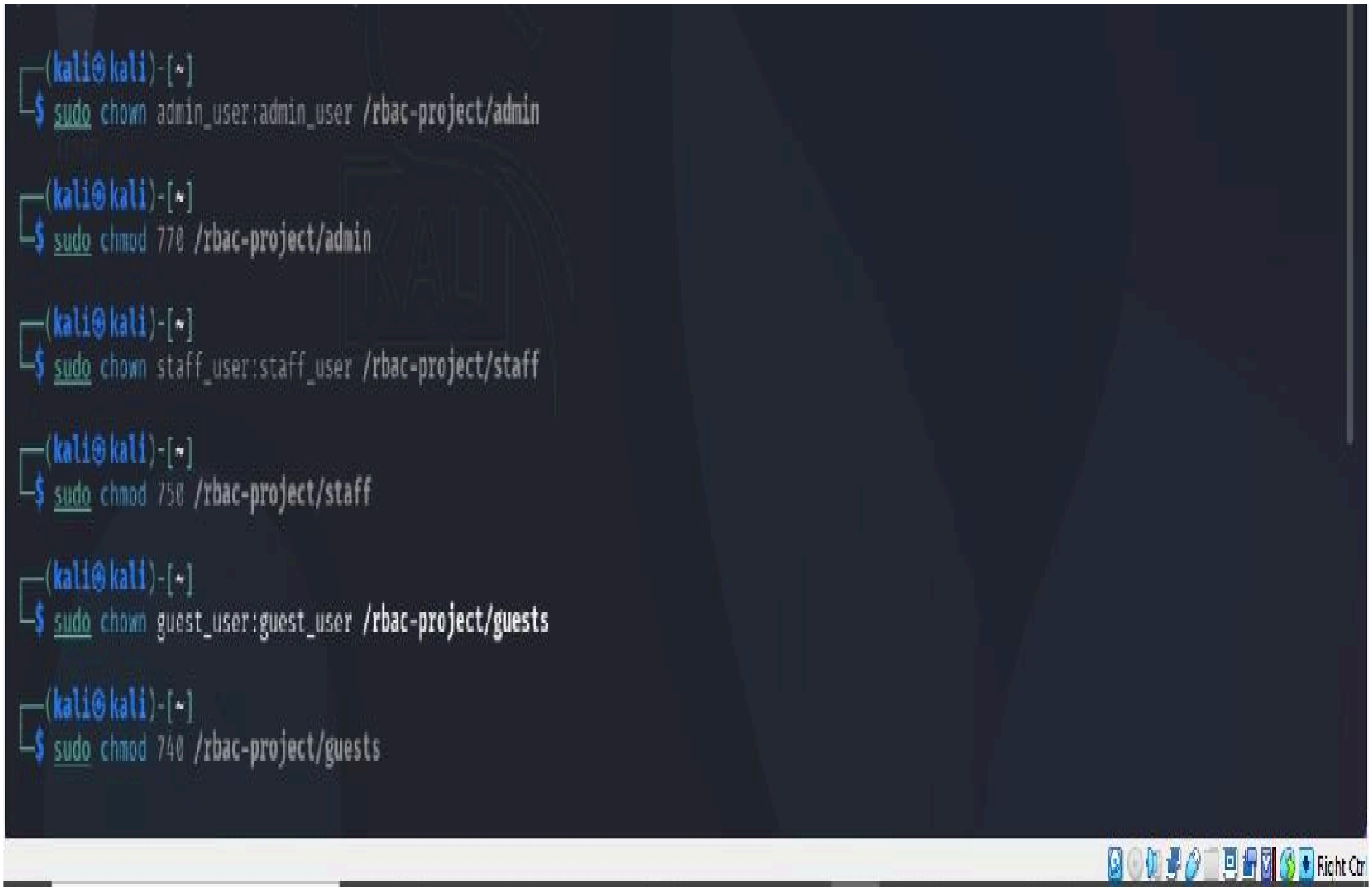
Configure Role-Based Access Control for a File System

Defined Roles and Permissions

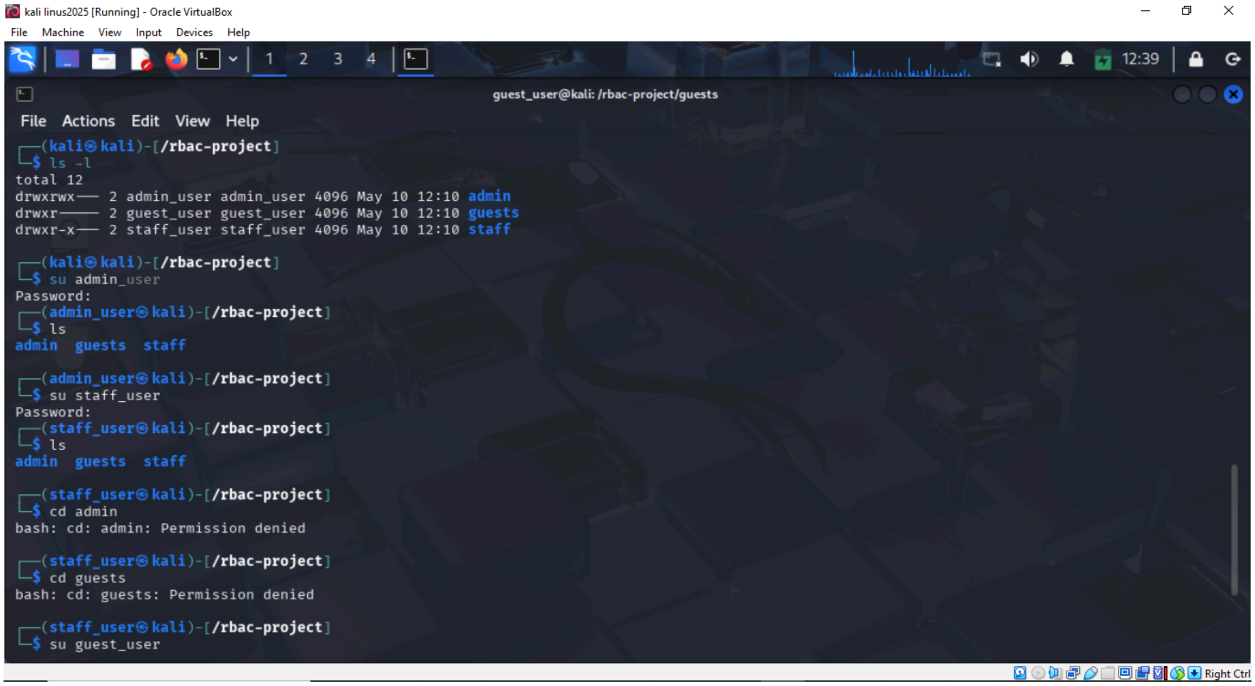
Administrative Role: It has full access to all directories and files. It can also modify, delete and create files.
770

Staff Role: It has read and write access to the’/rbac-project/staff’ directory. It can also read-access to the ‘/rbac-project/admin’ directory.
750

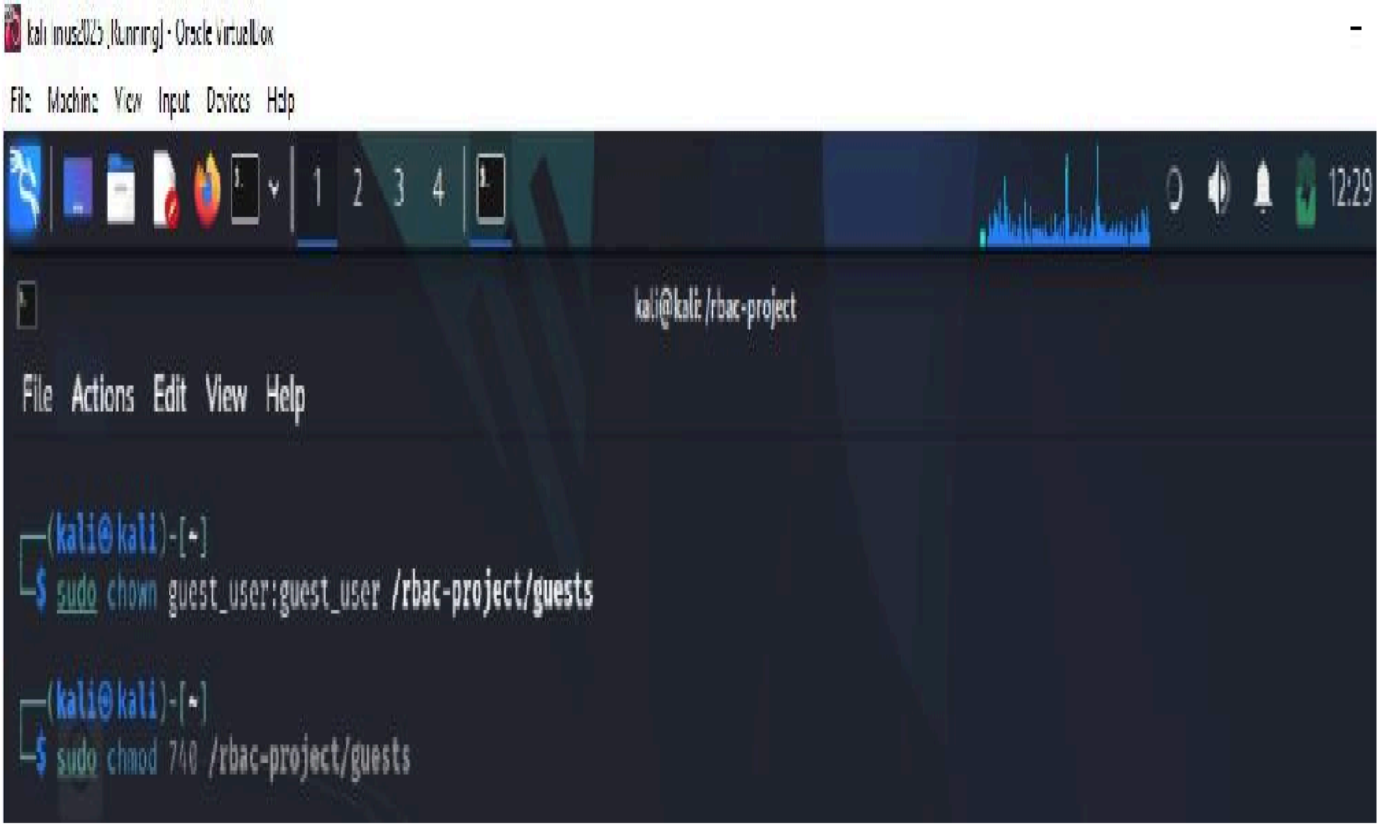
Guest Role: Read-only access to the ‘/rbac-project/guests’ directory.
740



```
┌──(kali㉿kali)-[~]
└─$ sudo chown admin_user:admin_user /rbac-project/admin

┌──(kali㉿kali)-[~]
└─$ sudo chmod 770 /rbac-project/admin

┌──(kali㉿kali)-[~]
└─$ sudo chown staff_user:staff_user /rbac-project/staff

┌──(kali㉿kali)-[~]
└─$ sudo chmod 750 /rbac-project/staff

┌──(kali㉿kali)-[~]
└─$ sudo chown guest_user:guest_user /rbac-project/guests

┌──(kali㉿kali)-[~]
└─$ sudo chmod 740 /rbac-project/guests
```

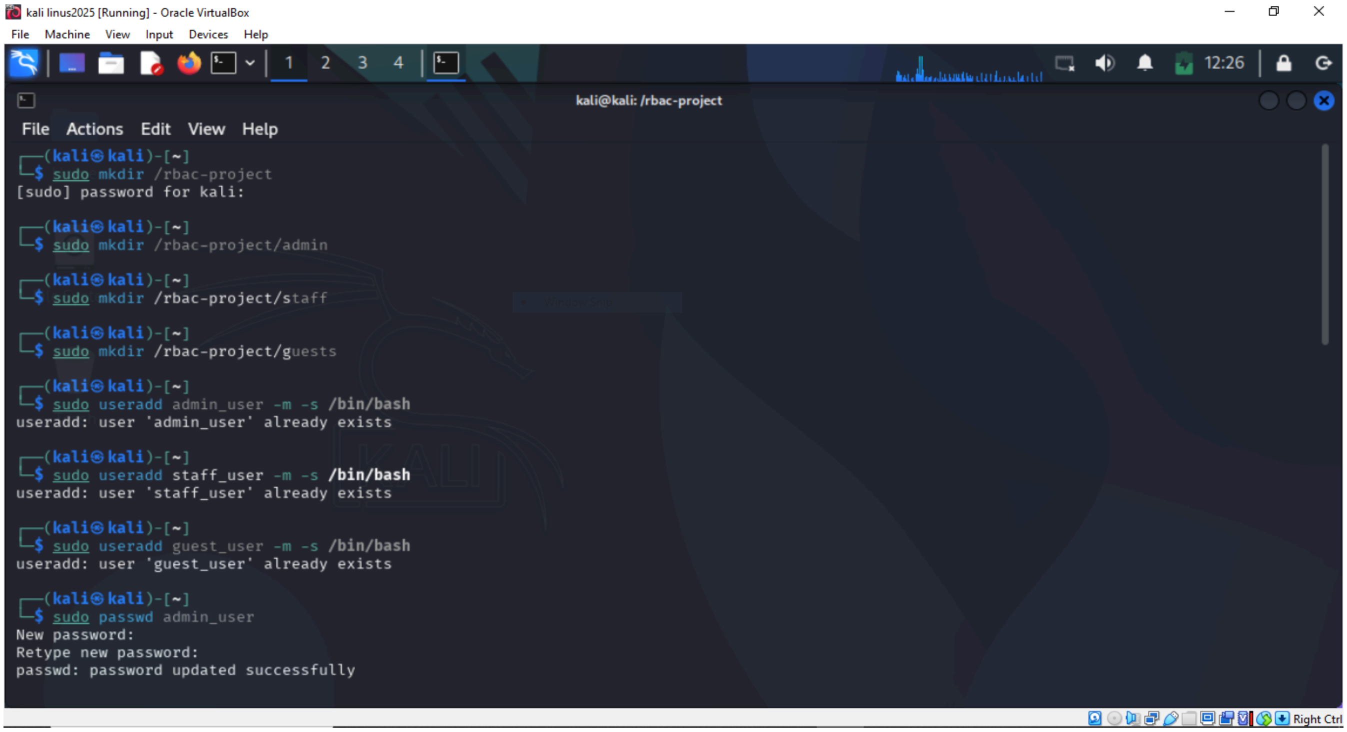

kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:39
guest_user@kali: /rbac-project/guests
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[/rbac-project]
└─$ ls -l
total 12
drwxrwx—— 2 admin_user admin_user 4096 May 10 12:10 admin
drwxr———— 2 guest_user guest_user 4096 May 10 12:10 guests
drwxr-x—— 2 staff_user staff_user 4096 May 10 12:10 staff

┌──(kali㉿kali)-[/rbac-project]
└─$ su admin_user
Password:
┌──(admin_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(admin_user㉿kali)-[/rbac-project]
└─$ su staff_user
Password:
┌──(staff_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd guests
bash: cd: guests: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ su guest_user
```

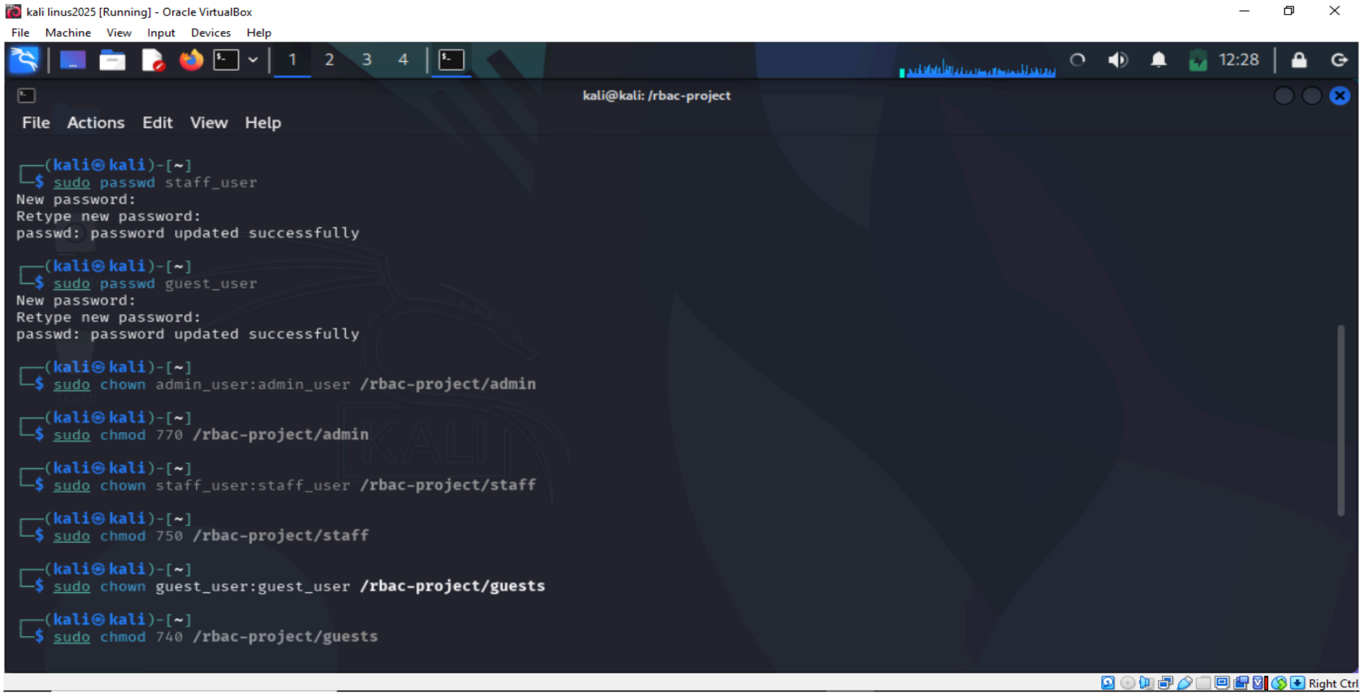

kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:29
kali@kali: /rbac-project
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo chown guest_user:guest_user /rbac-project/guests

┌──(kali㉿kali)-[~]
└─$ sudo chmod 740 /rbac-project/guests
```

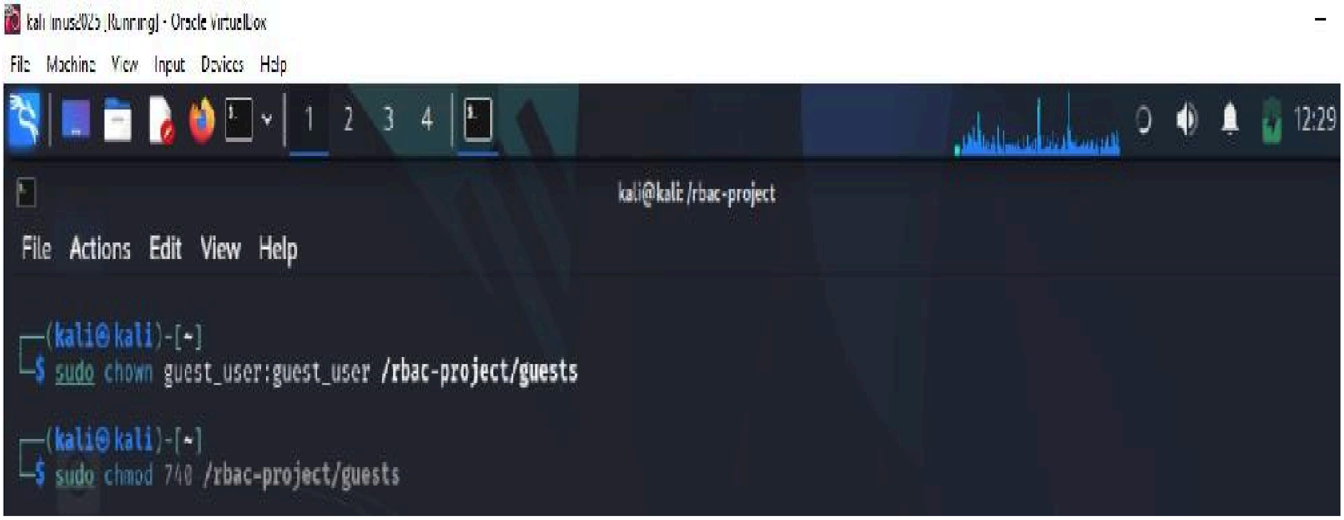
Commands used to configure RBAC


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:26
kali@kali: /rbac-project
File Actions Edit View Help
Right Ctrl

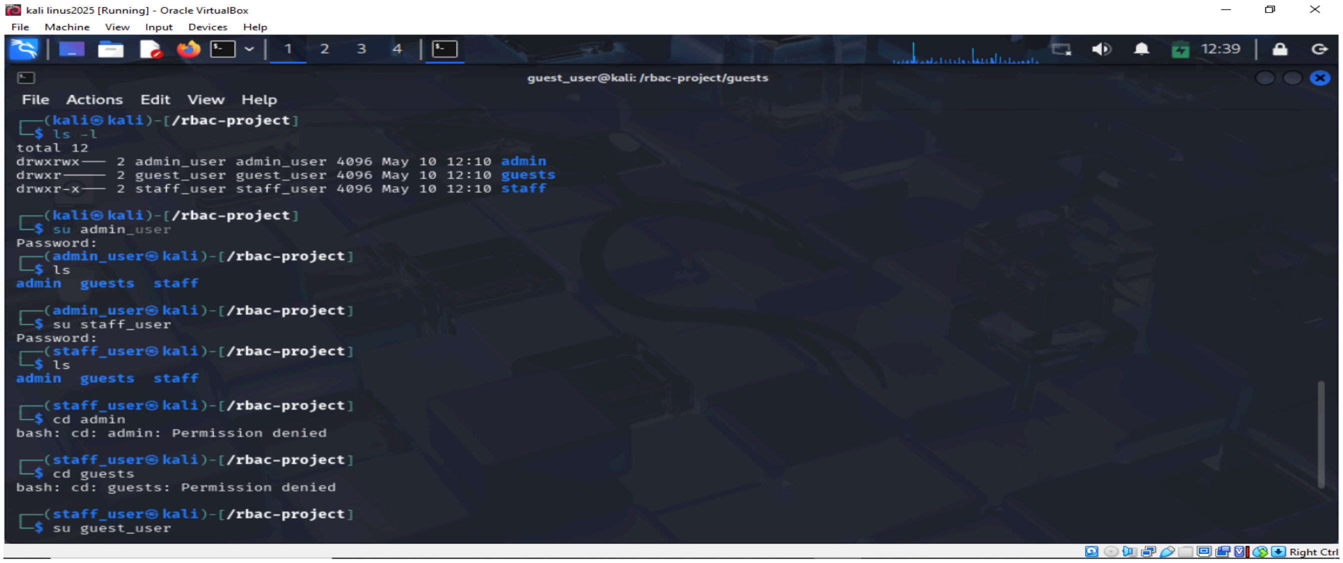
```
┌──(kali㉿kali)-[~]
└─$ sudo mkdir /rbac-project
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo mkdir /rbac-project/admin

┌──(kali㉿kali)-[~]
└─$ sudo mkdir /rbac-project/staff

┌──(kali㉿kali)-[~]
└─$ sudo mkdir /rbac-project/guests

┌──(kali㉿kali)-[~]
└─$ sudo useradd admin_user -m -s /bin/bash
useradd: user 'admin_user' already exists

┌──(kali㉿kali)-[~]
└─$ sudo useradd staff_user -m -s /bin/bash
useradd: user 'staff_user' already exists

┌──(kali㉿kali)-[~]
└─$ sudo useradd guest_user -m -s /bin/bash
useradd: user 'guest_user' already exists

┌──(kali㉿kali)-[~]
└─$ sudo passwd admin_user
New password:
Retype new password:
passwd: password updated successfully
```


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:28
kali@kali: /rbac-project
File Actions Edit View Help
Right Ctrl

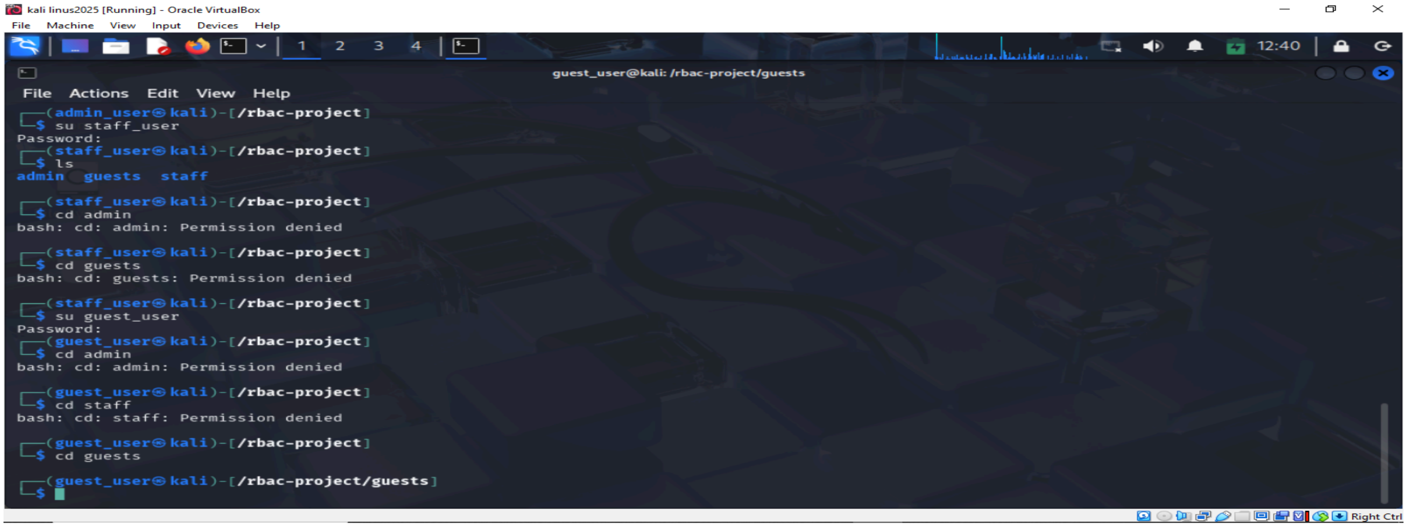
```
┌──(kali㉿kali)-[~]
└─$ sudo passwd staff_user
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo passwd guest_user
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ sudo chown admin_user:admin_user /rbac-project/admin

┌──(kali㉿kali)-[~]
└─$ sudo chmod 770 /rbac-project/admin

┌──(kali㉿kali)-[~]
└─$ sudo chown staff_user:staff_user /rbac-project/staff

┌──(kali㉿kali)-[~]
└─$ sudo chmod 750 /rbac-project/staff

┌──(kali㉿kali)-[~]
└─$ sudo chown guest_user:guest_user /rbac-project/guests

┌──(kali㉿kali)-[~]
└─$ sudo chmod 740 /rbac-project/guests
```


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:29
kali@kali: /rbac-project
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo chown guest_user:guest_user /rbac-project/guests

┌──(kali㉿kali)-[~]
└─$ sudo chmod 740 /rbac-project/guests
```

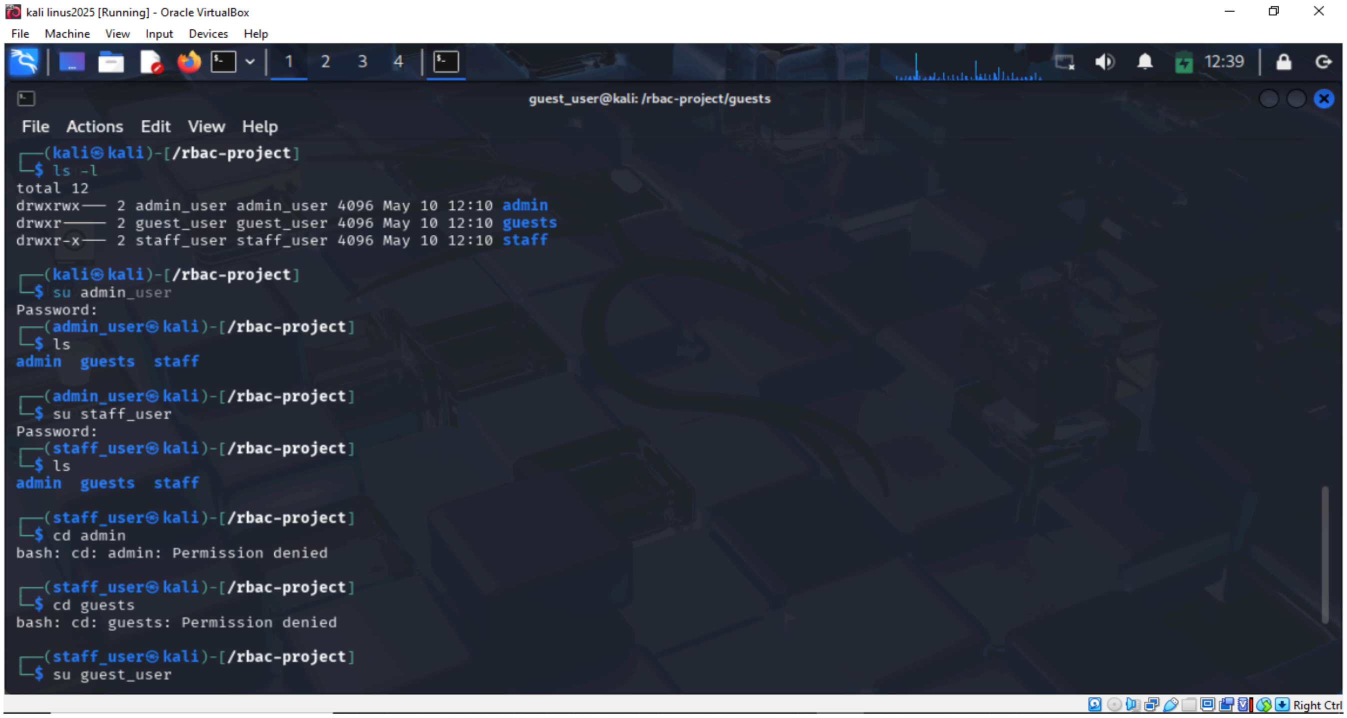

kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:39
guest_user@kali: /rbac-project/guests
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[/rbac-project]
└─$ ls -l
total 12
drwxrwx--- 2 admin_user admin_user 4096 May 10 12:10 admin
drwxr----- 2 guest_user guest_user 4096 May 10 12:10 guests
drwxr-x--- 2 staff_user staff_user 4096 May 10 12:10 staff

┌──(kali㉿kali)-[/rbac-project]
└─$ su admin_user
Password:
┌──(admin_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(admin_user㉿kali)-[/rbac-project]
└─$ su staff_user
Password:
┌──(staff_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd guests
bash: cd: guests: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ su guest_user
```

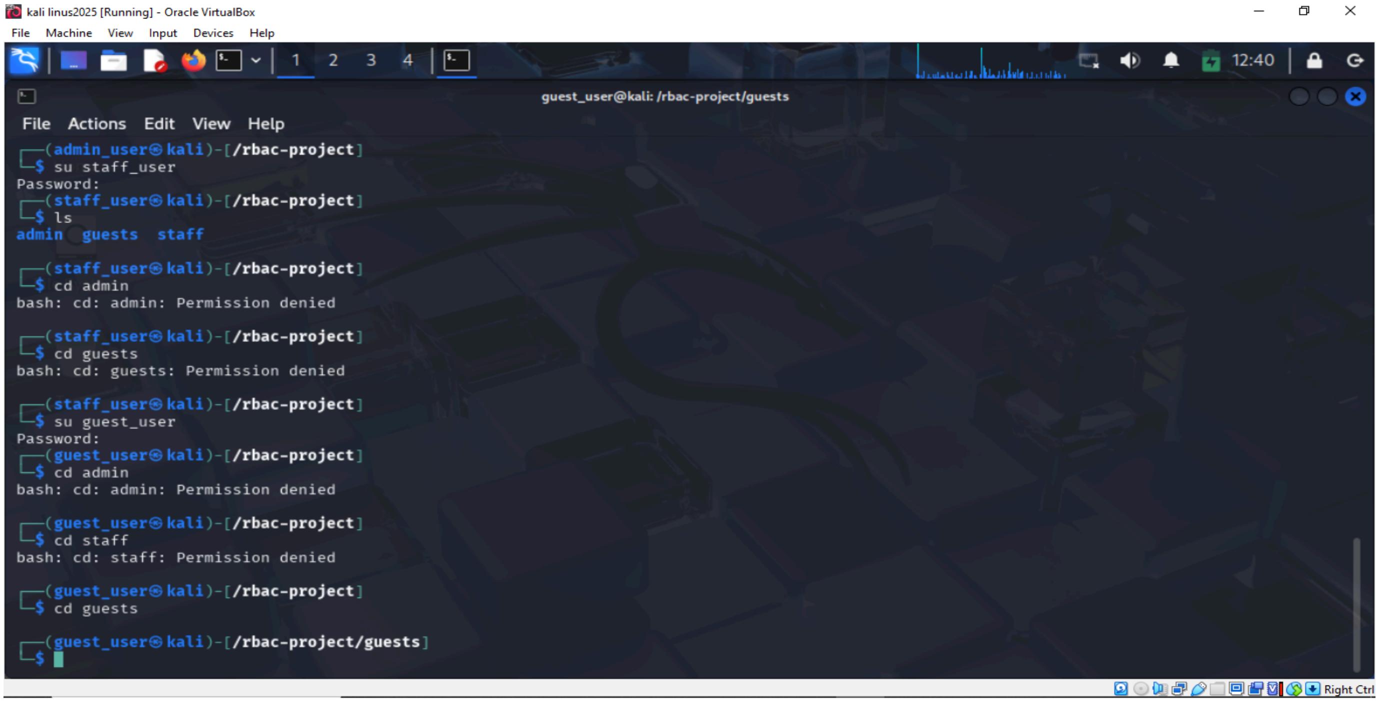

kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:40
guest_user@kali: /rbac-project/guests
File Actions Edit View Help
Right Ctrl

```
┌──(admin_user㉿kali)-[/rbac-project]
└─$ su staff_user
Password:
┌──(staff_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd guests
bash: cd: guests: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ su guest_user
Password:
┌──(guest_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(guest_user㉿kali)-[/rbac-project]
└─$ cd staff
bash: cd: staff: Permission denied

┌──(guest_user㉿kali)-[/rbac-project]
└─$ cd guests

┌──(guest_user㉿kali)-[/rbac-project/guests]
└─$ 
```

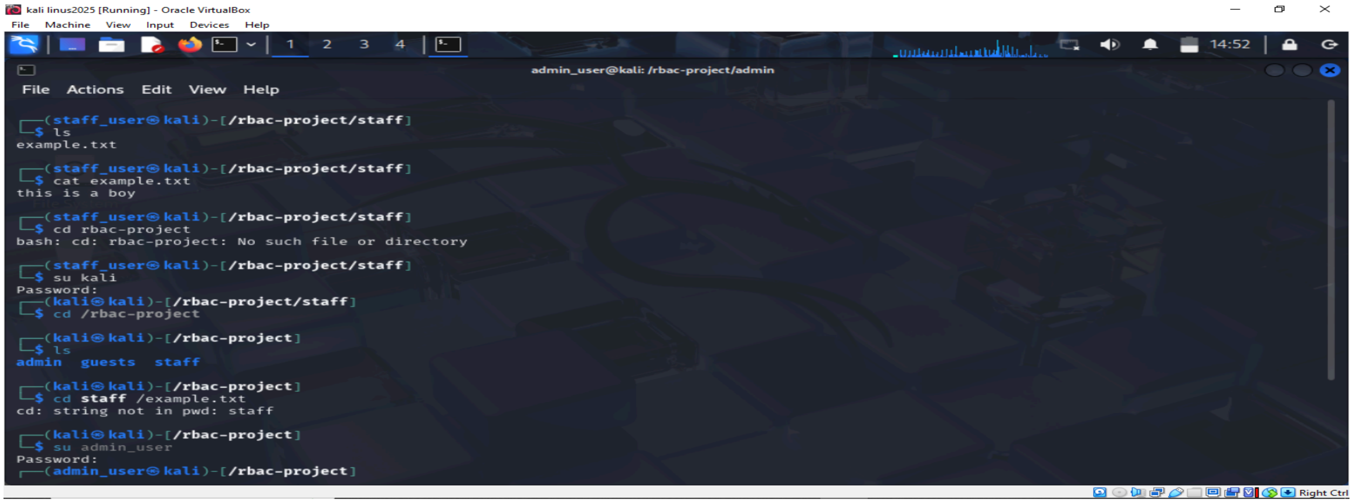
Screenshot of the results of the permission test for each role


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:39
guest_user@kali: /rbac-project/guests
File Actions Edit View Help
Right Ctrl

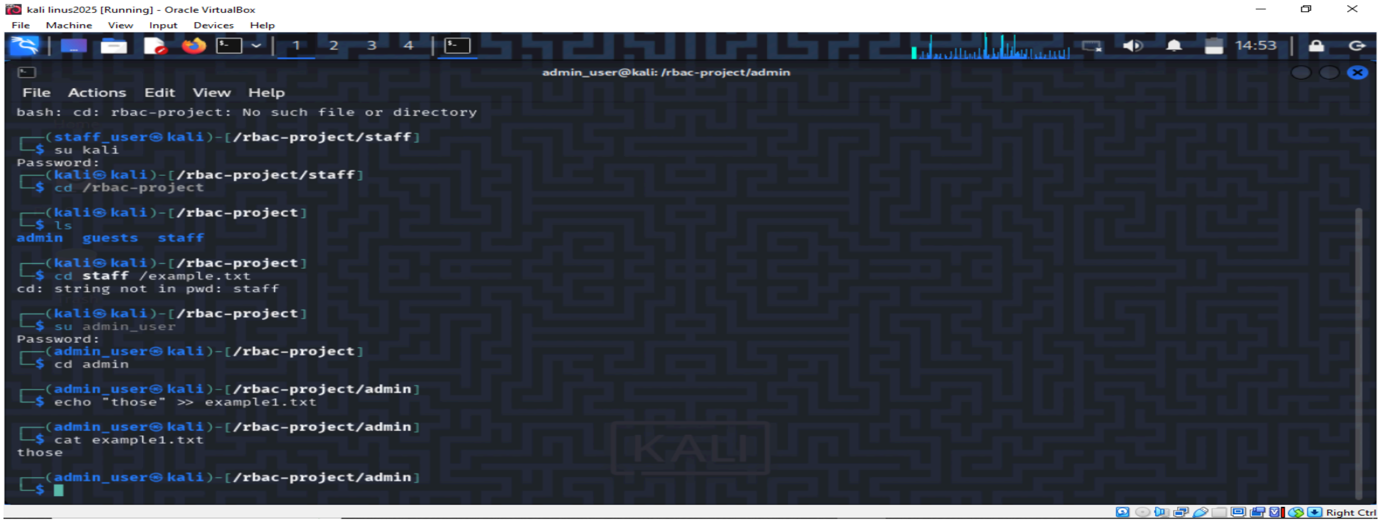
```
┌──(kali㉿kali)-[/rbac-project]
└─$ ls -l
total 12
drwxrwx--- 2 admin_user admin_user 4096 May 10 12:10 admin
drwxr----- 2 guest_user guest_user 4096 May 10 12:10 guests
drwxr-x--- 2 staff_user staff_user 4096 May 10 12:10 staff

┌──(kali㉿kali)-[/rbac-project]
└─$ su admin_user
Password:
┌──(admin_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(admin_user㉿kali)-[/rbac-project]
└─$ su staff_user
Password:
┌──(staff_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd guests
bash: cd: guests: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ su guest_user
```


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
12:40
guest_user@kali: /rbac-project/guests
File Actions Edit View Help
Right Ctrl

```
┌──(admin_user㉿kali)-[/rbac-project]
└─$ su staff_user
Password:
┌──(staff_user㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ cd guests
bash: cd: guests: Permission denied

┌──(staff_user㉿kali)-[/rbac-project]
└─$ su guest_user
Password:
┌──(guest_user㉿kali)-[/rbac-project]
└─$ cd admin
bash: cd: admin: Permission denied

┌──(guest_user㉿kali)-[/rbac-project]
└─$ cd staff
bash: cd: staff: Permission denied

┌──(guest_user㉿kali)-[/rbac-project]
└─$ cd guests

┌──(guest_user㉿kali)-[/rbac-project/guests]
└─$ 
```


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:52
admin_user@kali: /rbac-project/admin
File Actions Edit View Help
Right Ctrl

```
┌──(staff_user㉿kali)-[/rbac-project/staff]
└─$ ls
example.txt

┌──(staff_user㉿kali)-[/rbac-project/staff]
└─$ cat example.txt
this is a boy

┌──(staff_user㉿kali)-[/rbac-project/staff]
└─$ cd rbac-project
bash: cd: rbac-project: No such file or directory

┌──(staff_user㉿kali)-[/rbac-project/staff]
└─$ su kali
Password:
┌──(kali㉿kali)-[/rbac-project/staff]
└─$ cd /rbac-project

┌──(kali㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(kali㉿kali)-[/rbac-project]
└─$ cd staff /example.txt
cd: string not in pwd: staff

┌──(kali㉿kali)-[/rbac-project]
└─$ su admin_user
Password:
┌──(admin_user㉿kali)-[/rbac-project]
```


kali linus2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:53
admin_user@kali: /rbac-project/admin
File Actions Edit View Help
Right Ctrl

```
bash: cd: rbac-project: No such file or directory

┌──(staff_user㉿kali)-[/rbac-project/staff]
└─$ su kali
Password:
┌──(kali㉿kali)-[/rbac-project/staff]
└─$ cd /rbac-project

┌──(kali㉿kali)-[/rbac-project]
└─$ ls
admin  guests  staff

┌──(kali㉿kali)-[/rbac-project]
└─$ cd staff /example.txt
cd: string not in pwd: staff

┌──(kali㉿kali)-[/rbac-project]
└─$ su admin_user
Password:
┌──(admin_user㉿kali)-[/rbac-project]
└─$ cd admin

┌──(admin_user㉿kali)-[/rbac-project/admin]
└─$ echo "those" >> example1.txt

┌──(admin_user㉿kali)-[/rbac-project/admin]
└─$ cat example1.txt
those

┌──(admin_user㉿kali)-[/rbac-project/admin]
└─$ 
```

Observations

Role Design Complexity: Defining roles that accurately reflect user responsibilities can be complex, especially in large organizations. Overlapping or ambiguous roles can lead to access control errors or unintended consequences.
Documentation is Crucial: Thorough documentation of RBAC policies, role assignments, and associated permissions is essential for auditing, troubleshooting, and maintaining the system. Lack of documentation can hinder future maintenance and audits.
Ongoing Maintenance and Adaptation: RBAC systems are not static; they require periodic review and adjustments as user roles, responsibilities, and the organization's security posture evolve.
Integration with Other Security Measures: RBAC is most effective when combined with other security measures like multi-factor authentication (MFA) and strong passwords, which offer additional layers of protection.

User Education and Training: Users need to understand their roles and associated permissions to avoid unintentional violations of RBAC policies. Training and awareness programs can help improve user compliance.
Automated Tools and Processes: Utilizing automated tools and processes for RBAC configuration, monitoring, and auditing can improve efficiency and reduce the risk of manual errors.

Lessons Learned from RBAC Configuration:

Prioritize Least Privilege:
Grant users only the minimum necessary permissions to perform their duties. Over-permissive roles can create vulnerabilities.
Regularly Audit Roles and Permissions: Periodically review role assignments and permissions to ensure they are still aligned with user needs and organizational security policies.
Implement a Role Lifecycle Management Process: Define a process for creating, modifying, and deleting roles to ensure they are managed consistently.
Consider Dynamic Access Controls: Explore dynamic access control mechanisms that adjust permissions based on factors like user location, time of day, or device type.
Focus on Education and Awareness: Educate users about the importance of RBAC and their responsibilities in maintaining the security of the file system.
Embrace a Layered Approach: Combine RBAC with other security measures like MFA, strong passwords, and vulnerability management for a more robust security posture.