

NAME: PURITY CHEPKEMOI

E-MAIL: pyuah16@gmail.com

**DEV-SEC-OPS PROGRAM ASSIGNMENT 1 – LINUX USER & ACCESS CONTROL:
SCENARIO-BASED DEVSECOPS PRACTICAL ASSESSMENT**

TABLE OF CONTENTS

NAME: PURITY CHEPKEMOI	1
E-MAIL: pyuah16@gmail.com.....	1
DEV-SEC-OPS PROGRAM ASSIGNMENT 1 – LINUX USER & ACCESS CONTROL: SCENARIO-BASED DEVSECOPS PRACTICAL ASSESSMENT	1
INTRODUCTION	2
SUMMARY OF THE TASKS	2
 Scenario 1: Password State Investigation & Remediation.....	2
Part A: Create a User With No Password	3
Part B: Identify Users Without Passwords (Discovery Required)	6
Part C: Remediation – Setting a Password	9
Demonstrate, using the terminal, whether a normal (non-privileged) user can access the system location where password data is stored, and arrive at a conclusion based on your observation..	12
 Scenario 2: DevSecOps User & Department Access Configuration	14
1. Create all onboarded users using a mix of user management commands.	15
2. Assign users to departments as follows:.....	18
3. Ensure one user is created without a password, then later set the password and	20
confirm the change.	20
4. Configure the ci_runner account with a non-login shell.....	22
5. Grant sudo access to one user from ops_team only; all other users must remain	24
within their department privileges.....	24
6. Remove one user account while preserving the home directory for audit and security	25
reasons.....	25
7. Verify and demonstrate that:	26
CONCLUSION	29

INTRODUCTION

These exercises focused on investigating Linux authentication mechanisms and implementing secure user and access management in a DevSecOps environment. The tasks required identifying how the system stores password data, configuring department-based access control, enforcing least privilege, and validating all changes through direct system evidence.

I used Kali Linux deployed within an Oracle VirtualBox virtual machine to perform the practical tasks in this assignment.

SUMMARY OF THE TASKS

Scenario 1: Password State Investigation & Remediation

Context

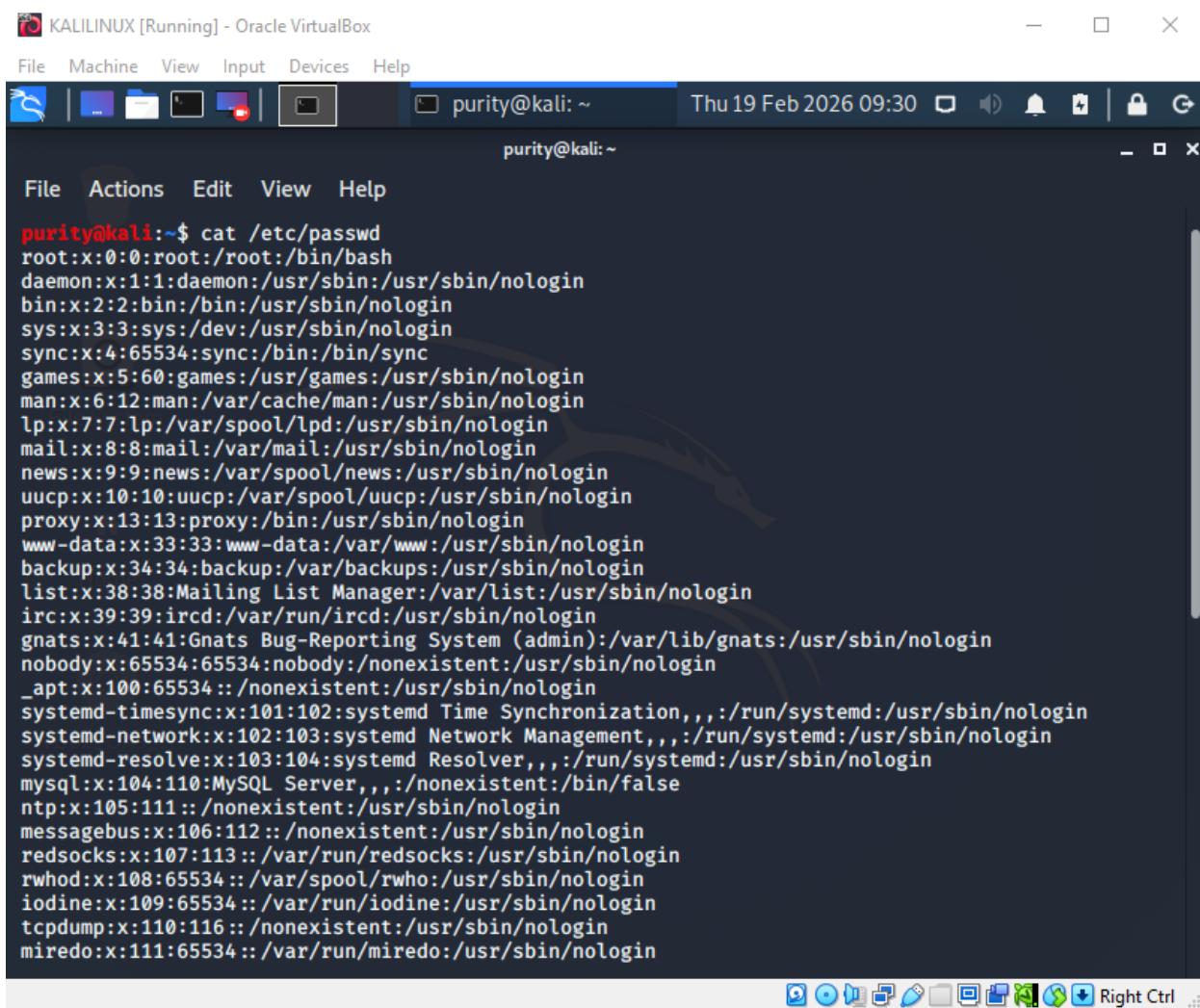
During a routine security audit, the Security Director asks you:

“Show me how you identify users on this system who do not have passwords set, and then demonstrate how you would remediate one.”

You are not told where Linux stores password state. You are expected to discover it, inspect it, and explain your reasoning.

Part A: Create a User with No Password

To list all users, I ran the following command; `cat /etc/passwd`



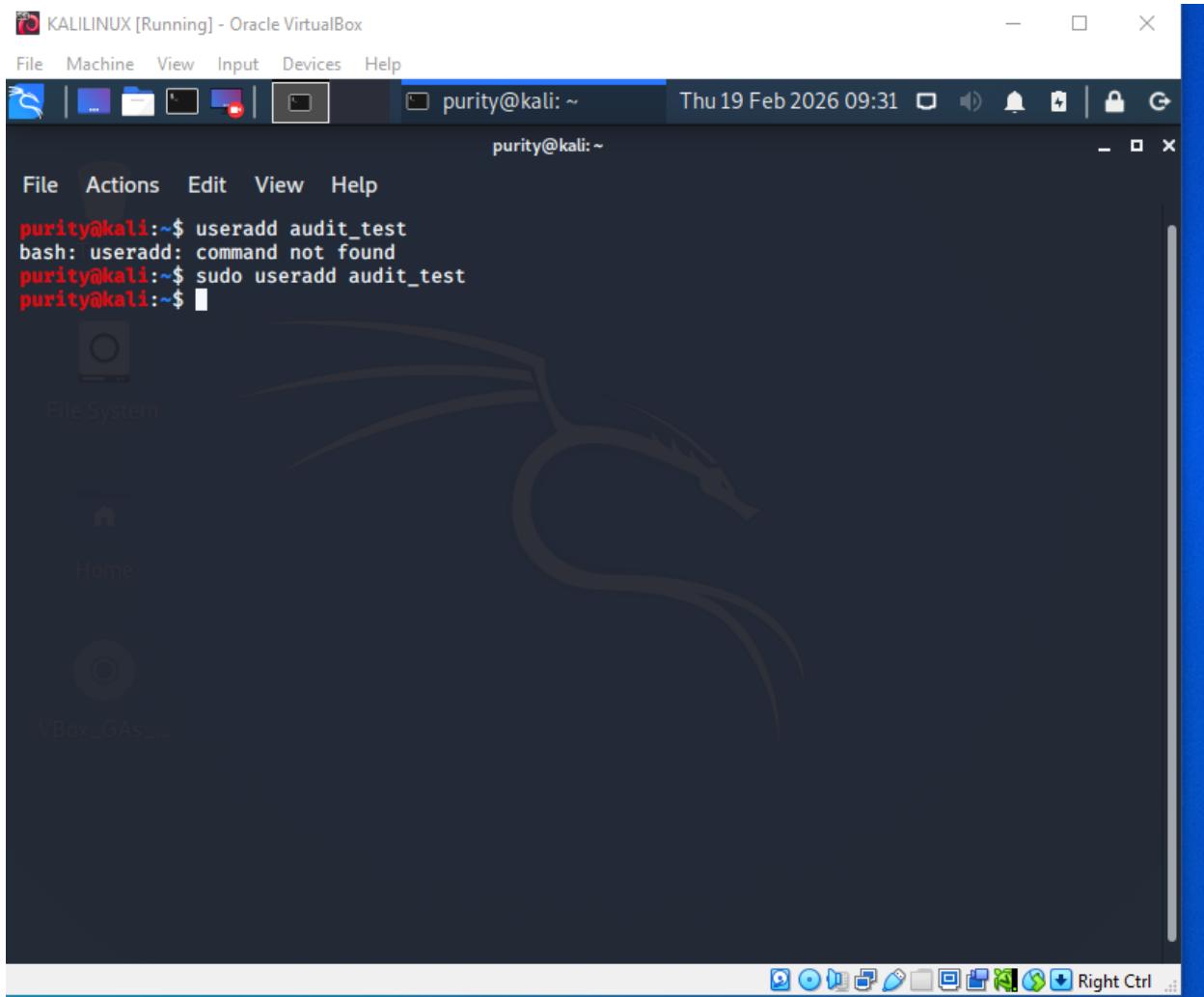
The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The window title bar includes icons for file operations and a lock. The terminal prompt is "purity@kali: ~". The date and time "Thu 19 Feb 2026 09:30" are displayed at the top right. The menu bar contains "File", "Actions", "Edit", "View", and "Help". Below the menu is a scrollable list of user entries from the "/etc/passwd" file. The list includes standard system accounts like root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, _apt, systemd-timesync, systemd-network, systemd-resolve, mysql, ntp, messagebus, redsocks, rwhod, iodine, tcpdump, and miredo. Each entry consists of a colon-separated list of fields: username, password (represented by an x), uid, gid, and home directory and shell.

```
purity@kali:~$ cat /etc/passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
ntp:x:105:111::/nonexistent:/usr/sbin/nologin
messagebus:x:106:112::/nonexistent:/usr/sbin/nologin
redsocks:x:107:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534::/var/run/iodine:/usr/sbin/nologin
tcpdump:x:110:116::/nonexistent:/usr/sbin/nologin
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin
```

1. Create a new user called **audit_test**
2. Ensure the user is created without setting a password

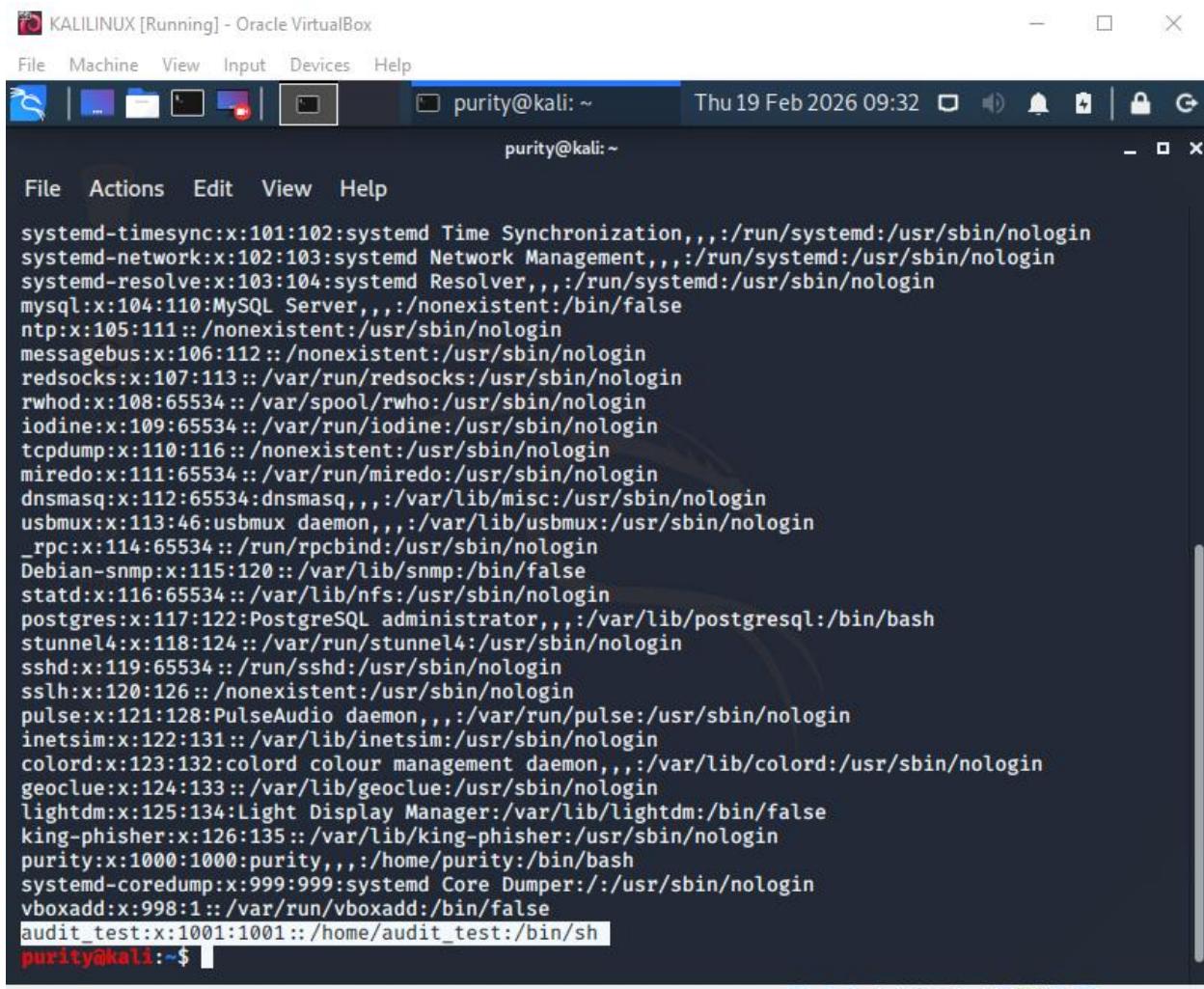
*I created a new user named **audit_test** using the `useradd` command. `useradd` creates a user with **no password by default**.*

The account was successfully created, and no prompt was given to set a password



3. Confirm that the user exists on the system

*To confirm the user exists I ran the **cat /etc/passwd** command*



```
systemd-timesync:x:101:102::systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103::systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104::systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110::MySQL Server,,,:/nonexistent:/bin/false
ntp:x:105:111::/nonexistent:/usr/sbin/nologin
messagebus:x:106:112::/nonexistent:/usr/sbin/nologin
redsocks:x:107:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534::/var/run/iodine:/usr/sbin/nologin
tcpdump:x:110:116::/nonexistent:/usr/sbin/nologin
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin
dnsmasq:x:112:65534::dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:113:46::usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
_rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:115:120::/var/lib/snmp:/bin/false
statd:x:116:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:117:122::PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
stunnel4:x:118:124::/var/run/stunnel4:/usr/sbin/nologin
sshd:x:119:65534::/run/sshd:/usr/sbin/nologin
sslh:x:120:126::/nonexistent:/usr/sbin/nologin
pulse:x:121:128::PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
inetsim:x:122:131::/var/lib/inetsim:/usr/sbin/nologin
colord:x:123:132::colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:133::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:125:134::Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:126:135::/var/lib/king-phisher:/usr/sbin/nologin
purity:x:1000:1000:purity,,,:/home/purity:/bin/bash
systemd-coredump:x:999:999::systemd Core Dumper,,,:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
audit_test:x:1001:1001::/home/audit_test:/bin/sh
purity@kali:~$
```

Security / System Implications

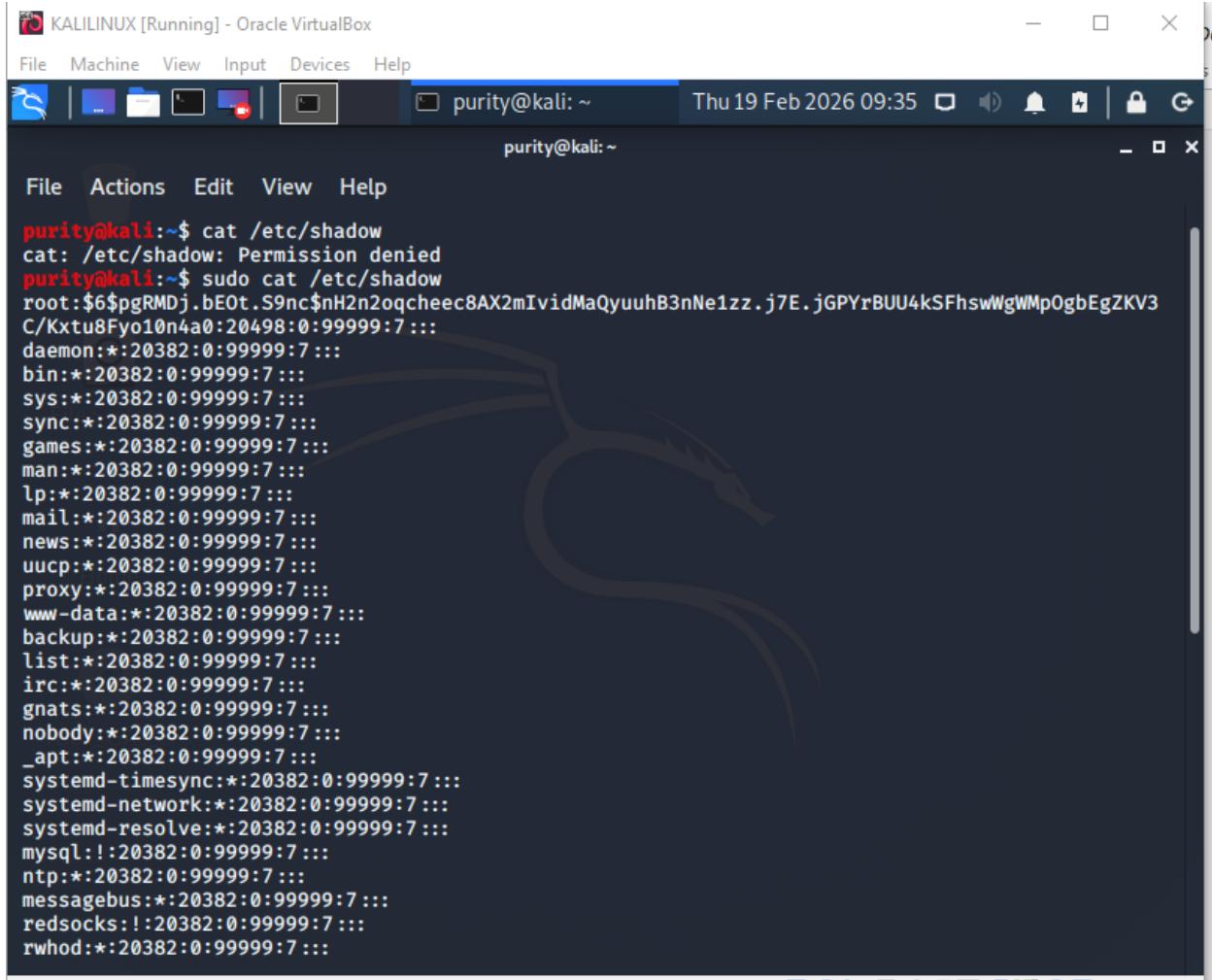
An account without a password may not allow password-based login, but it still represents a potential security risk depending on authentication configuration (e.g., SSH key access, misconfigured PAM rules). Accounts without proper password controls should always be reviewed.

Part B: Identify Users Without Passwords (Discovery Required)

1. Inspect the system location that stores password state

I inspected the /etc/shadow file:

sudo cat /etc/shadow

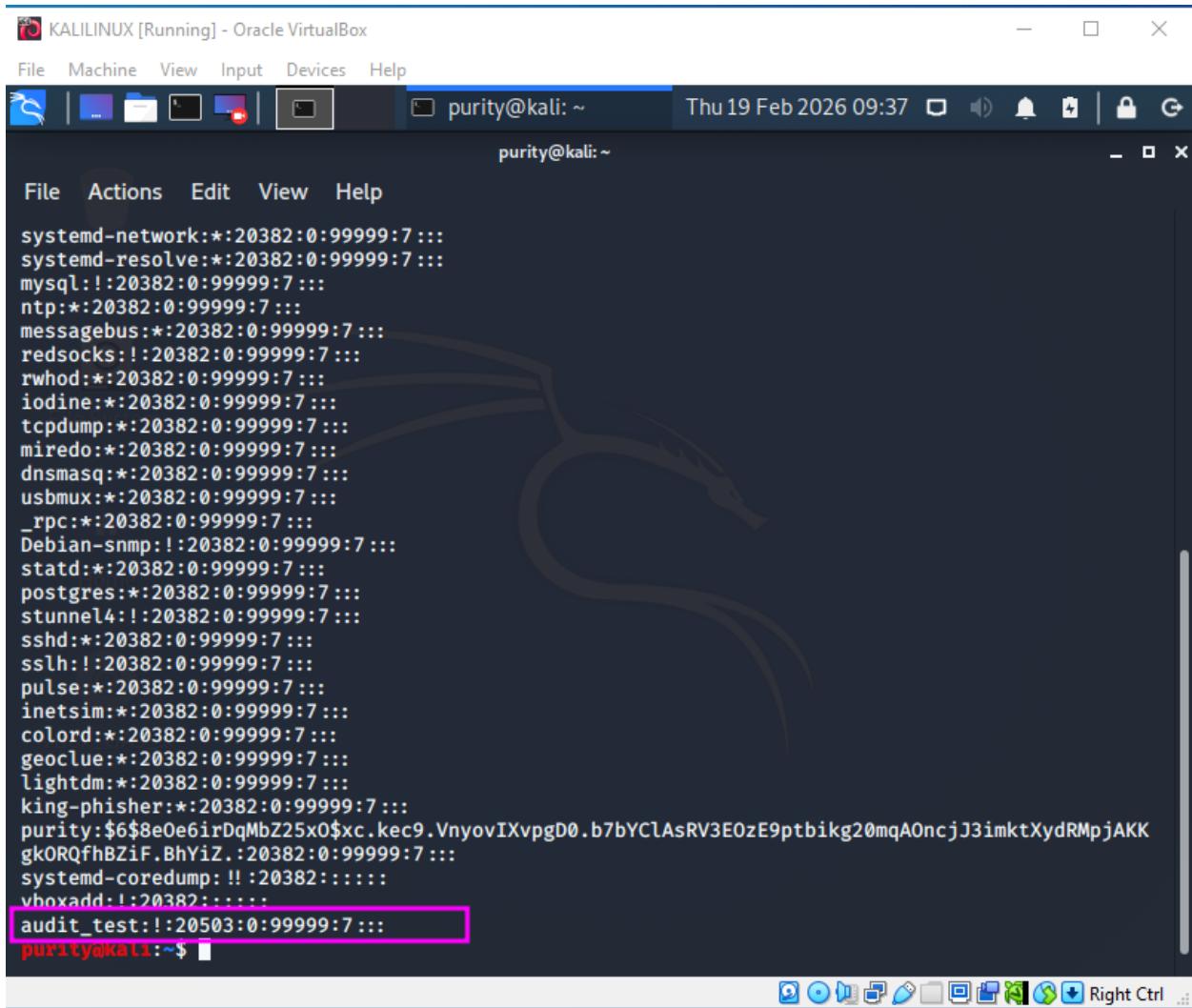


```
purity@kali:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
purity@kali:~$ sudo cat /etc/shadow
root:$6$pgRMDj.bE0t.S9nc$nH2n2oqcheec8AX2mIvidMaQyuhB3nNe1zz.j7E.jGPYrBUU4kSFhswWgWMp0gbEgZKV3
C/Kxtu8Fyo10n4a0:20498:0:99999:7:::
daemon:*:20382:0:99999:7:::
bin:*:20382:0:99999:7:::
sys:*:20382:0:99999:7:::
sync:*:20382:0:99999:7:::
games:*:20382:0:99999:7:::
man:*:20382:0:99999:7:::
lp:*:20382:0:99999:7:::
mail:*:20382:0:99999:7:::
news:**:20382:0:99999:7:::
uucp:**:20382:0:99999:7:::
proxy:**:20382:0:99999:7:::
www-data:**:20382:0:99999:7:::
backup:**:20382:0:99999:7:::
list:**:20382:0:99999:7:::
irc:**:20382:0:99999:7:::
gnats:**:20382:0:99999:7:::
nobody:**:20382:0:99999:7:::
_apt:**:20382:0:99999:7:::
systemd-timesync:**:20382:0:99999:7:::
systemd-network:**:20382:0:99999:7:::
systemd-resolve:**:20382:0:99999:7:::
mysql!:**:20382:0:99999:7:::
ntp:**:20382:0:99999:7:::
messagebus:**:20382:0:99999:7:::
redsocks!:**:20382:0:99999:7:::
rwhod:**:20382:0:99999:7:::
```

2. Identify which users do not have an active password
3. Clearly indicate how you know the password is missing or inactive Discovery Process

I examined /etc/shadow, which stores encrypted password hashes and password state information.

The second field in /etc/shadow represents the password hash.



```

KALILINUX [Running] - Oracle VirtualBox
File Machine View Input Devices Help
purity@kali: ~ Thu 19 Feb 2026 09:37
purity@kali: ~

File Actions Edit View Help

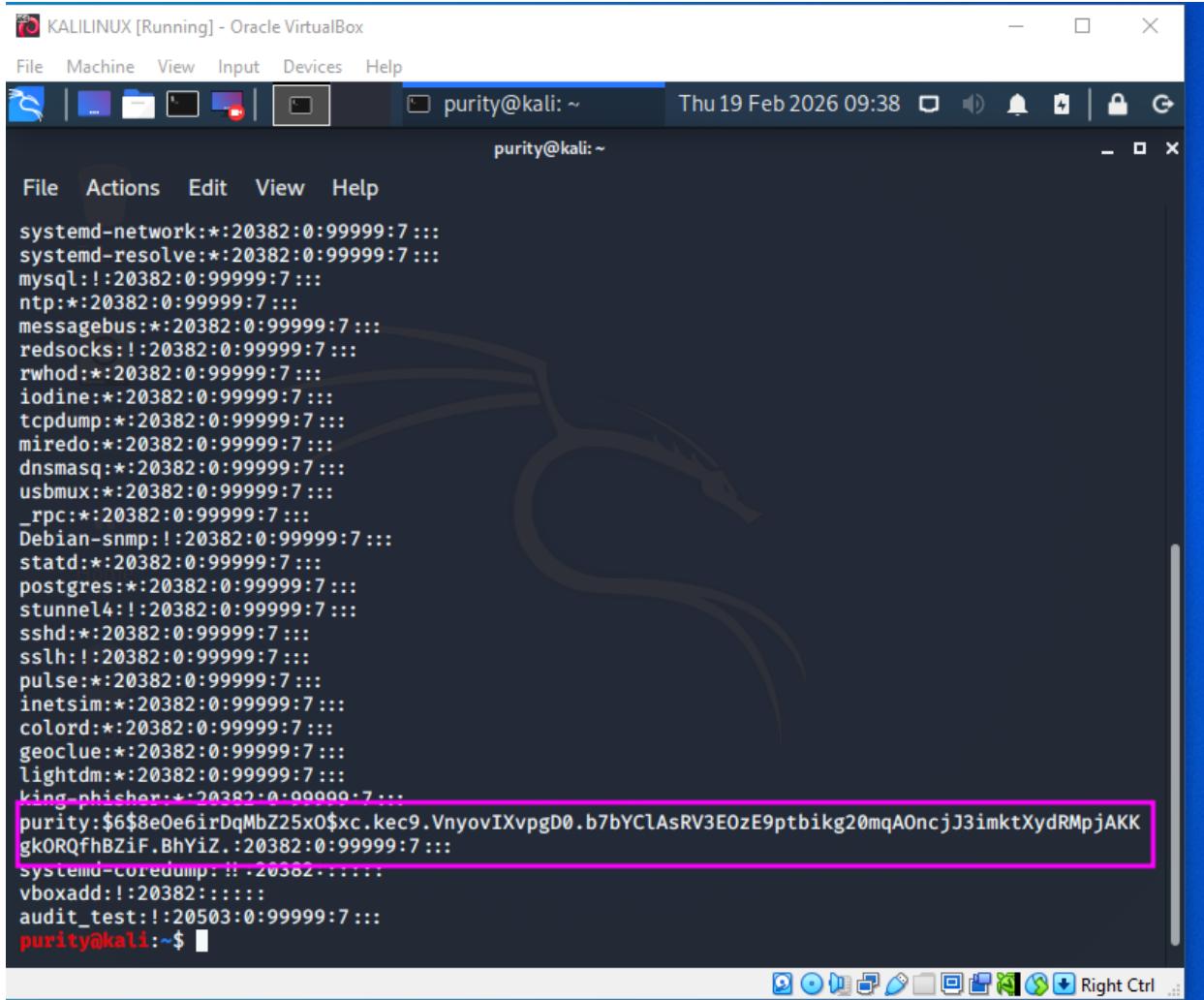
systemd-network:*:20382:0:99999:7:::
systemd-resolve:*:20382:0:99999:7:::
mysql:!:20382:0:99999:7:::
ntp:*:20382:0:99999:7:::
messagebus:*:20382:0:99999:7:::
redsocks!:20382:0:99999:7:::
rwhod:*:20382:0:99999:7:::
iodine:*:20382:0:99999:7:::
tcpdump:*:20382:0:99999:7:::
miredo:*:20382:0:99999:7:::
dnsmasq:*:20382:0:99999:7:::
usbmux:*:20382:0:99999:7:::
_rpc:*:20382:0:99999:7:::
Debian-snmp!:20382:0:99999:7:::
statd:*:20382:0:99999:7:::
postgres:*:20382:0:99999:7:::
stunnel4!:20382:0:99999:7:::
sshd:*:20382:0:99999:7:::
sslh!:20382:0:99999:7:::
pulse:*:20382:0:99999:7:::
inetSim:*:20382:0:99999:7:::
colord:*:20382:0:99999:7:::
geoclue:*:20382:0:99999:7:::
lightdm:*:20382:0:99999:7:::
king-phisher:*:20382:0:99999:7:::
purity:$6$8e6irDqMbZ25x0$xc.kec9.VnyovIXvpgD0.b7bYClAsRV3E0zE9ptbikg20mqA0ncjJ3imktXydRMpjAKK
gkORQfhBZif.BhYiz.:20382:0:99999:7:::
systemd-coredump: !! :20382:::::
vboxadd:l:20382:::::
audit_test:!:20503:0:99999:7:::
purity@kali:~$ 

```

For audit_test, the field contains:

!

*This indicates the account has **no valid password set** (locked or inactive password field).*



```
purity@kali: ~
```

```
File Actions Edit View Help
```

```
systemd-network:*:20382:0:99999:7:::
```

```
systemd-resolve:*:20382:0:99999:7:::
```

```
mysql:!:20382:0:99999:7:::
```

```
ntp:*:20382:0:99999:7:::
```

```
messagebus:*:20382:0:99999:7:::
```

```
redsocks!:20382:0:99999:7:::
```

```
rwhod:*:20382:0:99999:7:::
```

```
iodine:*:20382:0:99999:7:::
```

```
tcpdump:*:20382:0:99999:7:::
```

```
miredo:*:20382:0:99999:7:::
```

```
dnsmasq:*:20382:0:99999:7:::
```

```
usbmux:*:20382:0:99999:7:::
```

```
_rpc:*:20382:0:99999:7:::
```

```
Debian-snmp!:20382:0:99999:7:::
```

```
statd:*:20382:0:99999:7:::
```

```
postgres:*:20382:0:99999:7:::
```

```
stunnel4!:20382:0:99999:7:::
```

```
sshd:*:20382:0:99999:7:::
```

```
sslh!:20382:0:99999:7:::
```

```
pulse:*:20382:0:99999:7:::
```

```
inetsim:*:20382:0:99999:7:::
```

```
colord:*:20382:0:99999:7:::
```

```
geoclue:*:20382:0:99999:7:::
```

```
lightdm:*:20382:0:99999:7:::
```

```
king_phisher!:+:20382:0:99999:7:::
```

```
purity:$6$8e0e6irDqMbZ25x0$xc.kec9.VnyovIXvpgD0.b7bYClAsRV3E0zE9ptbikg20mqA0ncjJ3imktXydRMpjAKKgkORQfhBZiF.BhYiZ.:20382:0:99999:7:::
```

```
systemd-coredump:!!:20382:.....:
```

```
vboxadd!:20382:.....:
```

```
audit_test!:20503:0:99999:7:::
```

```
purity@kali:~$
```

For purity, the field contains a password hash meaning it has a password

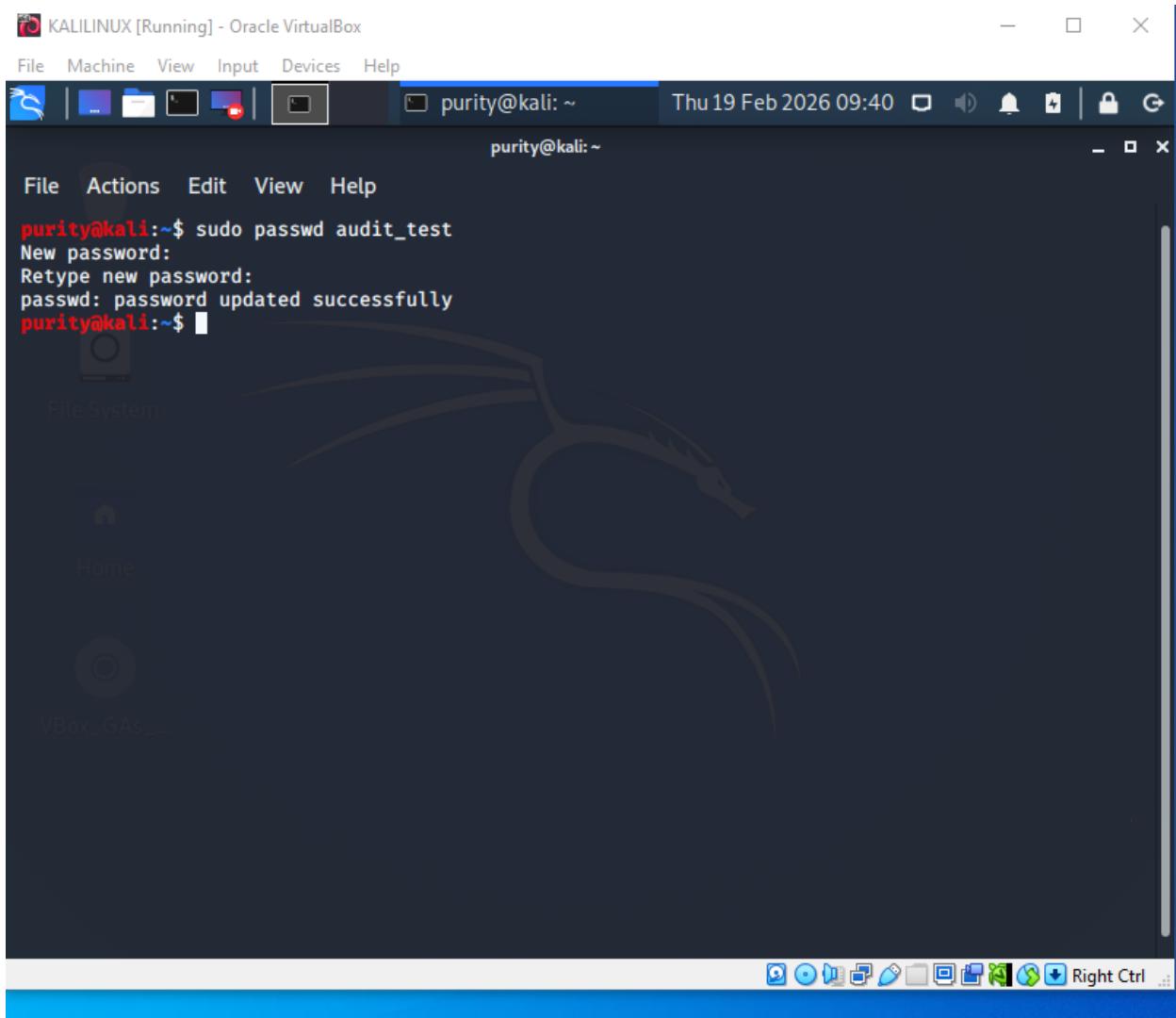
Security / System Implications

The /etc/shadow file is highly sensitive. It is permission-restricted because it contains password hashes. If readable by non-privileged users, it would present a serious security risk. Proper file permissions protect against offline password cracking attempts.

Part C: Remediation – Setting a Password

Password-Setting Command

`sudo passwd audit_test`



The screenshot shows a Kali Linux desktop environment within Oracle VirtualBox. The terminal window title is "purity@kali: ~". The terminal content is as follows:

```
purity@kali:~$ sudo passwd audit_test
New password:
Retype new password:
passwd: password updated successfully
purity@kali:~$
```

The desktop background features the Kali Linux logo (a stylized dragon). The taskbar at the bottom includes icons for File System, Home, and VBox_GAs_... along with other system icons.

KALILINUX [Running] - Oracle VirtualBox

File Machine View Input Devices Help

purity@kali: ~

Thu 19 Feb 2026 09:41

Lock Screen

File Actions Edit View Help

```
purity@kali:~$ sudo cat /etc/shadow
root:$6$pGRMDj.bE0t.S9nc$nH2n2oqheec8AX2mIvidMaQyuuhB3nNe1zz.j7E.jGPYrBUU4kSFhswWgWMpOgbEgZKV3
C/Kxtu8Fyo10n4a0:20498:0:99999:7:::
daemon:*:20382:0:99999:7:::
bin:*:20382:0:99999:7:::
sys:*:20382:0:99999:7:::
sync:*:20382:0:99999:7:::
games:*:20382:0:99999:7:::
man:*:20382:0:99999:7:::
lp:*:20382:0:99999:7:::
mail:*:20382:0:99999:7:::
news:*:20382:0:99999:7:::
uucp:*:20382:0:99999:7:::
proxy:*:20382:0:99999:7:::
www-data:*:20382:0:99999:7:::
backup:*:20382:0:99999:7:::
list:*:20382:0:99999:7:::
irc:*:20382:0:99999:7:::
gnats:*:20382:0:99999:7:::
nobody:*:20382:0:99999:7:::
_apt:*:20382:0:99999:7:::
systemd-timesync:*:20382:0:99999:7:::
systemd-network:*:20382:0:99999:7:::
systemd-resolve:*:20382:0:99999:7:::
mysql:!:20382:0:99999:7:::
ntp:*:20382:0:99999:7:::
messagebus:*:20382:0:99999:7:::
redsocks:!:20382:0:99999:7:::
rwhod:*:20382:0:99999:7:::
iodine:*:20382:0:99999:7:::
tcpdump:*:20382:0:99999:7:::
```

To verify I ran:

sudo cat /etc/shadow

KALILINUX [Running] - Oracle VirtualBox

File Machine View Input Devices Help

purity@kali: ~

purity@kali: ~

File Actions Edit View Help

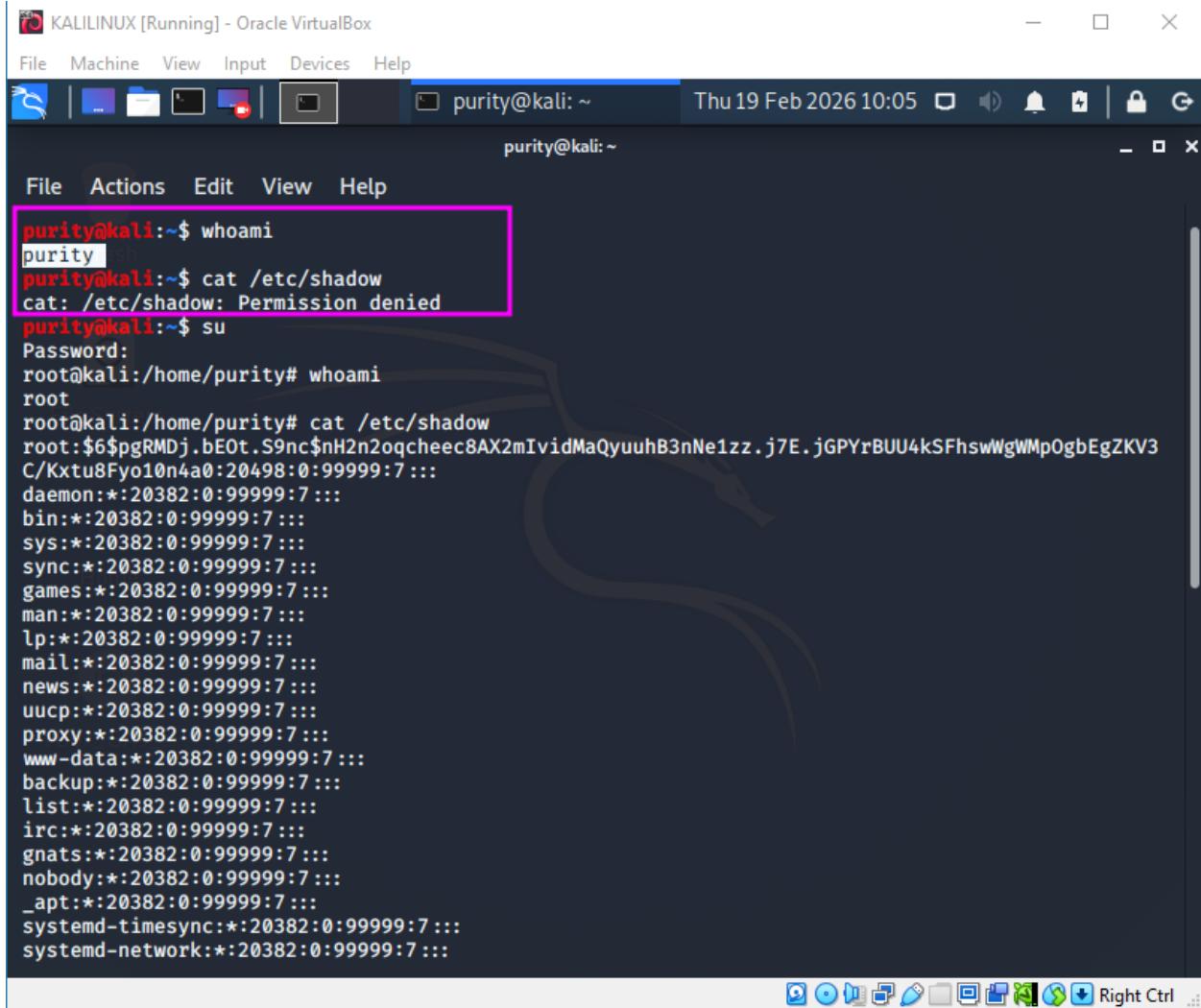
```
systemd-resolve::*:20382:0:99999:7:::  
mysql:!:20382:0:99999:7:::  
ntp::*:20382:0:99999:7:::  
messagebus::*:20382:0:99999:7:::  
redsocks:!:20382:0:99999:7:::  
rwhod:*:20382:0:99999:7:::  
iodine:*:20382:0:99999:7:::  
tcpdump:*:20382:0:99999:7:::  
miredo::*:20382:0:99999:7:::  
dnsmasq;*:20382:0:99999:7:::  
usbmux:*:20382:0:99999:7:::  
_rpc::*:20382:0:99999:7:::  
Debian-snmp!:20382:0:99999:7:::  
statd:*:20382:0:99999:7:::  
postgres:*:20382:0:99999:7:::  
stunnel4!:20382:0:99999:7:::  
sshd:*:20382:0:99999:7:::  
sslh!:20382:0:99999:7:::  
pulse:*:20382:0:99999:7:::  
inetsim:*:20382:0:99999:7:::  
colord:*:20382:0:99999:7:::  
geoclue::*:20382:0:99999:7:::  
lightdm-*:20382:0:99999:7:::  
king-phisher::*:20382:0:99999:7:::  
purity:$6$e0e6irDqMbZ25x0$xc.kec9.VnyovIXvpgD0.b7bYClAsRV3E0zE9ptbikg20mqA0ncjJ3imktXydRMpjAKK  
gkORQfhBZiF.BhYiZ.:20382:0:99999:7:::  
systemd-coredump: !!:20382:::::  
vboxadd;!:20382:::::  
audit_test:$6$u6KM0C9Nm/ccIfA2$xEWwogjCGgjDiZrDpv1DIJbdbLXVnlxj41hvIBNEpmPkEMv8MME1oGCeacwTJ1jY  
l4fYtQa80VOZI02sQRBbv1:20503:0:99999:7:::  
purity@kali:~$
```

The ! was replaced by a long hashed value.

Security / System Implications

The presence of a hashed password confirms that the account can now authenticate using password-based login (depending on system configuration). The hashing algorithm ensures that even if `/etc/shadow` is compromised, plaintext passwords are not directly exposed.

Demonstrate, using the terminal, whether a normal (non-privileged) user can access the system location where password data is stored, and arrive at a conclusion based on your observation.



KALILINUX [Running] - Oracle VirtualBox

File Machine View Input Devices Help

purity@kali: ~ Thu 19 Feb 2026 10:05

purity@kali: ~

File Actions Edit View Help

```
purity@kali:~$ whoami
purity
purity@kali:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
purity@kali:~$ su
Password:
root@kali:/home/purity# whoami
root
root@kali:/home/purity# cat /etc/shadow
root:$6$pgRMDj.bE0t.S9nc$nH2n2oqcheec8AX2mIvidMaQyuuB3nNe1zz.j7E.jGPYrBUU4kSFhsWgWMp0gbEgZKV3
C/Kxtu8Fyo10n4a0:20498:0:99999:7:::
daemon:*:20382:0:99999:7:::
bin:*:20382:0:99999:7:::
sys:*:20382:0:99999:7:::
sync:*:20382:0:99999:7:::
games:*:20382:0:99999:7:::
man:*:20382:0:99999:7:::
lp:*:20382:0:99999:7:::
mail:*:20382:0:99999:7:::
news:*:20382:0:99999:7:::
uucp:*:20382:0:99999:7:::
proxy:*:20382:0:99999:7:::
www-data:*:20382:0:99999:7:::
backup:*:20382:0:99999:7:::
list:*:20382:0:99999:7:::
irc:*:20382:0:99999:7:::
gnats:*:20382:0:99999:7:::
nobody:*:20382:0:99999:7:::
_apt:*:20382:0:99999:7:::
systemd-timesync*:20382:0:99999:7:::
systemd-network*:20382:0:99999:7:::
```

Right Ctrl

To test access permissions:

*I ran the command **whoami** to verify that I'm a normal user (purity)*

*Then ran the command **cat /etc/shadow** (should fail)*

The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal session is as follows:

```
purity@kali:~$ whoami
purity
purity@kali:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
purity@kali:~$ su
Password:
root@kali:/home/purity# whoami
root
root@kali:/home/purity# cat /etc/shadow
root:$6$pgRMDj.bEoT.S9nc$nh2n2oqcheec8AX2mIvidMaQyuuhB3nNe1zz.j7E.jGPYrBUU4kSFhswWgWMp0gbEgZKV3
C/Kxtu8Fyo10n4a0:20498:0:99999:7:::
daemon:*:20382:0:99999:7:::
bin:*:20382:0:99999:7:::
sys:*:20382:0:99999:7:::
sync:*:20382:0:99999:7:::
games:*:20382:0:99999:7:::
man:*:20382:0:99999:7:::
lp:*:20382:0:99999:7:::
mail:*:20382:0:99999:7:::
news:*:20382:0:99999:7:::
uucp:*:20382:0:99999:7:::
proxy:*:20382:0:99999:7:::
www-data:*:20382:0:99999:7:::
backup:*:20382:0:99999:7:::
list:*:20382:0:99999:7:::
irc:*:20382:0:99999:7:::
gnats:*:20382:0:99999:7:::
nobody:*:20382:0:99999:7:::
_apt:*:20382:0:99999:7:::
systemd-timesync:*:20382:0:99999:7:::
systemd-network:*:20382:0:99999:7:::
```

After switching user to **root**, I was able to view the **/etc/shadow**

Observation.

/etc/passwd is readable by normal users

/etc/shadow is not readable by normal users, permission denied for normal users

A normal (non-privileged) users **cannot access password data** stored in **/etc/shadow**.

Scenario 2: DevSecOps User & Department Access Configuration

You are a DevSecOps Engineer responsible for onboarding new staff onto a Linux server used for application development, security monitoring, QA, and CI/CD operations. Company policy enforces department-based access control, least privilege, and audit traceability.

Newly On boarded Staff

- lateef
- purity
- arthur
- paula
- yaa
- alex
- habiba
- aminat

Department Groups

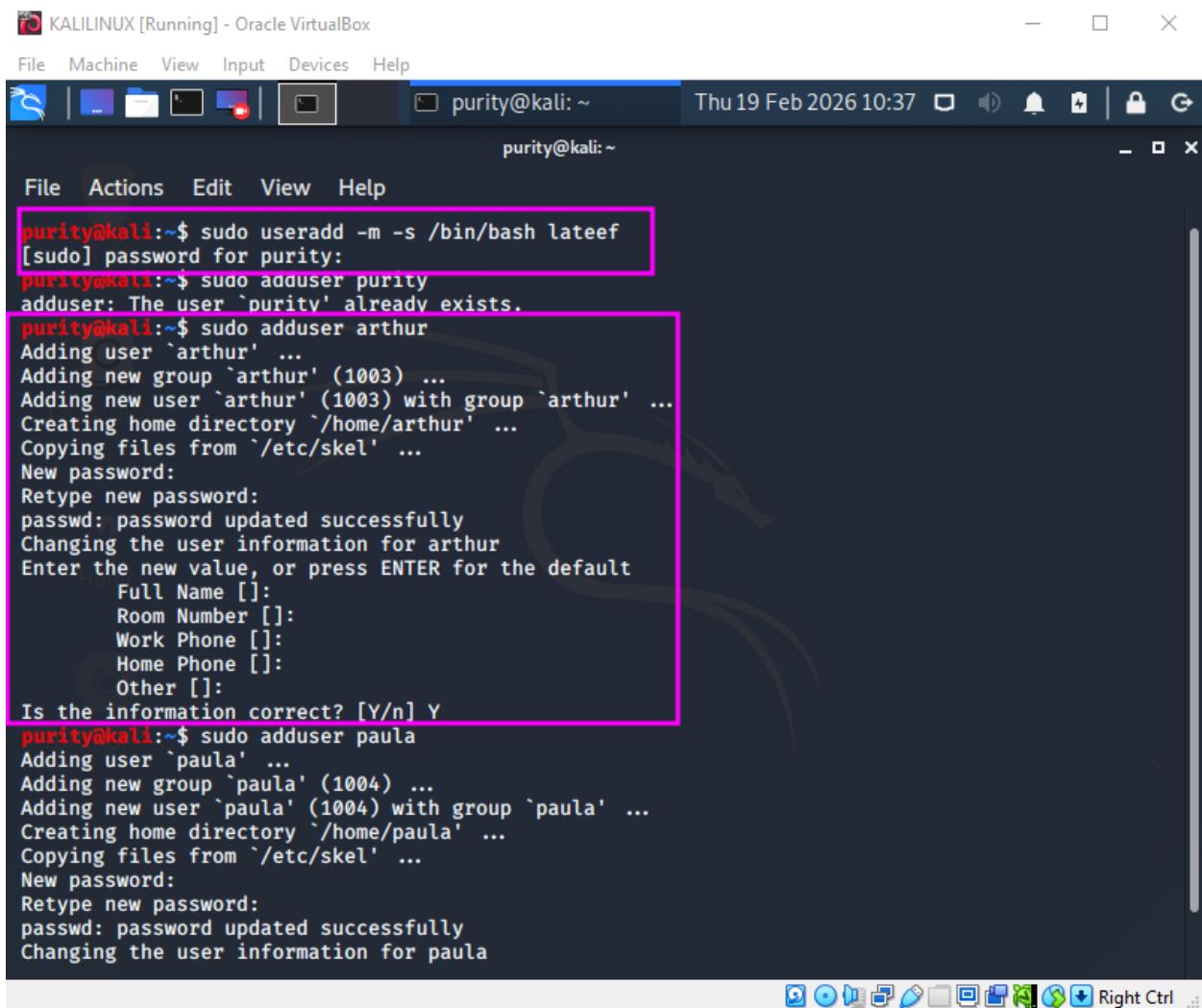
- dev_team – Application Developers
- sec_team – Security & SOC
- qa_team – Quality Assurance
- ops_team – Operations & Infrastructure

Service Account

- ci_runner – CI/CD automation (non-login account)

Tasks

1. Create all on boarded users using a mix of user management commands.



The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal session is for user "purity" at the command line "purity@kali: ~". The terminal window has a dark theme with a blue header bar. A pink rectangle highlights the first command entered: "purity@kali:~\$ sudo useradd -m -s /bin/bash lateef". The terminal then displays the password prompt "[sudo] password for purity:" followed by the error message "adduser: The user 'purity' already exists.". Subsequent commands show the creation of users "arthur" and "paula" using "adduser". Each user creation involves setting a password, creating a home directory, and updating user information. The terminal ends with the question "Is the information correct? [Y/n] Y". The bottom of the terminal window shows a toolbar with various icons.

```
purity@kali:~$ sudo useradd -m -s /bin/bash lateef
[sudo] password for purity:
purity@kali:~$ sudo adduser purity
adduser: The user 'purity' already exists.

purity@kali:~$ sudo adduser arthur
Adding user `arthur' ...
Adding new group `arthur' (1003) ...
Adding new user `arthur' (1003) with group `arthur' ...
Creating home directory `/home/arthur' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for arthur
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []
Is the information correct? [Y/n] Y

purity@kali:~$ sudo adduser paula
Adding user `paula' ...
Adding new group `paula' (1004) ...
Adding new user `paula' (1004) with group `paula' ...
Creating home directory `/home/paula' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for paula
```

I used `useradd -m -s /bin/bash lateef` to manually create the user `lateef`, where:

- `-m` created the home directory.
- `-s /bin/bash` assigned Bash as the default login shell.

```
KALILINUX [Running] - Oracle VirtualBox
File Machine View Input Devices Help
purity@kali: ~ Thu 19 Feb 2026 10:42
purity@kali: ~
File Actions Edit View Help
Creating home directory `/home/habiba' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for habiba
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
purity@kali:~$ sudo adduser aminat
Adding user `aminat' ...
Adding new group `aminat' (1008) ...
Adding new user `aminat' (1008) with group `aminat' ...
Creating home directory `/home/aminat' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for aminat
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []
Is the information correct? [Y/n] Y
purity@kali:~$
```

I used the **adduser** command to create other users such as arthur and paula. This command:

- Automatically created their home directories.
- Prompted me to set passwords.
- Allowed me to configure additional user information.
- Created a corresponding primary group for each user.

KALILINUX [Running] - Oracle VirtualBox

File Machine View Input Devices Help

purity@kali: ~

Thu 19 Feb 2026 10:49

purity@kali: ~

File Actions Edit Help

```
purity@kali:~$ sudo groupadd dev_team
purity@kali:~$ sudo groupadd sec_team
purity@kali:~$ sudo groupadd qa_team
purity@kali:~$ sudo groupadd ops_team
purity@kali:~$ gousps
bash: gousps: command not found
purity@kali:~$ groups
purity cdrom floppy sudo audio dip video plugdev netdev bluetooth lpadmin scanner
purity@kali:~$ cat /etc/groups
cat: /etc/groups: No such file or directory
purity@kali:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:purity
floppy:x:25:purity
tape:x:26:
```

I created four department groups using the command **sudo groupadd** and verified their creation using the command **cat /etc/group**



```
purity@kali:~
```

```
File Machine View Input Devices Help
```

```
purity@kali:~
```

```
File Actions Edit View Help
```

```
postgres:x:122:  
i2c:x:123:  
stunnel4:x:124:  
lpadmin:x:125:purity  
sslh:x:126:  
scanner:x:127:purity  
pulse:x:128:  
pulse-access:x:129:  
sambashare:x:130:  
inetsim:x:131:  
colord:x:132:  
geoclue:x:133:  
lightdm:x:134:  
kpadmins:x:135:  
purity:x:1000:  
systemd-coredump:x:999:  
vboxsf:x:998:  
vboxdrmipc:x:997:  
audit_test:x:1001:  
lateef:x:1002:  
arthur:x:1003:  
paula:x:1004:  
yaa:x:1005:  
alex:x:1006:  
habiba:x:1007:  
aminat:x:1008:  
dev_team:x:1009:  
sec_team:x:1010:  
qa_team:x:1011:  
ops_team:x:1012:  
purity@kali:~$
```

2. Assign users to departments as follows:

- lateef, arthur → dev_team
- purity, habiba → sec_team
- paula, yaa → qa_team
- alex, aminat → ops_team

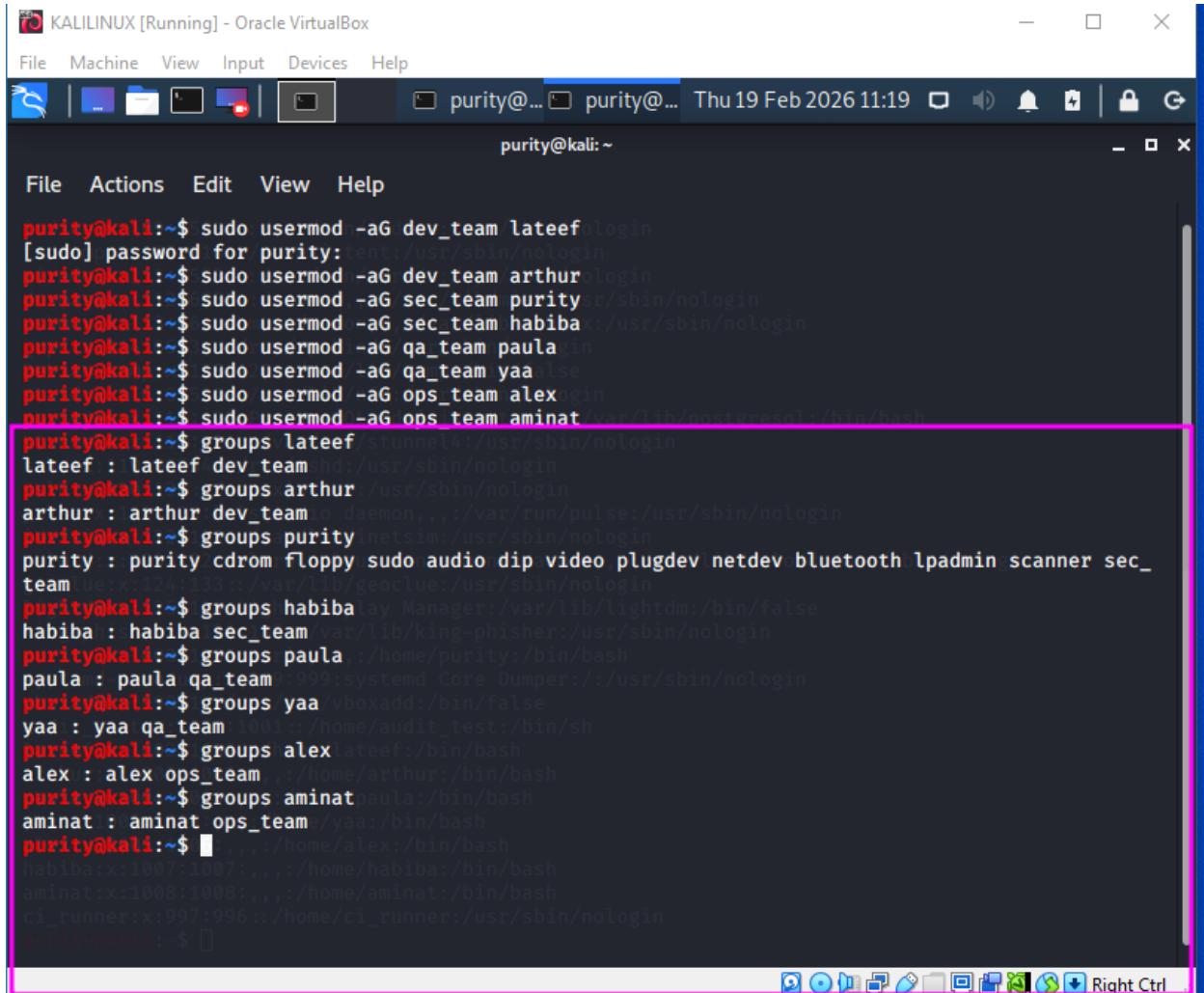
The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal is running on a Kali Linux system. The user "purity" is executing several "sudo usermod" commands to add users to specific groups. The output of these commands is as follows:

```
purity@kali:~$ sudo usermod -aG dev_team lateef
[sudo] password for purity: lateef:/usr/sbin/nologin
purity@kali:~$ sudo usermod -aG dev_team arthur
purity@kali:~$ sudo usermod -aG sec_team purity
purity@kali:~$ sudo usermod -aG sec_team habiba
purity@kali:~$ sudo usermod -aG qa_team paula
purity@kali:~$ sudo usermod -aG qa_team yaa
purity@kali:~$ sudo usermod -aG ops_team alex
purity@kali:~$ sudo usermod -aG ops_team aminat
purity@kali:~$ 
sshd:x:119:65534::/run/sshd:/usr/sbin/nologin
sslh:x:120:126::/nonexistent:/usr/sbin/nologin
pulse:x:121:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
inetsim:x:122:131::/var/lib/inetsim:/usr/sbin/nologin
colord:x:123:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:133::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:125:134:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:126:135::/var/lib/king-phisher:/usr/sbin/nologin
purity:x:1000:1000:purity,,,:/home/purity:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
audit_test:x:1001:1001::/home/audit_test:/bin/sh
lateef:x:1002:1002::/home/lateef:/bin/bash
arthur:x:1003:1003::/home/arthur:/bin/bash
paula:x:1004:1004::/home/paula:/bin/bash
yaa:x:1005:1005::/home/yaa:/bin/bash
alex:x:1006:1006::/home/alex:/bin/bash
habiba:x:1007:1007::/home/habiba:/bin/bash
aminat:x:1008:1008::/home/aminat:/bin/bash
ci_runner:x:997:996::/home/ci_runner:/usr/sbin/nologin
purity@kali:~$ 
```

I assigned users strictly according to their departments:

- **dev_team** → lateef, arthur
- **sec_team** → purity, habiba
- **qa_team** → paula, yaa
- **ops_team** → alex, aminat

This ensures that each user only has access to resources relevant to their assigned department. This structure supports proper access control and audit traceability within the system.



The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal is running on the "purity" user account. The user has run several "sudo usermod" commands to add users to specific groups. The output of these commands is highlighted with a pink rectangle. The user has also run the "groups" command for each user to verify their group membership.

```
purity@kali:~$ sudo usermod -aG dev_team lateef
[sudo] password for purity: 
purity@kali:~$ sudo usermod -aG dev_team arthur
purity@kali:~$ sudo usermod -aG sec_team purity
purity@kali:~$ sudo usermod -aG sec_team habiba
purity@kali:~$ sudo usermod -aG qa_team paula
purity@kali:~$ sudo usermod -aG qa_team yaa
purity@kali:~$ sudo usermod -aG ops_team alex
purity@kali:~$ sudo usermod -aG ops_team aminat
purity@kali:~$ groups lateef
lateef : lateef dev_team
purity@kali:~$ groups arthur
arthur : arthur dev_team
purity@kali:~$ groups purity
purity : purity cdrom floppy sudo audio dip video plugdev netdev bluetooth lpadmin scanner sec_team
purity@kali:~$ groups habiba
habiba : habiba sec_team
purity@kali:~$ groups paula
paula : paula qa_team
purity@kali:~$ groups yaa
yaa : yaa qa_team
purity@kali:~$ groups alex
alex : alex ops_team
purity@kali:~$ groups aminat
aminat : aminat ops_team
purity@kali:~$
```

After assigning users to their respective departments, I verified group membership using the **groups username** command.

The command output displayed the primary and supplementary groups associated with each user, confirming that the system correctly recognized and stored the group memberships.

3. Ensure one user is created without a password, then later set the password and confirm the change.

useradd does *not* set passwords.

I used **useradd -m -s /bin/bash lateef** to manually create the user **lateef**, where:

- **-m** created the home directory.
- **-s /bin/bash** assigned Bash as the default login shell.

KALILINUX [Running] - Oracle VirtualBox

File Machine View Input Devices Help

purity@... purity@... Thu 19 Feb 2026 11:21

purity@kali:~

File Actions Edit View Help

```
purity@kali:~$ sudo passwd lateef
New password: 116::/nonexistent:/usr/sbin/nologin
Retype new password: /var/run/miredo:/usr/sbin/nologin
passwd: password updated successfully
purity@kali:~$ lsusbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
 rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
 Debian-snmp:x:115:120::/var/lib/snmp:/bin/false
 statd:x:116:65534::/var/lib/nfs:/usr/sbin/nologin
 postgres:x:117:122:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
 stunnel4:x:118:124::/var/run/stunnel4:/usr/sbin/nologin
 sshd:x:119:65534::/run/sshd:/usr/sbin/nologin
 ssh:x:120:126::/nonexistent:/usr/sbin/nologin
 pulse:x:121:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
 inetsim:x:122:131::/var/lib/inetsim:/usr/sbin/nologin
 colord:x:123:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
 geoclue:x:124:133::/var/lib/geoclue:/usr/sbin/nologin
 lightdm:x:125:134:Light Display Manager:/var/lib/lightdm:/bin/false
 king-phisher:x:126:135::/var/lib/king-phisher:/usr/sbin/nologin
 purity:x:1000:1000:purity,,,:/home/purity:/bin/bash
 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
 vboxadd:x:998:1::/var/run/vboxadd:/bin/false
 audit_test:x:1001:1001::/home/audit_test:/bin/sh
 lateef:x:1002:1002::/home/lateef:/bin/bash
 arthur:x:1003:1003,,,:/home/arthur:/bin/bash
 paula:x:1004:1004,,,:/home/paula:/bin/bash
 yaa:x:1005:1005,,,:/home/yaa:/bin/bash
 alex:x:1006:1006,,,:/home/alex:/bin/bash
 habiba:x:1007:1007,,,:/home/habiba:/bin/bash
 aminat:x:1008:1008,,,:/home/aminat:/bin/bash
 ci_runner:x:997:996::/home/ci_runner:/usr/sbin/nologin
 purity@kali:~$ 
```

The account existed but **did not** have an active password.

To remediate this, I used the command: **sudo passwd lateef**

4. Configure the ci_runner account with a non-login shell.

The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal session is for user "purity" on the "kali" host. The command "sudo useradd -r -s /usr/sbin/nologin ci_runner" is run, followed by "cat /etc/passwd" to show the updated password file. A pink rectangle highlights the command and its output. The output lists various system accounts with their respective user IDs, group IDs, and shells. The "ci_runner" account is listed with a user ID of 65534, a group ID of 65534, and a shell of "/usr/sbin/nologin".

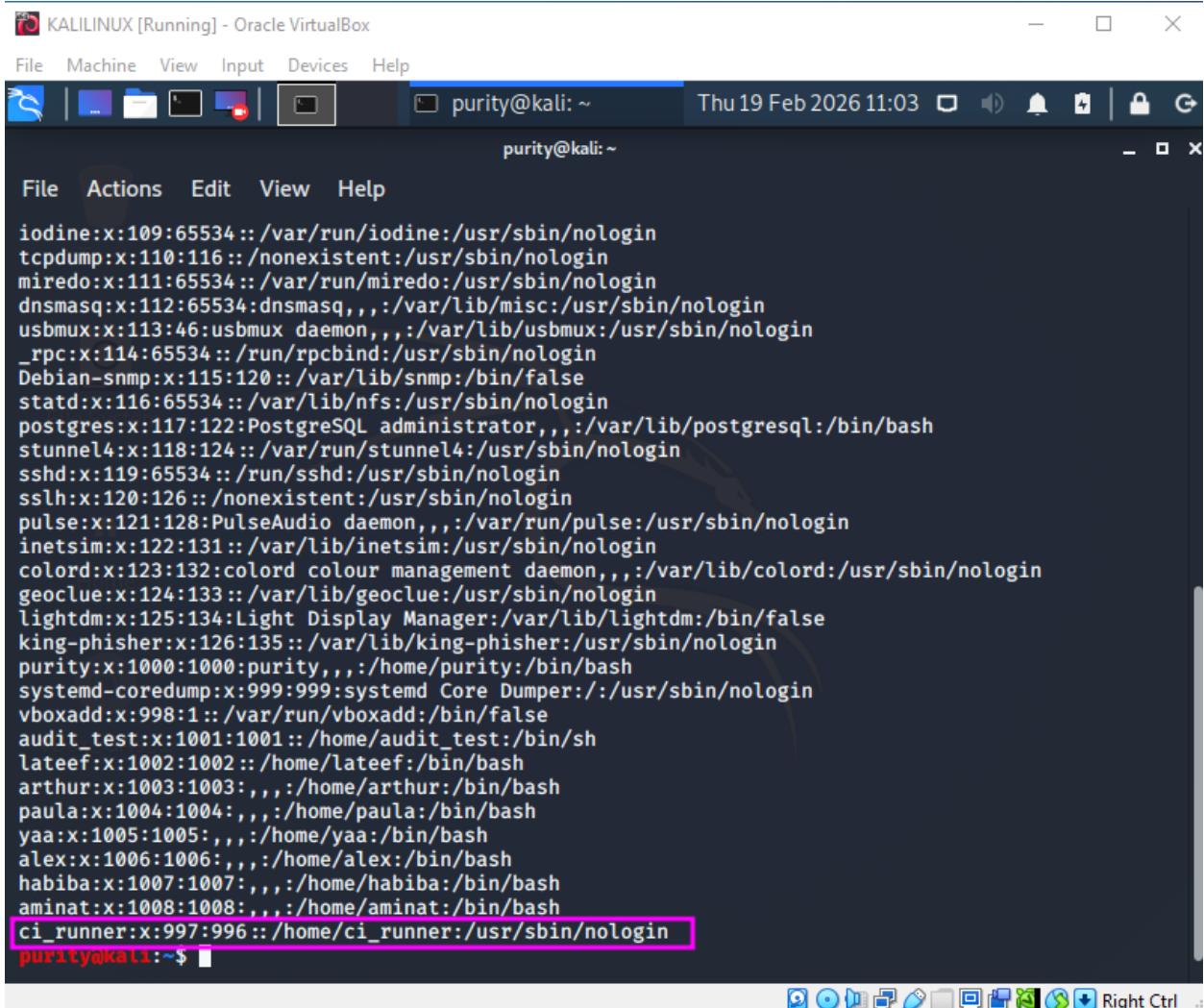
```
purity@kali:~$ sudo useradd -r -s /usr/sbin/nologin ci_runner
purity@kali:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,,:/nonexistent:/bin/false
ntp:x:105:111::/nonexistent:/usr/sbin/nologin
messagebus:x:106:112::/nonexistent:/usr/sbin/nologin
redsocks:x:107:113::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:108:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:109:65534::/var/run/iodine:/usr/sbin/nologin
tcpdump:x:110:116::/nonexistent:/usr/sbin/nologin
```

I created the ci_runner service account using the command:

sudo useradd -r -s /usr/sbin/nologin ci_runner

- **-r** created the account as a **system account** (used for services, not regular users).
- **-s /usr/sbin/nologin** assigned a **non-login shell**, preventing interactive access.

This ensures the account is strictly used for automated CI/CD processes and cannot be used to log into the system manually.



```
iodine:x:109:65534::/var/run/iodine:/usr/sbin/nologin
tcpdump:x:110:116::/nonexistent:/usr/sbin/nologin
miredo:x:111:65534::/var/run/miredo:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
_rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:115:120::/var/lib/snmp:/bin/false
statd:x:116:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:x:117:122:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
stunnel4:x:118:124::/var/run/stunnel4:/usr/sbin/nologin
sshd:x:119:65534::/run/sshd:/usr/sbin/nologin
sslh:x:120:126::/nonexistent:/usr/sbin/nologin
pulse:x:121:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
inetsim:x:122:131::/var/lib/inetsim:/usr/sbin/nologin
colord:x:123:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:133::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:125:134:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:126:135::/var/lib/king-phisher:/usr/sbin/nologin
purity:x:1000:1000:purity,,,:/home/purity:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
audit_test:x:1001:1001::/home/audit_test:/bin/sh
lateef:x:1002:1002::/home/lateef:/bin/bash
arthur:x:1003:1003:,,,,:/home/arthur:/bin/bash
paula:x:1004:1004:,,,,:/home/paula:/bin/bash
yaa:x:1005:1005:,,,,:/home/yaa:/bin/bash
alex:x:1006:1006:,,,,:/home/alex:/bin/bash
habiba:x:1007:1007:,,,,:/home/habiba:/bin/bash
aminat:x:1008:1008:,,,,:/home/aminat:/bin/bash
ci_runner:x:997:996::/home/ci_runner:/usr/sbin/nologin
```

To verify the configuration, I ran:

`cat /etc/passwd`

From the output, I confirmed that: the `ci_runner` account exists.

5. Grant sudo access to one user from ops_team only; all other users must remain within their department privileges.

KALILINUX [Running] - Oracle VirtualBox

File Machine View Input Devices Help

purity@... purity@... Thu 19 Feb 2026 11:24

purity@kali:~

File Actions Edit View Help

```
purity@kali:~$ sudo usermod -aG sudo alex:bin/nologin
purity@kali:~$ groups alex
alex : alex sudo ops_team
purity@kali:~$ ls -la /var/lib/nologin
lsbmonix:113:46:lsbmux_daemon,,,:/var/lib/lsbmux:/usr/sbin/nologin
_rpcx:114:65534:ct/run/rpcbind:/usr/sbin/nologin
Debian-snmp:115:128::/var/lib/snmp:/bin/false
statdix:116:65534::/var/lib/nfs:/usr/sbin/nologin
postgres:127:128:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
stunnel4:128:124:ct/run/stunnel4:/usr/sbin/nologin
sshdix:129:65534:ct/run/sshd:/usr/sbin/nologin
sshdix:130:126::/nonexistent:/usr/sbin/nologin
pulseix:121:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
inetssimix:122:131::/var/lib/inetssim:/usr/sbin/nologin
colordisx:123:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclueix:124:133::/var/lib/geoclue:/usr/sbin/nologin
lightdmix:125:134:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisherix:126:135::/var/lib/king-phisher:/usr/sbin/nologin
purityix:1000:1000:purity,,,:/home/purity:/bin/bash
systemd-coredumpix:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxaddix:1998:1ct/run/vboxadd:/bin/false
audit-testix:1001:1001:/home/audit_test:/bin/sh
tateefix:1002:1002::/home/tateef:/bin/bash
arthurix:1003:1003,,,:/home/arthur:/bin/bash
paulaxix:1004:1004,,,:/home/paulax:/bin/bash
yaaxix:1005:1005,,,:/home/yaax:/bin/bash
alexix:1006:1006,,,:/home/alex:/bin/bash
habibatix:1007:1007,,,:/home/habibat:/bin/bash
aminatix:1008:1008,,,:/home/aminat:/bin/bash
ci_runnerix:997:996::/home/ci_runner:/usr/sbin/nologin
```

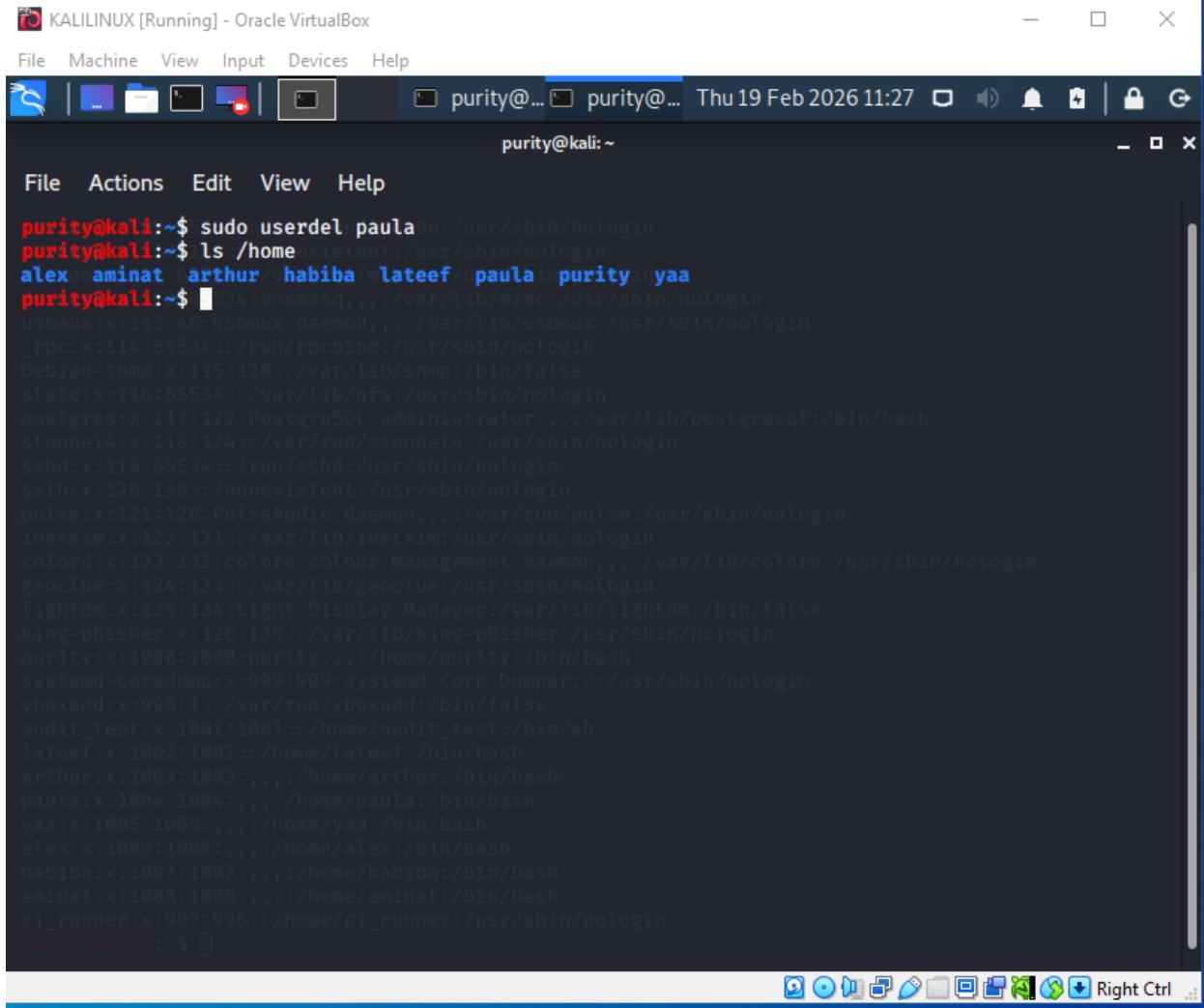
I granted sudo privileges to only one user from the ops_team group- **alex** by adding him to the **sudo** group. All other users in the system do not have sudo access and are restricted.

To verify that alex has sudo privileges, I checked his group membership using the command:

groups alex

The output showed that **alex** is a member of the **sudo** group which grants administrative privileges. Being part of the sudo group means **alex** can execute commands with elevated privileges using **sudo**, while other users without this group membership cannot.

6. Remove one user account while preserving the home directory for audit and security reasons.



The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal window has a dark background and contains the following text:

```
purity@kali:~$ sudo userdel paula
purity@kali:~$ ls /home
existent:/usr/sbin/nologin
alex:aminat: arthur:habiba: lateef: paula: purity:yaa
purity@kali:~$ █ 534: dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
_rpc:x:114:65534 ::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:115:120 ::/var/lib/snmp:/bin/false
statd:x:116:65534 ::/var/lib/nfs:/usr/sbin/nologin
postgres:x:117:122:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
stunnel4:x:118:124 ::/var/run/stunnel4:/usr/sbin/nologin
sshd:x:119:65534 ::/run/sshd:/usr/sbin/nologin
sshd:x:120:126 ::/nonexistent:/usr/sbin/nologin
pulse:x:121:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
inetsim:x:122:131 ::/var/lib/inetsim:/usr/sbin/nologin
colord:x:123:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geooclue:x:124:133 ::/var/lib/geooclue:/usr/sbin/nologin
lightdm:x:125:134:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:126:135 ::/var/lib/king-phisher:/usr/sbin/nologin
purity:x:1000:1000:purity,,,:/home/purity:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:::/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
audit_test:x:1001:1001::/home/audit_test:/bin/sh
lateef:x:1002:1002::/home/lateef:/bin/bash
arthur:x:1003:1003:,,,:/home/arthur:/bin/bash
paula:x:1004:1004:,,,:/home/paula:/bin/bash
yaa:x:1005:1005:,,,:/home/yaa:/bin/bash
alex:x:1006:1006:,,,:/home/alex:/bin/bash
habiba:x:1007:1007:,,,:/home/habiba:/bin/bash
aminat:x:1008:1008:,,,:/home/aminat:/bin/bash
ci_runner:x:997:996::/home/ci_runner:/usr/sbin/nologin
purity@kali:~$ █
```

I removed the user **paula** from the system using the command: **sudo userdel paula**.

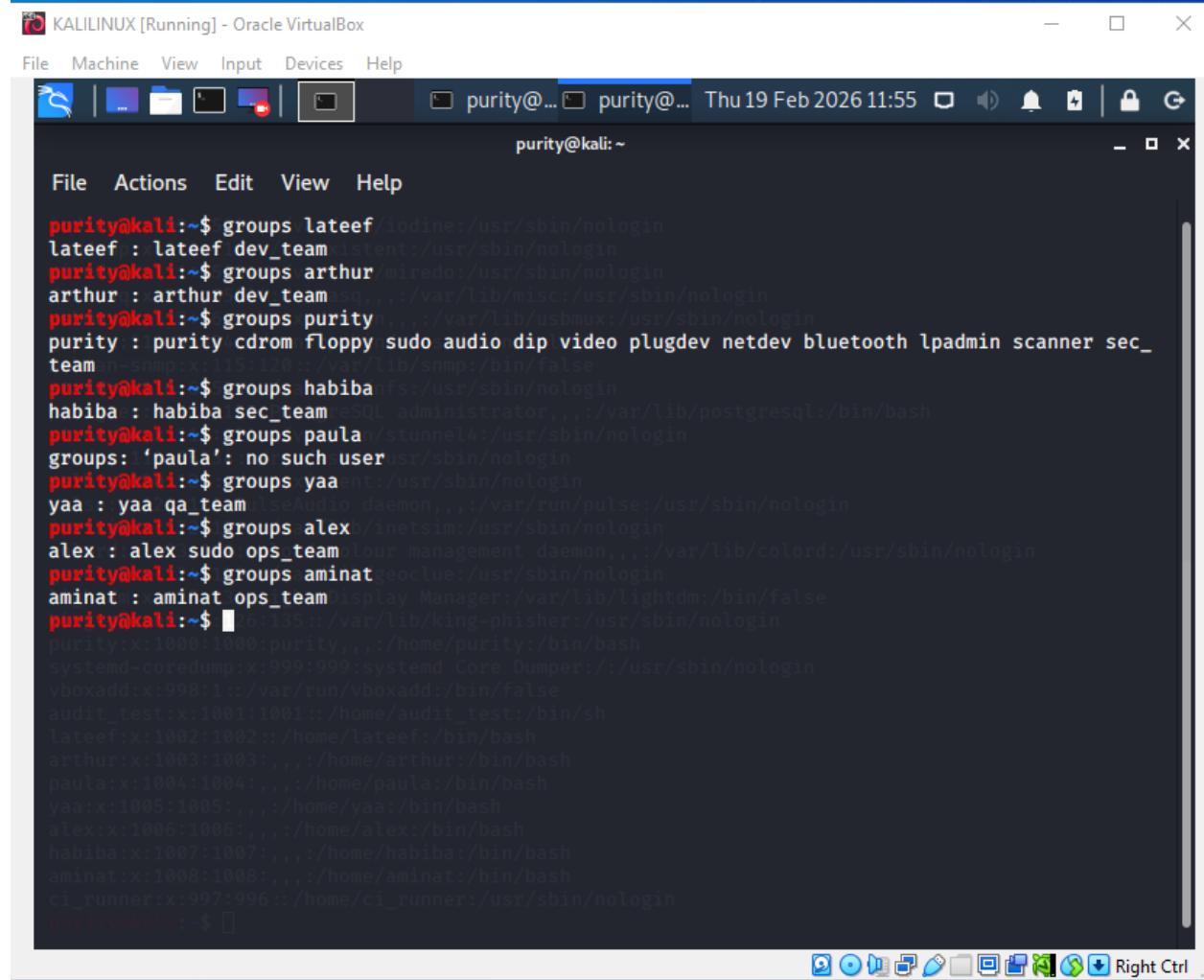
sudo userdel -r paula removes home directory

I verified home directory for paula still exists using **ls /home** command.

The home directory **/home/paula** remained intact, preserving files and configuration for audit or forensic purposes.

7. Verify and demonstrate that:

- Department group membership is correctly assigned



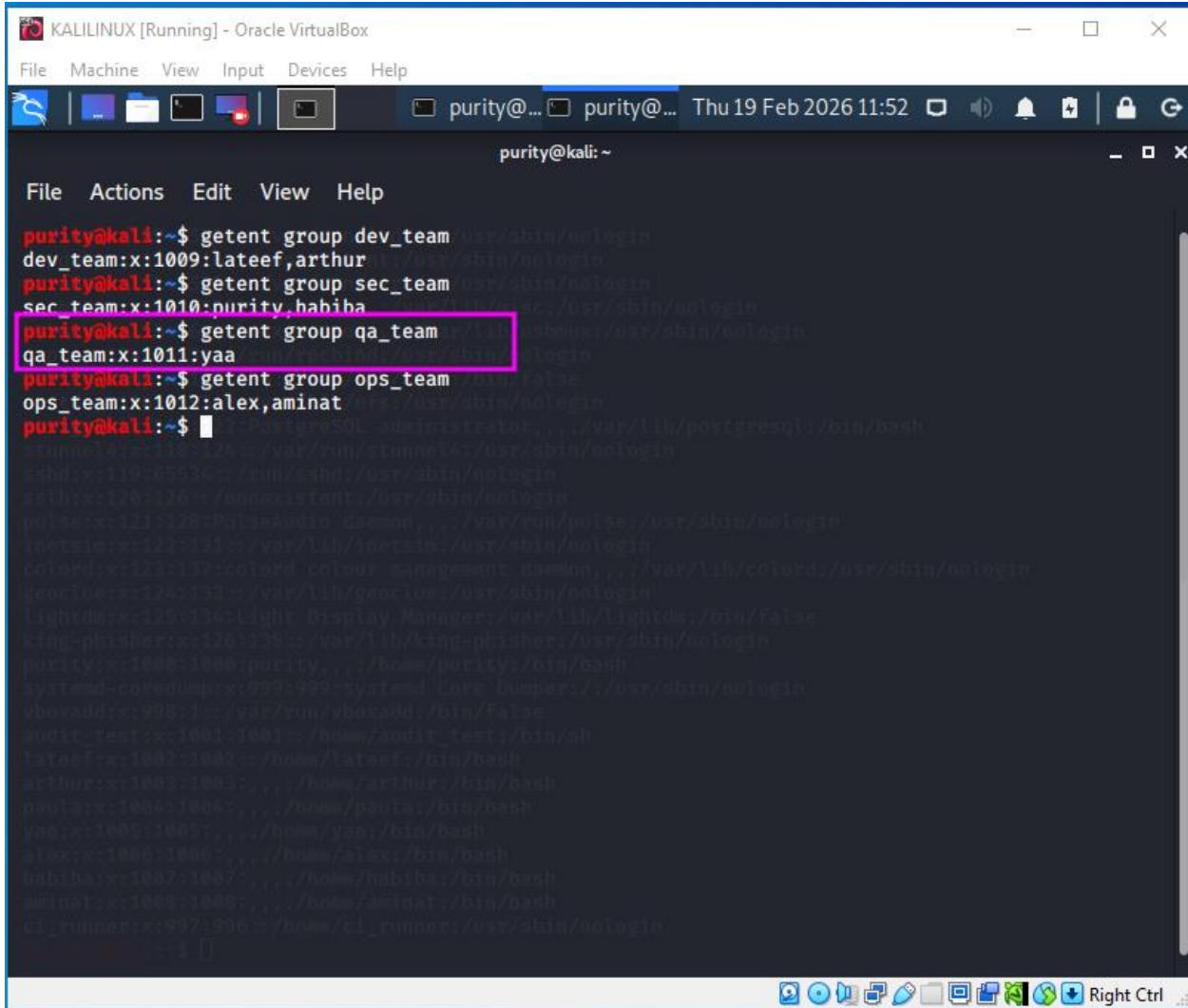
The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal displays the output of the "groups" command for various users on a Kali Linux system. The users listed include lateef, arthur, purity, paula, yaa, alex, aminat, and ci_runner. The terminal interface includes a menu bar with File, Actions, Edit, View, Help, and a toolbar with icons for file operations like Open, Save, and Print.

```
purity@kali:~$ groups lateef iodine:/usr/sbin/nologin
lateef : lateef dev_team cent:/usr/sbin/nologin
purity@kali:~$ groups arthur miredo:/usr/sbin/nologin
arthur : arthur dev_team snmp:/var/lib/misc:/usr/sbin/nologin
purity@kali:~$ groups purity yaa:/var/lib/usbmux:/usr/sbin/nologin
purity : purity cdrom floppy sudo audio dip video plugdev netdev bluetooth lpadmin scanner sec_
team man-snmp:x:115:120::/var/lib/snmp:/bin/false
purity@kali:~$ groups habiba habiba:/usr/sbin/nologin
habiba : habiba sec_team esql administrator,,,:/var/lib/postgresql:/bin/bash
purity@kali:~$ groups paula stunnel4:/usr/sbin/nologin
groups: 'paula': no such user
purity@kali:~$ groups yaa yaa:/usr/sbin/nologin
yaa : yaa qa_team lseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
purity@kali:~$ groups alex alex/inetsim:/usr/sbin/nologin
alex : alex sudo ops_team colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
purity@kali:~$ groups aminat aminat@oclue:/usr/sbin/nologin
aminat : aminat ops_team display Manager:/var/lib/lightdm:/bin/false
purity@kali:~$ ci_runner:x:1000:1000:purity,,,:/home/purity:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
audit_test:x:1001:1001::/home/audit_test:/bin/sh
lateef:x:1002:1002::/home/lateef:/bin/bash
arthur:x:1003:1003::/home/arthur:/bin/bash
paula:x:1004:1004::/home/paula:/bin/bash
yaa:x:1005:1005::/home/yaa:/bin/bash
alex:x:1006:1006::/home/alex:/bin/bash
habiba:x:1007:1007::/home/habiba:/bin/bash
aminat:x:1008:1008::/home/aminat:/bin/bash
ci_runner:x:997:996::/home/ci_runner:/usr/sbin/nologin
purity@kali: ~
```

I used the **groups** command to verify that each user was correctly mapped to their specific department.

The command **groups paula** confirms the removal of a user (Task 6), as the command **groups paula** returns **no such user**, proving the account was successfully deleted while the system remains clean.

- Group data is recorded and retrievable from the system



```

KALILINUX [Running] - Oracle VirtualBox
File Machine View Input Devices Help
purity@... purity@... Thu 19 Feb 2026 11:52
purity@kali:~ - x
File Actions Edit View Help
purity@kali:~$ getent group dev_team
dev_team:x:1009:lateef,arthur
purity@kali:~$ getent group sec_team
sec_team:x:1010:purity,habiba
purity@kali:~$ getent group qa_team
qa_team:x:1011:yaa
purity@kali:~$ getent group ops_team
ops_team:x:1012:alex,aminat
purity@kali:~$ 

```

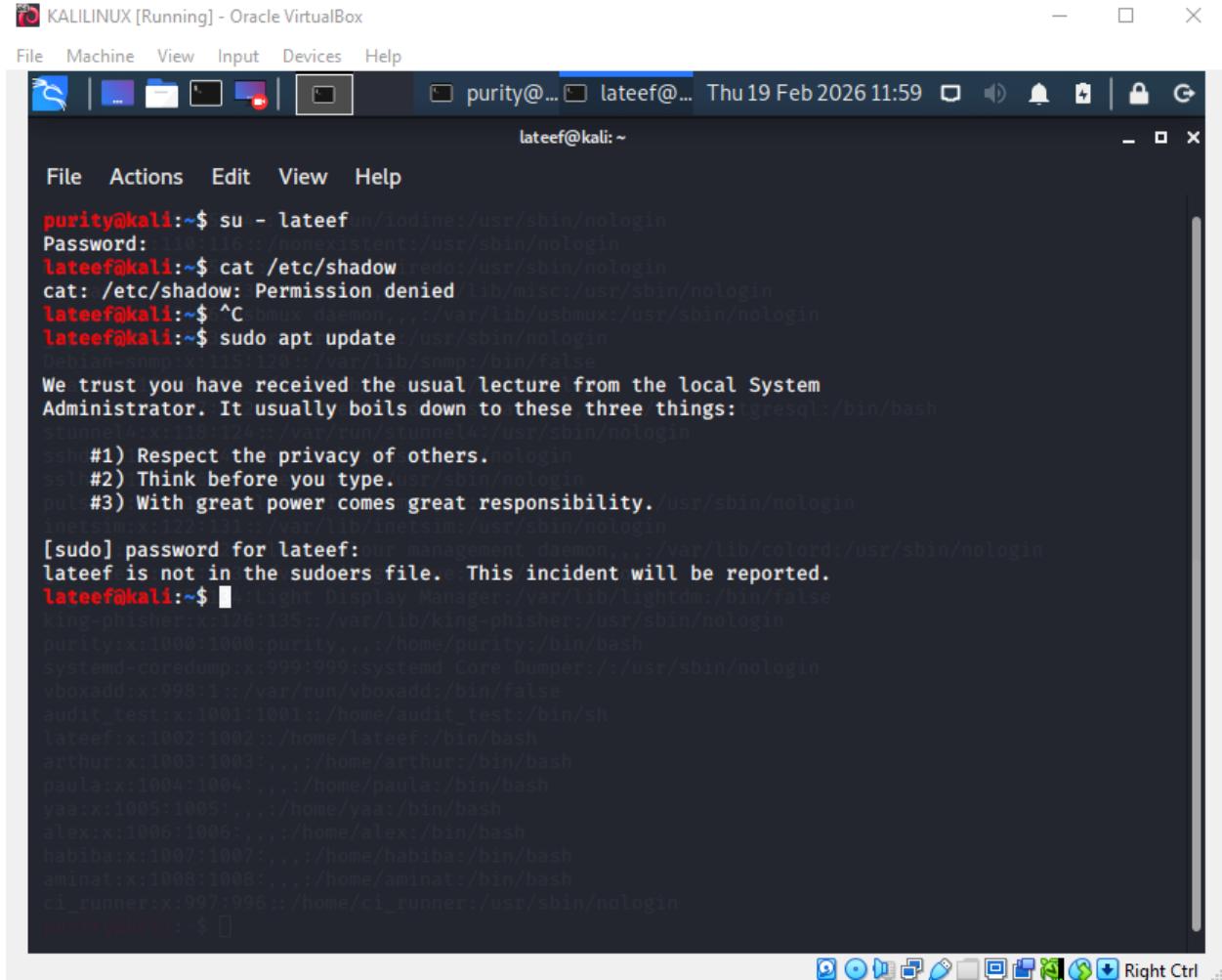
I ran the command **getent group [group_name]** for every team (**dev_team**, **sec_team**, **qa_team**, and **ops_team**) to verify that the departments have been recorded.

The command **getent group qa_team** also verifies the removal of **paula**.

Even though the initial onboarding instructions required both **paula** and **yaa** to be members of this group, only **yaa** is listed. Because I ran the command to delete the account, the Linux system automatically updated the group database to strip her name from the member list. The absence of her name here, combined with the "no such user" error I received when I ran the command **groups paula**, provides the necessary audit trail to show that the account is no longer active on the server.

- User privilege boundaries are enforced

To verify that the access controls were working in a real-world scenario, I simulated the login session for different users to test their specific permissions.



The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal is running on a Kali Linux system. The user "purity" is logged in as root. They attempt to switch to the user "lateef" using the command "su - lateef". This action fails because "lateef" is not listed in the sudoers file. The terminal output shows the password prompt for "lateef", followed by the error message: "cat: /etc/shadow: Permission denied". When "purity" tries to run the command "sudo apt update", the terminal displays a warning: "lateef is not in the sudoers file. This incident will be reported." The terminal also lists other users and their entries in the /etc/shadow file, such as "root", "bin", "daemon", "lp", "sync", "shutdown", "halt", "mail", "uucp", "operator", "games", "gopher", "nobody", "nologin", and various system daemons like "stunnel4", "sshd", "ssl", "polkit", "inetsim", "King-phisher", "purity", "systemd", "vboxadd", "audit_test", "lateef", "arthur", "paula", "yaa", "alex", "habiba", "aminat", and "ci_runner".

```
purity@kali:~$ su - lateef
Password: 
lateef@kali:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
lateef@kali:~$ sudo apt update
[sudo] password for lateef: 
lateef is not in the sudoers file. This incident will be reported.
lateef@kali:~$
```

I ran the command **su - lateef** to switch from my administrative account to Lateef's profile. Once identified as a **normal user** in the **dev_team**, I attempted to perform an administrative task.

I ran the command **sudo apt update**, and as shown in the screenshot, the system correctly denied the request with the warning: "lateef is not in the sudoers file. This incident will be reported." This confirms that Lateef is a less-privileged user.

The screenshot shows a terminal window titled "KALILINUX [Running] - Oracle VirtualBox". The terminal session is as follows:

```
lateef@kali:~$ su - alex
Password:
alex@kali:~$ sudo cat /etc/shadow
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for alex:
root:$6$pgRMDj.bE0t.S9nc$nH2n2oqcheec8AX2mIvidMaQyuuuhB3nNe1zz.j7E.jGPYrBUU4kSFhsWWgWMp0gbEgZKV3
C/Kxtu8Fyo10n4a0:20498:0:99999:7:::
daemon:*:20382:0:99999:7:::
bin:*:20382:0:99999:7:::
sys:*:20382:0:99999:7:::
sync:*:20382:0:99999:7:::
games:*:20382:0:99999:7:::
man:*:20382:0:99999:7:::
lp:*:20382:0:99999:7:::
mail:*:20382:0:99999:7:::
news:*:20382:0:99999:7:::
uucp:*:20382:0:99999:7:::
proxy:*:20382:0:99999:7:::
www-data:*:20382:0:99999:7:::
backup:*:20382:0:99999:7:::
list:*:20382:0:99999:7:::
irc:*:20382:0:99999:7:::
gnats:*:20382:0:99999:7:::
nobody:*:20382:0:99999:7:::
```

Since user **alex** was granted **sudo** access, he successfully executes **sudo cat /etc/shadow** and **sudo apt update** commands. The system displays the contents of the sensitive file, confirming that **alex** has the necessary elevated privileges to perform infrastructure and operations tasks that other users like **lateef** cannot.

This demonstrated that the system correctly distinguishes between a "normal" user and an "authorized" administrator, ensuring that only the right people have the right level of access.

CONCLUSION

The activities demonstrated practical control over Linux user lifecycle management, password auditing, group-based access enforcement, and privilege restriction. They reinforced the importance of proper access boundaries, secure configuration of service accounts, controlled privilege escalation, and maintaining audit traceability to support a secure and well-governed system environment.