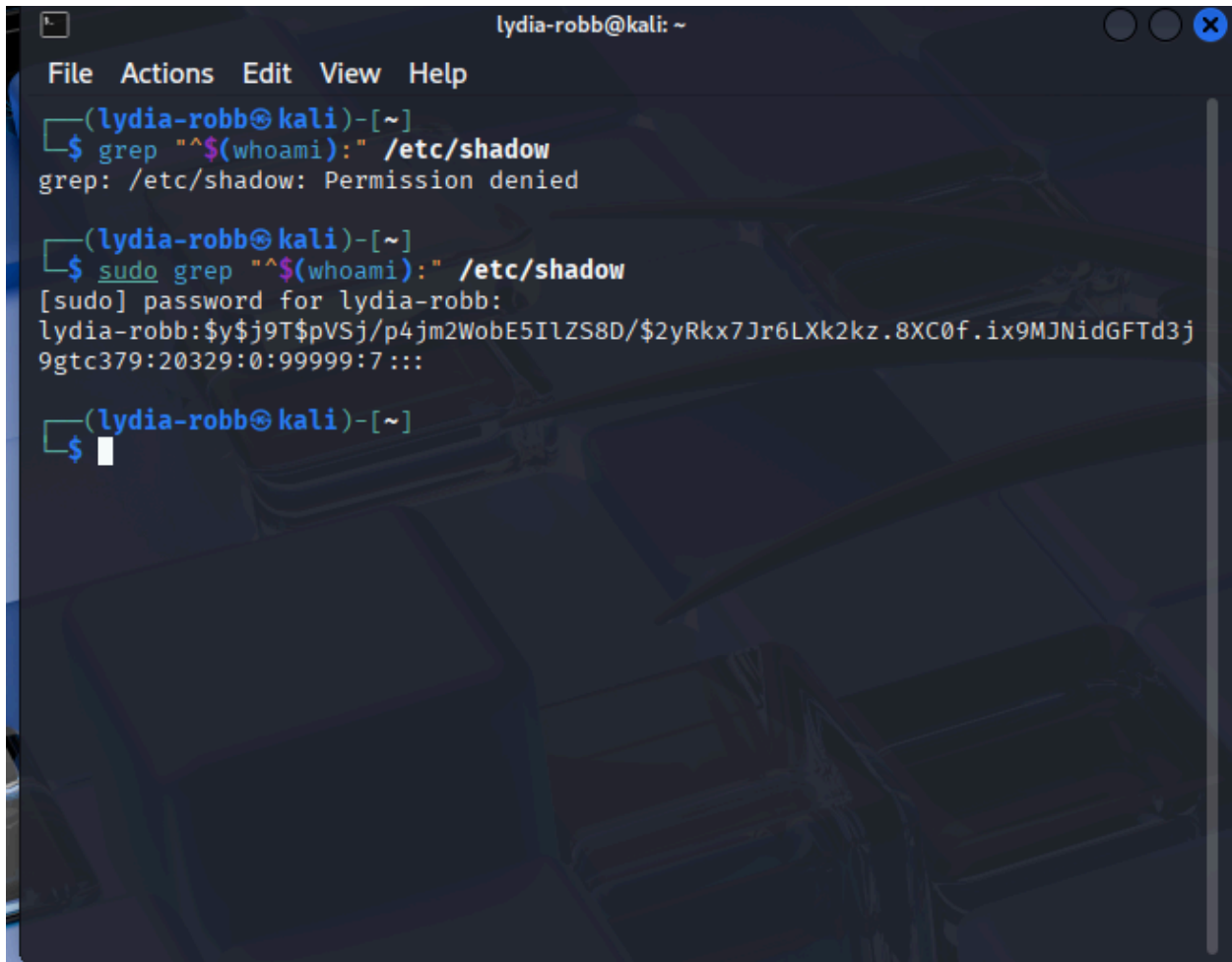


Task A

Step 1: `grep "^$(whoami):" /etc/passwd`

- The output was “access denied”, therefore it requires sudo

Step 2: `sudo grep "^$(whoami):" /etc/shadow`



```
lydia-robb@kali: ~  
File Actions Edit View Help  
(lydia-robb@kali)-[~]  
└─$ grep "^$(whoami):" /etc/shadow  
grep: /etc/shadow: Permission denied  
  
(lydia-robb@kali)-[~]  
└─$ sudo grep "^$(whoami):" /etc/shadow  
[sudo] password for lydia-robb:  
lydia-robb:$y$j9T$pVSj/p4jm2WobE5I1ZS8D/$2yRkx7Jr6LXk2kz.8XC0f.ix9MJNidGFTd3j9gtc379:20329:0:99999:7::  
  
(lydia-robb@kali)-[~]  
└─$
```

Step 3: `sudo useradd -m -d /home/lrobb005`

```
lydia-robb@kali: ~  
File Actions Edit View Help  
└─$ sudo useradd -m -d /home/lrobb005  
Usage: useradd [options] LOGIN  
       useradd -D  
       useradd -D [options]  
  
Options:  
  --badname           do not check for bad names (DEPRECATED)  
  -b, --base-dir BASE_DIR  base directory for the home directory of the  
                           new account  
  --btrfs-subvolume-home  use BTRFS subvolume for home directory  
  -c, --comment COMMENT   GECOS field of the new account  
  -d, --home-dir HOME_DIR  home directory of the new account  
  -D, --defaults          print or change default useradd configuration  
  -e, --expiredate EXPIRE_DATE  expiration date of the new account  
  -f, --inactive INACTIVE  password inactivity period of the new account  
  -F, --add-subids-for-system  add entries to sub[ud]id even when adding a s  
ystem user  
  -g, --gid GROUP         name or ID of the primary group of the new  
                           account  
  -G, --groups GROUPS     list of supplementary groups of the new  
                           account  
  -h, --help              display this help message and exit  
  -k, --skel SKEL_DIR     use this alternative skeleton directory  
  -K, --key KEY=VALUE     override /etc/login.defs defaults  
  -m, --create-home       create the user's home directory  
  -M, --no-create-home    do not create the user's home directory  
  -N, --no-user-group     do not create a group with the same name as  
                           the user
```

Step 4-5: Set password as bash as default shell

```
sudo passwd lrobb005  
sudo usermod -s /bin/bash lrobb005  
grep "^lrobb005:" /etc/passwd
```

```
lydia-robb@kali: ~  
File Actions Edit View Help  
passwd: user 'lrobb005' does not exist  
  
(lydia-robb@kali)-[~]  
└─$ getent passwd lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ sudo useradd -m -d /home/lrobb005 -s /bin/bash lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ getent passwd lrobb005  
lrobb005:x:1001:1001::/home/lrobb005:/bin/bash  
  
(lydia-robb@kali)-[~]  
└─$ ls -ld /home/lrobb005  
drwx----- 5 lrobb005 lrobb005 4096 Sep 27 13:27 /home/lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ sudo passwd lrobb005  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(lydia-robb@kali)-[~]  
└─$ grep "^lrobb005:" /etc/passwd  
lrobb005:x:1001:1001::/home/lrobb005:/bin/bash  
  
(lydia-robb@kali)-[~]  
└─$
```

Step 6: `sudo grep "^lrobb005:" /etc/shadow`

```
lydia-robb@kali: ~  
File Actions Edit View Help  
(lydia-robb@kali)-[~]  
└─$ sudo useradd -m -d /home/lrobb005 -s /bin/bash lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ getent passwd lrobb005  
lrobb005:x:1001:1001::/home/lrobb005:/bin/bash  
  
(lydia-robb@kali)-[~]  
└─$ ls -ld /home/lrobb005  
drwx----- 5 lrobb005 lrobb005 4096 Sep 27 13:27 /home/lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ sudo passwd lrobb005  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(lydia-robb@kali)-[~]  
└─$ grep "^lrobb005:" /etc/passwd  
lrobb005:x:1001:1001::/home/lrobb005:/bin/bash  
  
(lydia-robb@kali)-[~]  
└─$ sudo grep "^lrobb005:" /etc/shadow  
lrobb005:$y$j9T$WOPW7bTBh0.nBt/JV7j6A0$YMfBpzIr5oeNevD5KRvUH/W6rXfYjqywg7CJm  
YmZy.:20358:0:99999:7:::  
  
(lydia-robb@kali)-[~]  
└─$
```

Step 7-8: sudo usermod -aG sudo lrobb005
su - lrobb005

```
lrobb005@kali: ~  
File Actions Edit View Help  
  
(lydia-robb@kali)-[~]  
└─$ ls -ld /home/lrobb005  
drwx----- 5 lrobb005 lrobb005 4096 Sep 27 13:27 /home/lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ sudo passwd lrobb005  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(lydia-robb@kali)-[~]  
└─$ grep "^lrobb005:" /etc/passwd  
lrobb005:x:1001:1001::/home/lrobb005:/bin/bash  
  
(lydia-robb@kali)-[~]  
└─$ sudo grep "^lrobb005:" /etc/shadow  
lrobb005:$y$j9T$WOPW7bTBh0.nBt/JV7j6A0$YmfBpzIr5oeNevD5KRvUH/W6rXfYjqywg7CJm  
YmZy.:20358:0:99999:7:::  
  
(lydia-robb@kali)-[~]  
└─$ sudo usermod -aG sudo lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ su - lrobb005  
Password:  
(lrobb005@kali)-[~]  
└─$ █
```

Task B

Step 1-3: cd ~

```
echo "$SHELL"
```

```
id
```

```
groups root
```

```
lrobb005@kali: ~  
File Actions Edit View Help  
└─(lydia-robb@kali)-[~]  
└─$ sudo grep "^lrobb005:" /etc/shadow  
lrobb005:$y$j9T$WOPW7bTBh0.nBt/JV7j6A0$YMfBpzIr5oeNevD5KRvUH/W6rXfYjqywg7CJm  
YmZy.:20358:0:99999:7:::  
  
└─(lydia-robb@kali)-[~]  
└─$ sudo usermod -aG sudo lrobb005  
  
└─(lydia-robb@kali)-[~]  
└─$ su - lrobb005  
Password:  
└─(lrobb005@kali)-[~]  
└─$ cd ~  
  
└─(lrobb005@kali)-[~]  
└─$ echo "$SHELL"  
/bin/bash  
  
└─(lrobb005@kali)-[~]  
└─$ groups root  
root : root  
  
└─(lrobb005@kali)-[~]  
└─$ id  
uid=1001(lrobb005) gid=1001(lrobb005) groups=1001(lrobb005),27(sudo)  
  
└─(lrobb005@kali)-[~]  
└─$ █
```

Step 4: ls -l /etc/group

```
lrobb005@kali: ~  
File Actions Edit View Help  
  
(lydia-robb@kali)-[~]  
└─$ sudo usermod -aG sudo lrobb005  
  
(lydia-robb@kali)-[~]  
└─$ su - lrobb005  
Password:  
(lrobb005@kali)-[~]  
└─$ cd ~  
  
(lrobb005@kali)-[~]  
└─$ echo "$SHELL"  
/bin/bash  
  
(lrobb005@kali)-[~]  
└─$ groups root  
root : root  
  
(lrobb005@kali)-[~]  
└─$ id  
uid=1001(lrobb005) gid=1001(lrobb005) groups=1001(lrobb005),27(sudo)  
  
(lrobb005@kali)-[~]  
└─$ ls -l /etc/group  
-rw-r--r-- 1 root root 1406 Sep 27 13:39 /etc/group  
  
(lrobb005@kali)-[~]  
└─$ █
```

Step 5: sudo groupadd -g 01192240 test

```
lrobb005@kali: ~  
File Actions Edit View Help  
└─$ cd ~  
  
└─(lrobb005@kali)-[~]  
└─$ echo "$SHELL"  
/bin/bash  
  
└─(lrobb005@kali)-[~]  
└─$ groups root  
root : root  
  
└─(lrobb005@kali)-[~]  
└─$ id  
uid=1001(lrobb005) gid=1001(lrobb005) groups=1001(lrobb005),27(sudo)  
  
└─(lrobb005@kali)-[~]  
└─$ ls -l /etc/group  
-rw-r--r-- 1 root root 1406 Sep 27 13:39 /etc/group  
  
└─(lrobb005@kali)-[~]  
└─$ sudo groupadd -g 12345678 test  
[sudo] password for lrobb005:  
  
└─(lrobb005@kali)-[~]  
└─$ sudo groupadd -g 001192240 test  
groupadd: group 'test' already exists  
  
└─(lrobb005@kali)-[~]  
└─$ █
```

Step 6-8: `grep "^test:" /etc/group`

```
sudo groupmod -n newtest test  
sudo usermod -aG newtest lrobb005
```

- I accidentally forgot to replace “12345678” with my UIN

```
lrobb005@kali: ~  
File Actions Edit View Help  
lrobb005@kali)-[~]  
└─$ id  
uid=1001(lrobb005) gid=1001(lrobb005) groups=1001(lrobb005),27(sudo)  
  
lrobb005@kali)-[~]  
└─$ ls -l /etc/group  
-rw-r--r-- 1 root root 1406 Sep 27 13:39 /etc/group  
  
lrobb005@kali)-[~]  
└─$ sudo groupadd -g 12345678 test  
[sudo] password for lrobb005:  
  
lrobb005@kali)-[~]  
└─$ sudo groupadd -g 001192240 test  
groupadd: group 'test' already exists  
  
lrobb005@kali)-[~]  
└─$ grep "^test:" /etc/group  
test:x:12345678:  
  
lrobb005@kali)-[~]  
└─$ sudo groupmod -n newtest test  
  
lrobb005@kali)-[~]  
└─$ sudo usermod -aG newtest lrobb005  
  
lrobb005@kali)-[~]  
└─$ █
```

Step 9-11: touch ~/testfile
sudo chgrp newtest ~/testfile
ls -l ~/testfile
sudo groupdel newtest
ls -l ~/testfile

- I can now see the numeric GID instead of the group name because the name was removed but the GID remains on the file

```
lrobb005@kali: ~  
File Actions Edit View Help  
└─$ grep "^test:" /etc/group  
test:x:12345678:  
  
└─(lrobb005@kali)-[~]  
└─$ sudo groupmod -n newtest test  
  
└─(lrobb005@kali)-[~]  
└─$ sudo usermod -aG newtest lrobb005  
  
└─(lrobb005@kali)-[~]  
└─$ touch ~/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ sudo chgrp newtest ~/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ ls -l ~/testfile  
-rw-rw-r-- 1 lrobb005 newtest 0 Sep 27 13:56 /home/lrobb005/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ sudo groupdel newtest  
  
└─(lrobb005@kali)-[~]  
└─$ ls -l ~/testfile  
-rw-rw-r-- 1 lrobb005 12345678 0 Sep 27 13:56 /home/lrobb005/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ █
```

Step 12: exit

sudo userdel -r lrobb005

```
lydia-robb@kali: ~  
File Actions Edit View Help  
└─$ sudo chgrp newtest ~/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ ls -l ~/testfile  
-rw-rw-r-- 1 lrobb005 newtest 0 Sep 27 13:56 /home/lrobb005/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ sudo groupdel newtest  
  
└─(lrobb005@kali)-[~]  
└─$ ls -l ~/testfile  
-rw-rw-r-- 1 lrobb005 12345678 0 Sep 27 13:56 /home/lrobb005/testfile  
  
└─(lrobb005@kali)-[~]  
└─$ sudo userdel -r lrobb005  
userdel: user lrobb005 is currently used by process 50999  
  
└─(lrobb005@kali)-[~]  
└─$ exit  
logout  
  
└─(lydia-robb@kali)-[~]  
└─$ sudo userdel -r lrobb005  
[sudo] password for lydia-robb:  
userdel: lrobb005 mail spool (/var/mail/lrobb005) not found  
  
└─(lydia-robb@kali)-[~]  
└─$ █
```