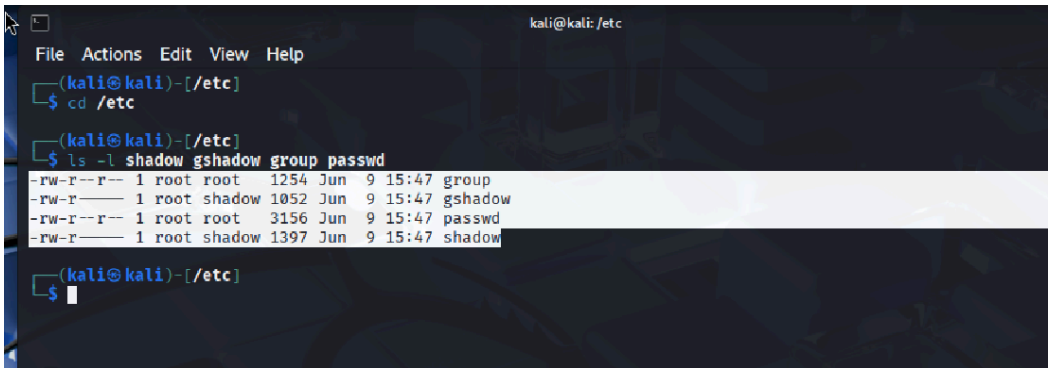
Step 1: Check and Fix Permissions on Sensitive Files

```
cd /etc
ls -l shadow gshadow group passwd
```



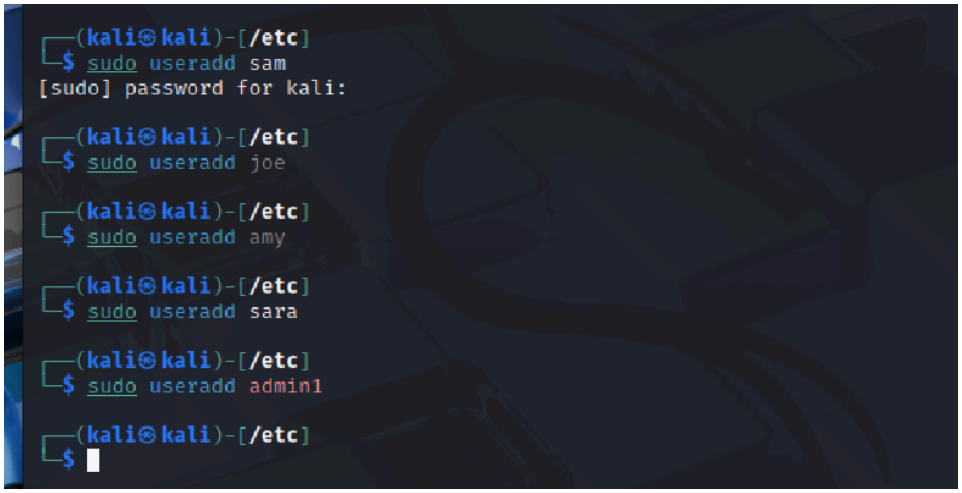
Result:

- `/etc/shadow` **and** `/etc/gshadow`: `-rw-r-----` **(root read/write, group read only or none)**
- `/etc/group` **and** `/etc/passwd`: `-rw-r--r--` **(root read/write, others read only)**

Conclusion:
File permissions are properly configured to secure sensitive user and group data.

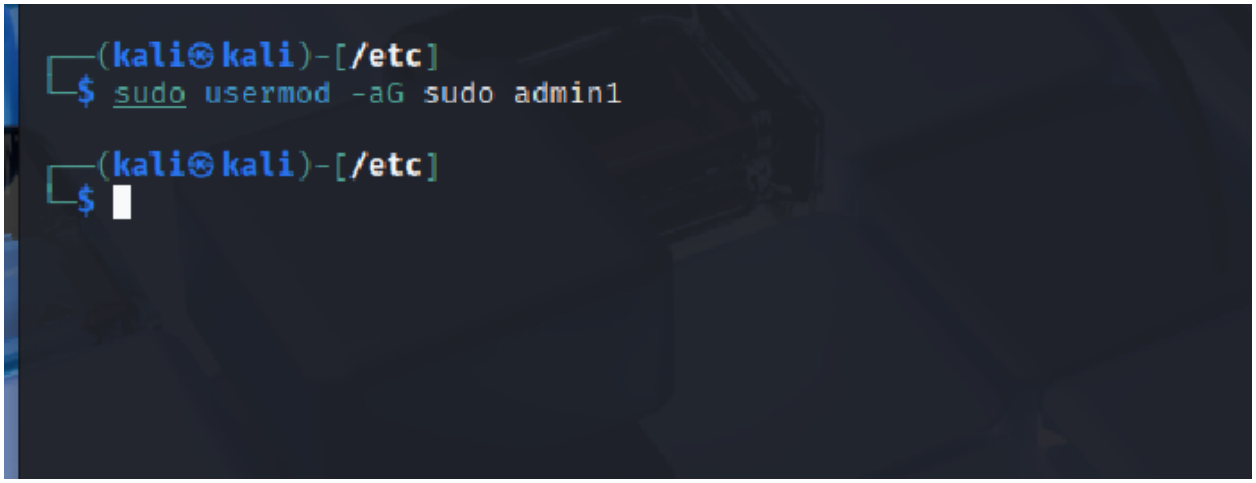
Step 2: Create User Accounts

```
sudo useradd sam
sudo useradd joe
sudo useradd amy
sudo useradd sara
sudo useradd admin1
```



Step 3: Add Sudo Privileges to `admin1`

```
sudo usermod -aG sudo admin1
```



Result:

- `usermod -aG` adds the user to the `sudo` group without removing others.

Step 4: Create a Group and Shared Folder

```
sudo groupadd engineers
sudo usermod -aG engineers sam
sudo usermod -aG engineers joe
sudo usermod -aG engineers amy
sudo usermod -aG engineers sara

sudo mkdir /home/engineers
sudo chown :engineers /home/engineers
sudo chmod 770 /home/engineers
```

```
┌──(kali㉿kali)-[/etc]
└─$ sudo groupadd engineers

┌──(kali㉿kali)-[/etc]
└─$ sudo usermod -aG engineers sam

┌──(kali㉿kali)-[/etc]
└─$ sudo usermod -aG engineers joe

┌──(kali㉿kali)-[/etc]
└─$ sudo usermod -aG engineers amy

┌──(kali㉿kali)-[/etc]
└─$ sudo usermod -aG engineers sara

┌──(kali㉿kali)-[/etc]
└─$ sudo mkdir /home/engineers

┌──(kali㉿kali)-[/etc]
└─$ sudo chown :engineers /home/engineers

┌──(kali㉿kali)-[/etc]
└─$ sudo chmod 770 /home/engineers
```

To confirm users were adding to the ‘engineers’ group:

```
┌──(kali㉿kali)-[/etc]
└─$ groups sam
sam : sam engineers

┌──(kali㉿kali)-[/etc]
└─$ groups joe
joe : joe engineers

┌──(kali㉿kali)-[/etc]
└─$ groups amy
amy : amy engineers

┌──(kali㉿kali)-[/etc]
└─$ groups amy
amy : amy engineers

┌──(kali㉿kali)-[/etc]
└─$ groups sara
sara : sara engineers
```

Conclusion: This sets up a team folder only accessible to the ‘engineer’ group members.

Step 5: Run Lynis Auditclear

`sudo apt update`

```
┌──(kali㉿kali)-[/etc]
└─$ sudo apt update
[sudo] password for kali:
Hit:1 http://mirror.johnnybegood.fr/kali kali-rolling InRelease
1246 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

`sudo apt install lynis`

```
┌──(kali㉿kali)-[/etc]
└─$ sudo apt install -y lynis
Installing:
  lynis

Installing dependencies:
  menu

Suggested packages:
  apt-listbugs  debsecan  debsums  tripwire  samhain  aide  fail2ban  menu-l10n

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1246
  Download size: 605 kB
  Space needed: 3,225 kB / 13.1 GB available

Get:1 http://kali.darklab.sh/kali kali-rolling/main arm64 lynis all 3.1.4-1 [273 kB]
Get:2 http://kali.download/kali kali-rolling/main arm64 menu arm64 2.1.51 [332 kB]
Fetched 605 kB in 1s (486 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 404061 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.1.4-1_all.deb ...
Unpacking lynis (3.1.4-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../archives/menu_2.1.51_arm64.deb ...
Unpacking menu (2.1.51) ...
Setting up lynis (3.1.4-1) ...
Created symlink '/etc/systemd/system/timers.target.wants/lynis.timer' → '/usr/lib/systemd/system/lynis.timer'.
lynis.service is a disabled or a static unit, not starting it.
Setting up menu (2.1.51) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 added doc-base file...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for menu (2.1.51) ...
```

sudo lynis audit system

```
┌──(kali㉿kali)-[/etc]
└─$ sudo lynis audit system | tee lynis-report.txt
tee: lynis-report.txt: Permission denied

[ Lynis 3.1.4 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2024, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]
```

Result:

```
Lynis security scan details:

Hardening index : 62 [############        ]
Tests performed : 272
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```

Conclusion:

- `lynis` scans your system and gives **hardening recommendations**.