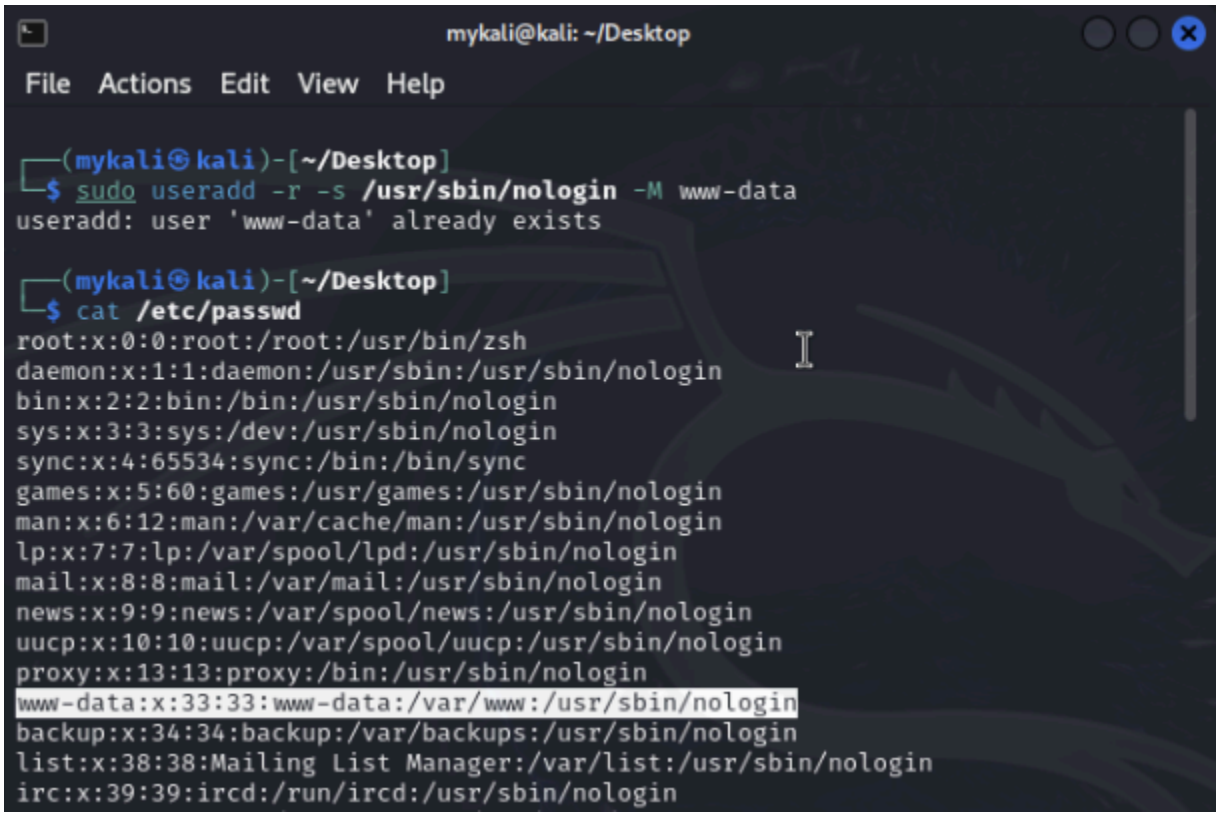
Task 1: Modify the home directory for user john using usermod
- sudo usermod -d /home/mykali john
Task 2: Change the default shell for john to /bin/bash
- sudo usermod -s /bin/sh john {TO CREATE SHELL}
- sudo usermod -s /bin/bash john {TO CHANGE SHELL}
Task 3: Change the user's full name using the chfn command
- sudo chfn -f johnwick john
Task 4: Verify the changes using grep john /etc/passwd
- grep john /etc/passwd

Objective 4: Delete a User

Task 1 and Task 2: Delete the user john using the userdel command and Ensure the user's home directory and files are removed by using userdel -r
- sudo userdel -r john
Task 2: Verify the deletion by checking the /etc/passwd file
- cat /etc/passwd

Objective 5: Create a System User

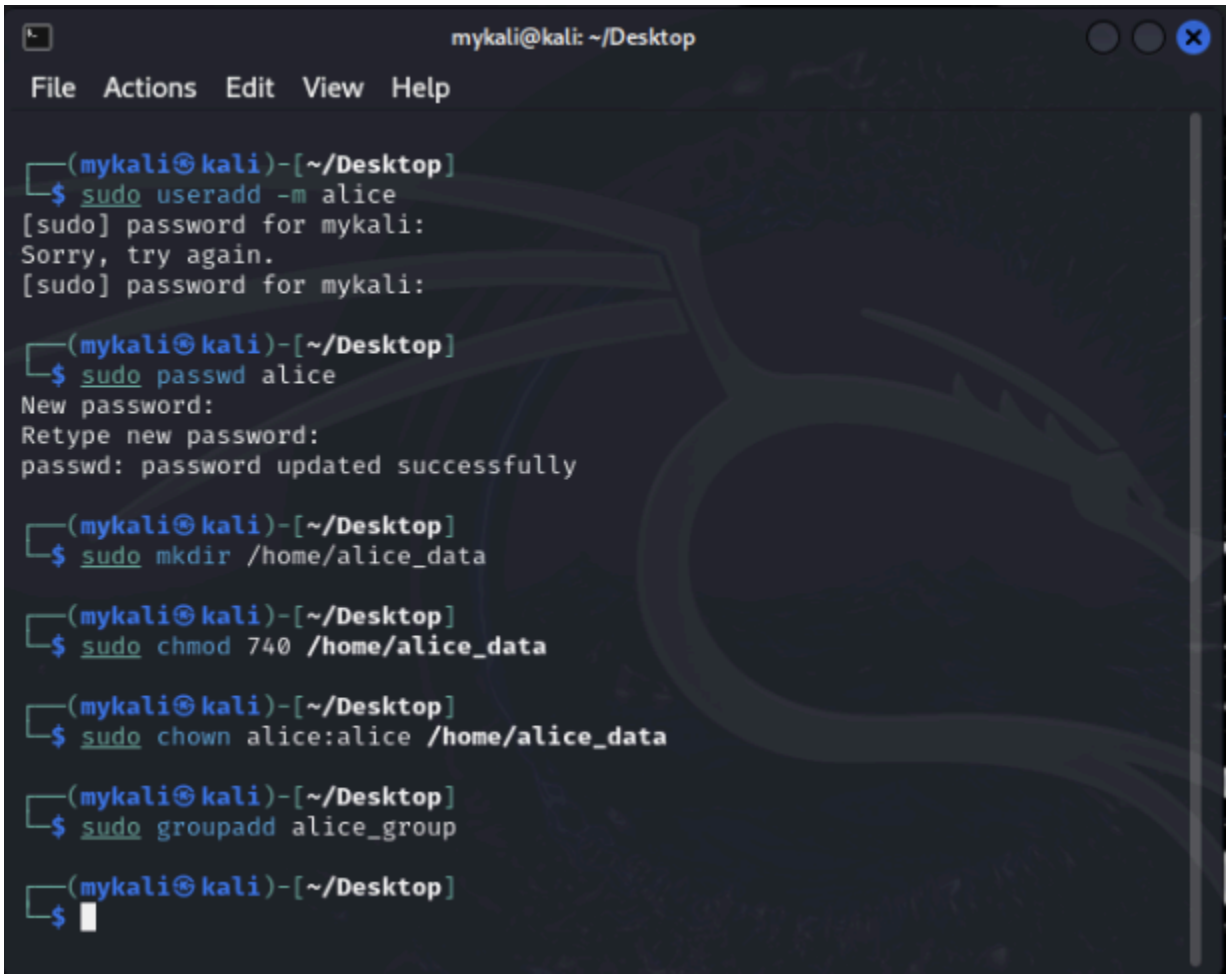
Task 1 and Task 2: Create a system user for an application (e.g., www-data for web server users) and Ensure that the system user has no login shell and that no home directory is created by using useradd -r
- sudo useradd -r -s /usr/sbin/nologin -M www-data
NOTE: -r: Creates a system user.
-s /usr/sbin/nologin: Assigns the nologin shell, which prevents the user from logging in.
-M: Ensures no home directory is created.
Task 3: Verify the user is created with no login shell by inspecting /etc/passwd
- cat /etc/passwd

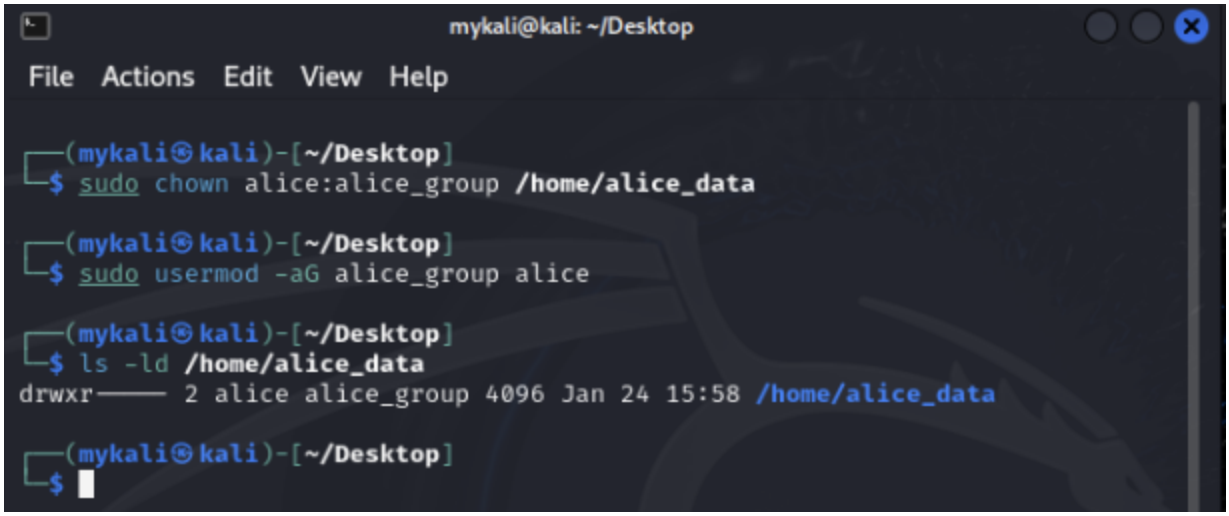


Objective 6: Managing User Permissions

Task 1: Create a new user alice
- sudo useradd -m alice
- sudo passwd alice
Task 2: Create a directory /home/alice_data and set it as rw for the owner, r for the group, and no permissions for others
- sudo mkdir /home/alice_data
- sudo chmod 740 /home/alice_data
- sudo chown alice:alice /home/alice_data
NOTE: chown alice:alice: Makes alice the owner of the directory.
Task 3: Add alice to the group that has access to this directory

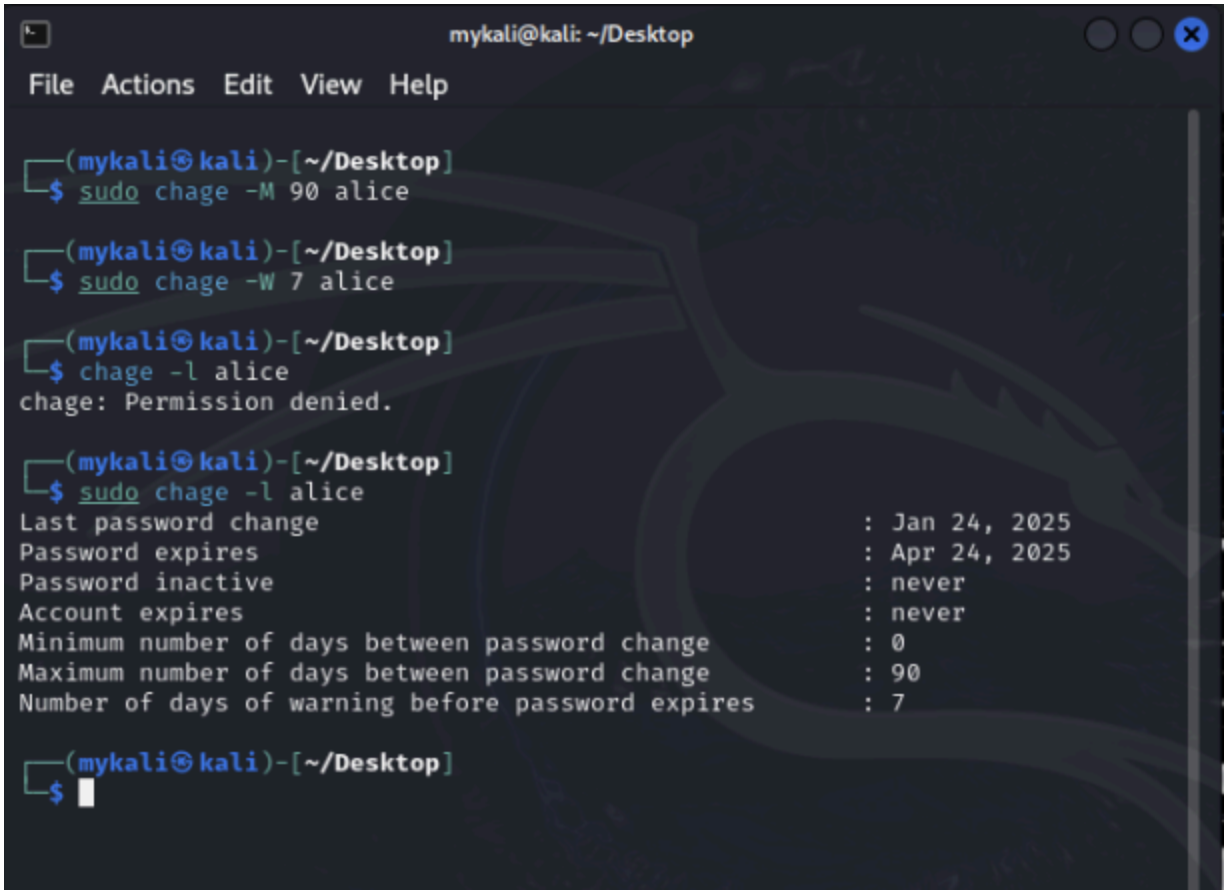
- sudo groupadd alice_group
NOTE: Change Directory Group Ownership
- sudo chown alice:alice_group /home/alice_data
NOTE: Add alice to the group
- sudo usermod -aG alice_group alice
Task 4: Verify the permissions using ls -l
- ls -ld /home/alice_data
NOTE: d: Indicates it's a directory.





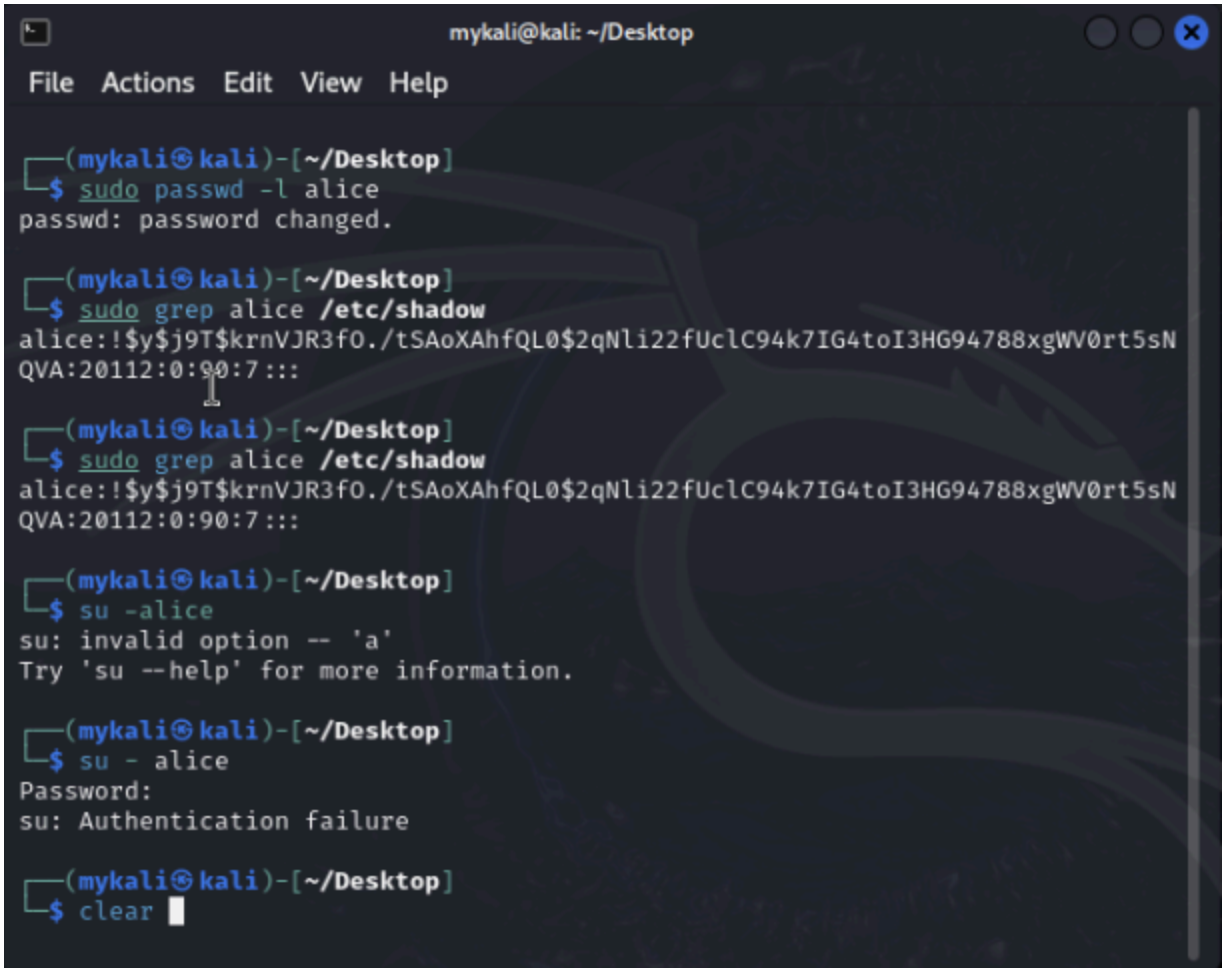
Objective 7: Password Aging and Expiry

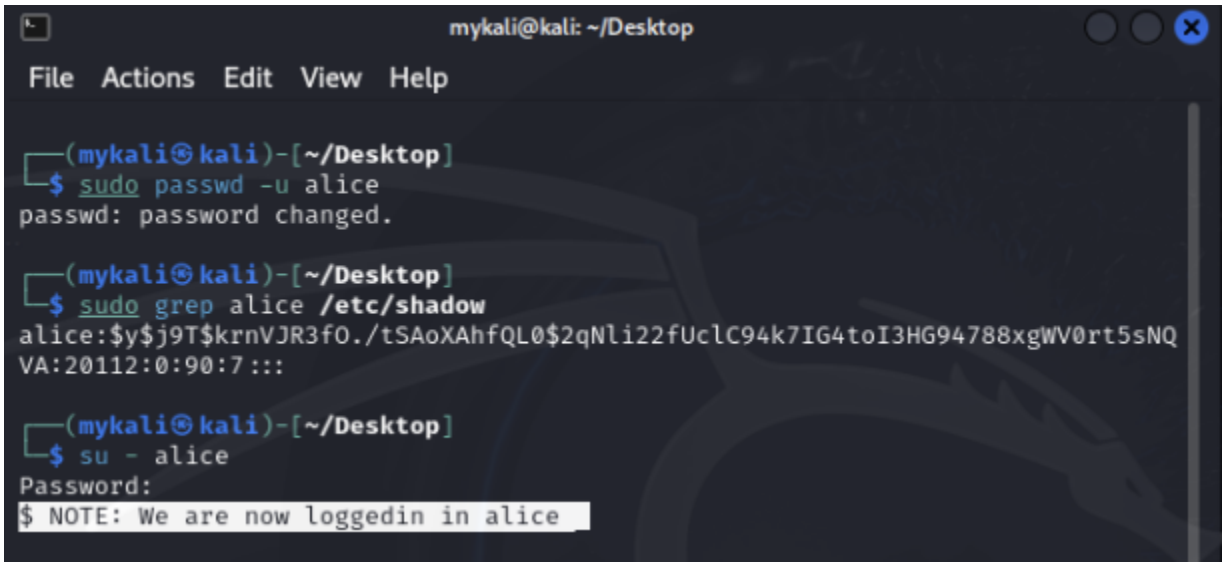
Task 1: Set a password expiration period of 90 days for user alice using chage
- sudo chage -M 90 alice
Task 2: Set a warning period to notify the user 7 days before the password expires
- sudo chage -W 7 alice
Task 3: Verify the changes using chage -l alice
- sudo chage -l alice



Objective 8: Lock and Unlock User Accounts

Task 1: Lock the user account alice by using the passwd -l command
- sudo passwd -l alice
Task 2: Verify that the account is locked by trying to log in as alice
- sudo grep alice /etc/shadow
NOTE: Expected output: alice:!<hashed-password>:<other-fields>
The ! in front of the hashed password indicates the account is locked
Also, Attempt to Log In: Try to switch to the alice account
- su - alice
Task 3: Unlock the account using the passwd -u command
- sudo passwd -u alice
Task 4: Verify the account is unlocked by trying to log in again
- sudo grep alice /etc/shadow
NOTE: The absence of ! indicates the account is unlocked
Also, Attempt to Log In Again:
- su - alice
NOTE: To reset the password: sudo passwd alice

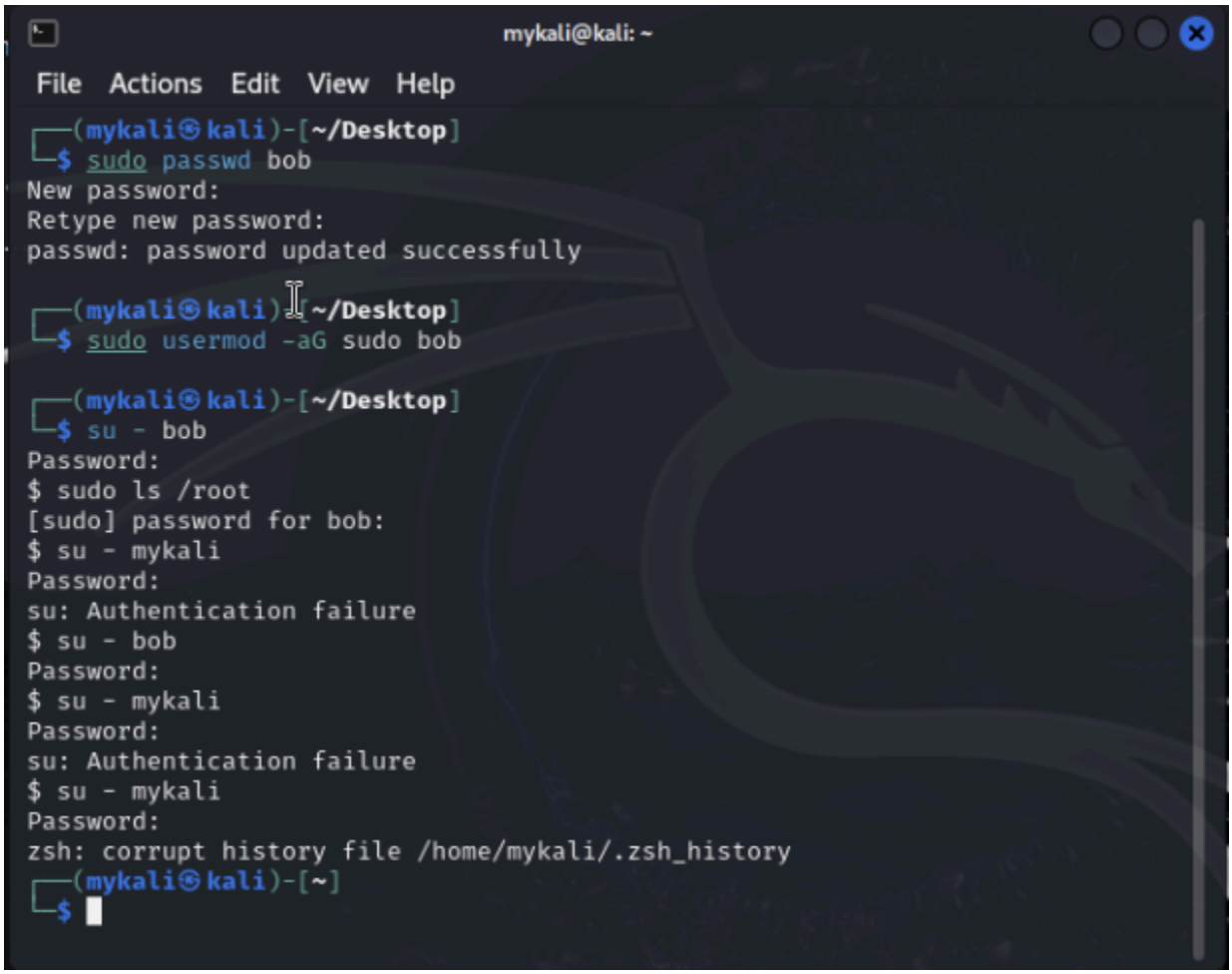




Objective 9: Create and Manage Sudo Access

Task 1: Add a user bob to the sudo group, allowing bob to execute commands as root

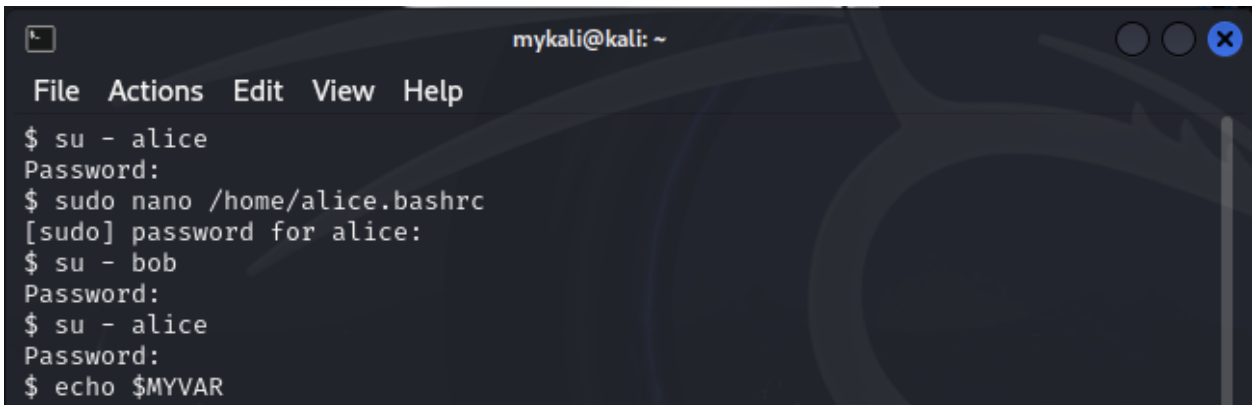
- sudo useradd -m bob
- sudo passwd bob
- sudo usermod -aG sudo bob
NOTE: -aG sudo: Adds the user to the sudo group without removing them from other groups
Task 2: Test by logging in as bob and running a command with sudo
- su - bob
- su - mykali (Trying to log into another account from the user bob we can check if sudo command is working for the bob or not)
Task 3: Optionally, restrict bob's sudo access by editing the /etc/sudoers file using visudo (e.g., allow only apt-get commands)
- sudo visudo



Objective 10: Set Up User Environment Variables

Task 1: Modify the .bashrc file for a user (alice) to set a custom environment variable (e.g., MYVAR=HelloWorld)
- su - alice (Switch accounts to alice)

- sudo nano /home/alice/.bashrc
NOTE: If the user not in the sudoers file
    - su - mykali (Change to user with sudo access)
    - sudo usermod -aG sudo alice
    - aG sudo: Adds the user to the sudo group without removing them from other groups
Type the text:
- export MYVAR="HelloWorld"
NOTE: Press Ctrl+X to exit the editor
    Log out and login back using : su - alice
Task 2: Have the user log out and log back in, then check the environment variable using echo $MYVAR
- echo $MYVAR



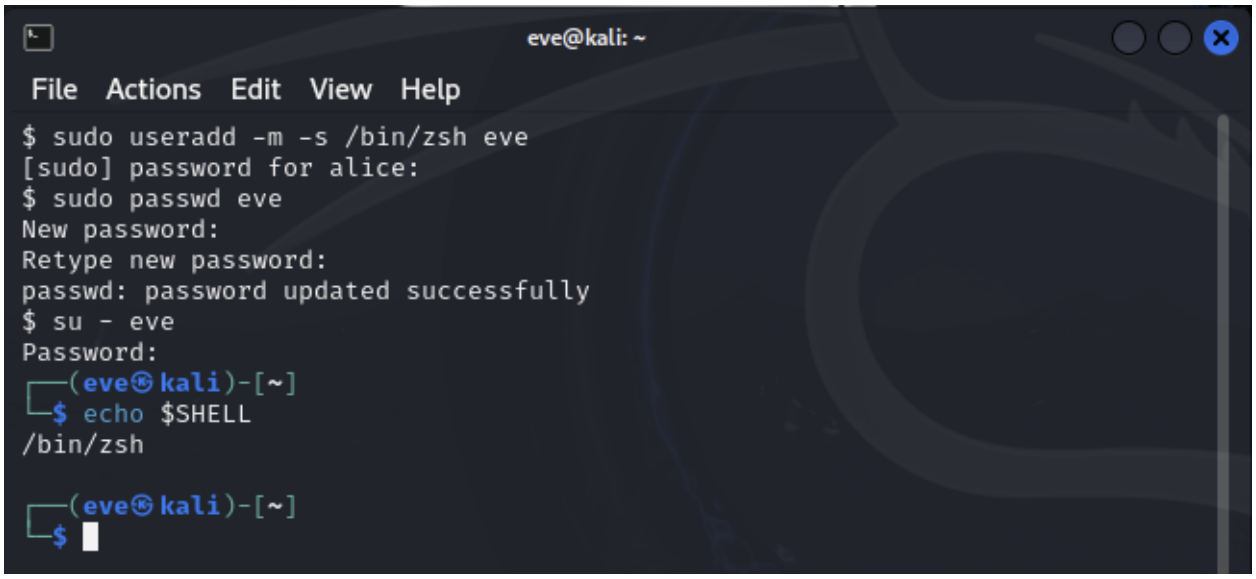
Objective 11: Create and Manage User Quotas

Task 1: Enable disk quotas on a specific file system (/home)
Task 2: Set a soft and hard limit for user alice (e.g., 1 GB for soft, 1.5 GB for hard)
Task 3: Test the quota by attempting to exceed the disk usage limit
Task 4: Verify the user's quota using the quota command

Objective 12: Configure User Shells

Task 1: Create a user eve and set their default shell to /bin/zsh using usermod -s /bin/zsh
- sudo useradd -m -s /bin/zsh eve
- sudo passwd eve
Task 2: Verify that eve's default shell is set to Zsh by checking /etc/passwd
- grep eve /etc/passwd
Task 3: Log in as eve and confirm the shell is now Zsh
- su - eve
- echo $SHELL
NOTE: Expected output: /bin/zsh
    Also, If Zsh is not installed, install it

- sudo apt install zsh



Objective 13: Automate User Creation with a Script

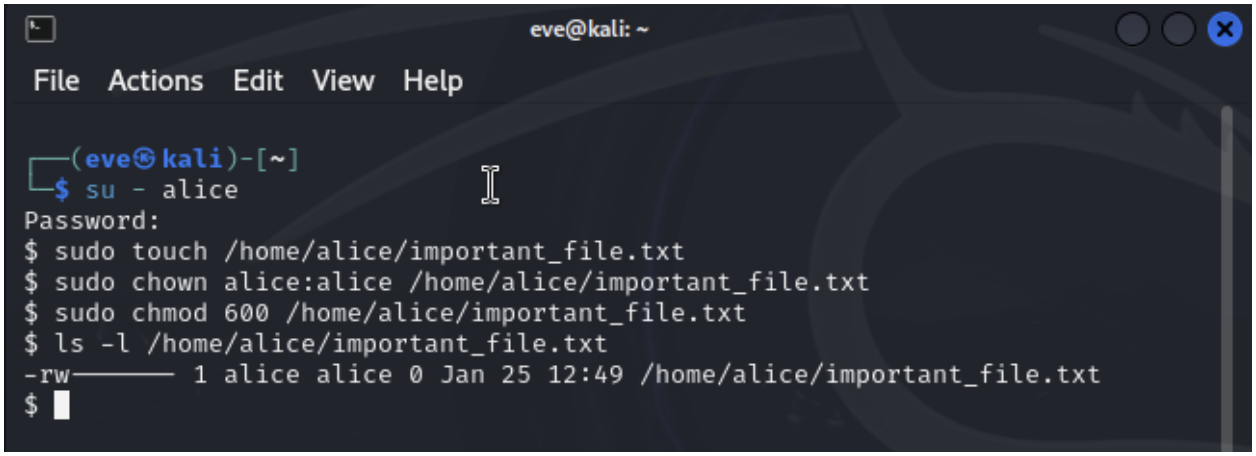
Task 1: Write a Bash script that takes a username and a group as input
Task 2: Create the user, create the group if it does not exist, and add the user to the group
Task 3: Set a default password for the new user and notify the administrator by email

Objective 14: User Account Audit

Task 1: Write a script to list all users who have not logged in for the past 90 days
Task 2: Optionally, send an email alert for these inactive accounts
Task 3: Disable inactive accounts by locking them (passwd -l)

Objective 15: Check and Modify User File Permissions

1. Create a file /home/alice/important_file.txt
- sudo touch /home/alice/important_file.txt
2. Change the ownership of the file to the user alice using chown
- sudo chown alice:alice /home/alice/important_file.txt
3. Set the file permissions so that only alice has read and write access, while others have no access
- sudo chmod 600 /home/alice/important_file.txt
4. Verify the permissions using ls -l
- ls -l /home/alice/important_file.txt


eve@kali: ~
File Actions Edit View Help
┌──(eve㉿kali)-[~]
└─$ su - alice
Password:
$ sudo touch /home/alice/important_file.txt
$ sudo chown alice:alice /home/alice/important_file.txt
$ sudo chmod 600 /home/alice/important_file.txt
$ ls -l /home/alice/important_file.txt
-rw------- 1 alice alice 0 Jan 25 12:49 /home/alice/important_file.txt
$