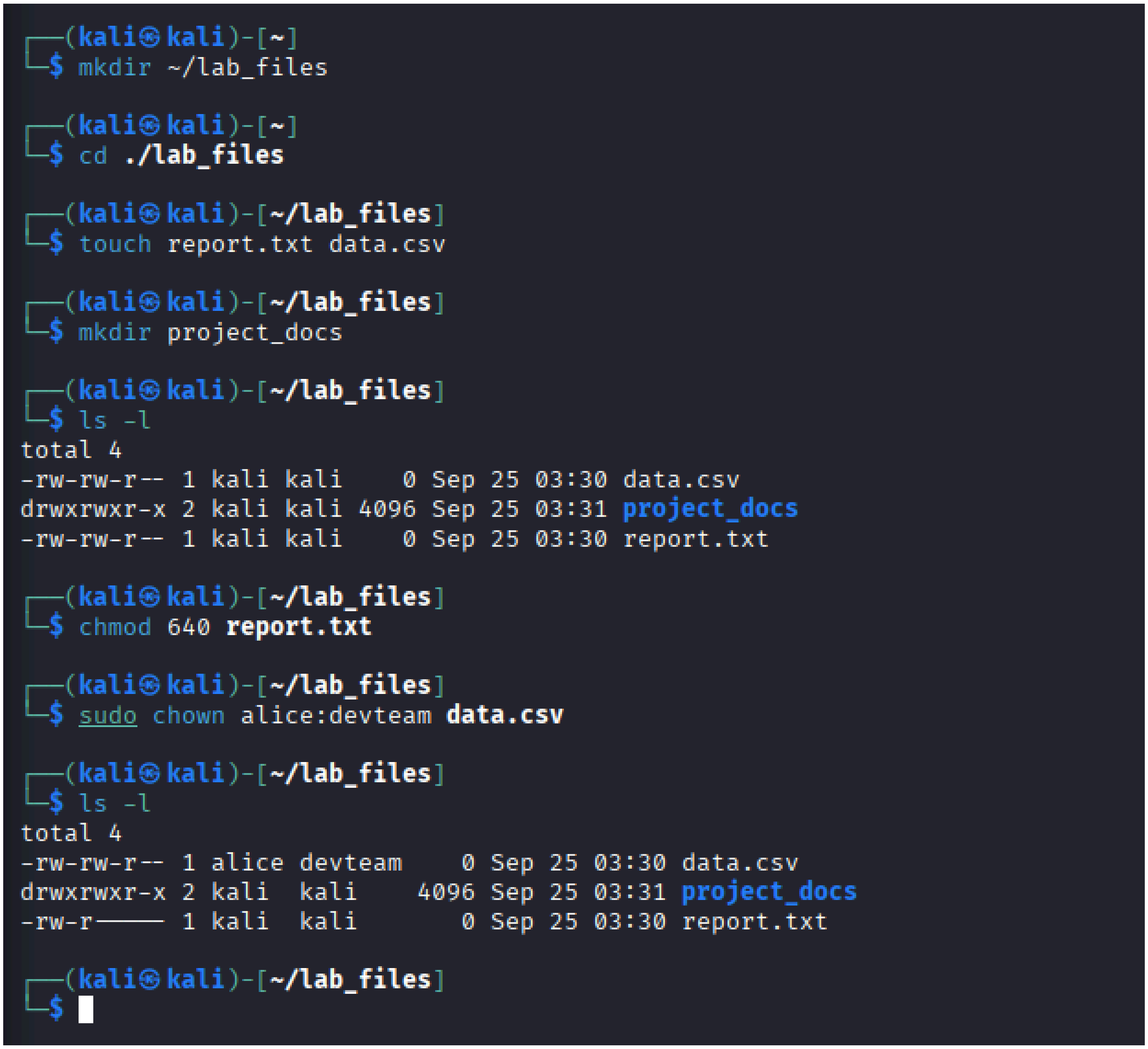
Task 1

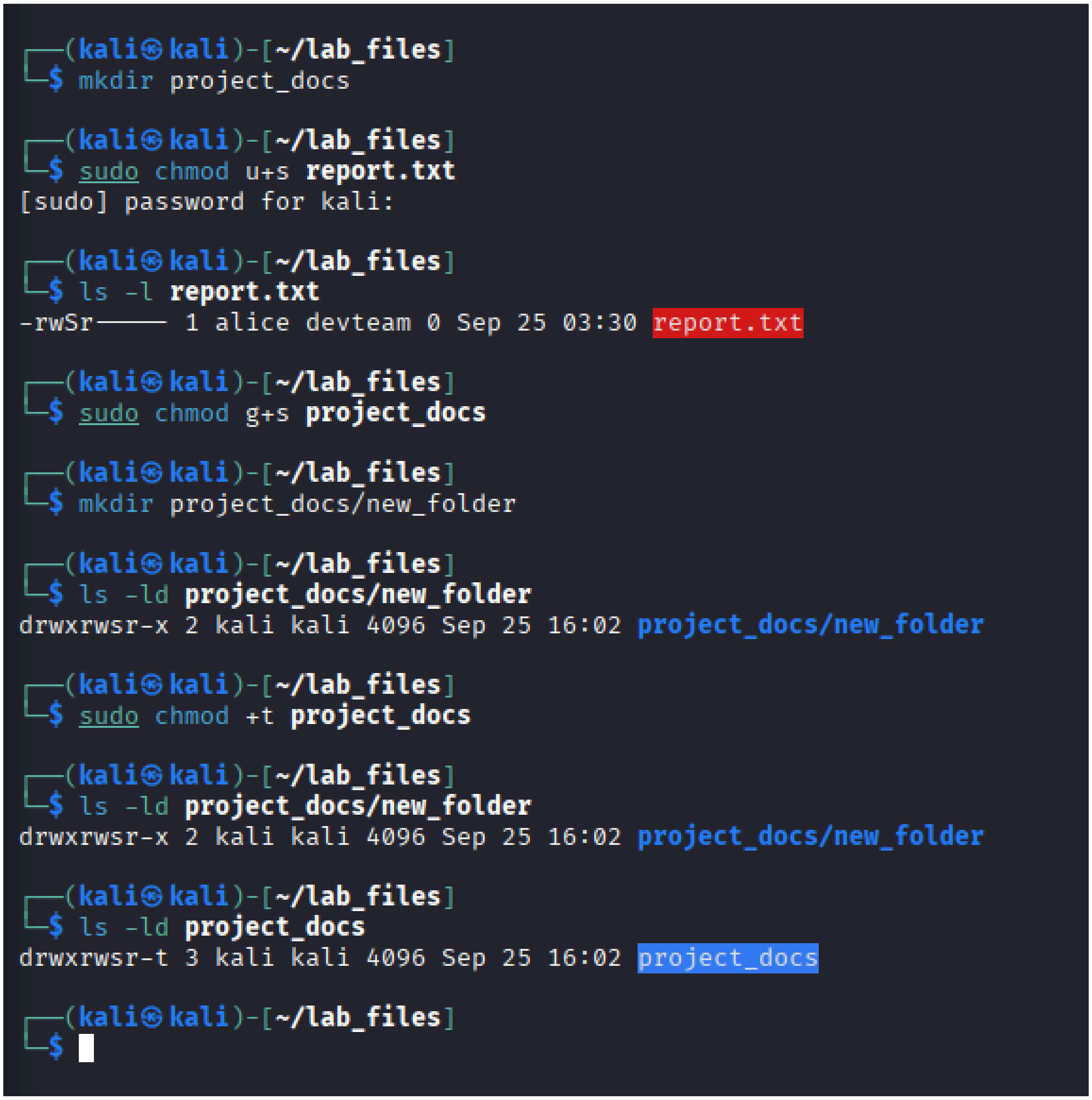
1. Password must be 16 characters long, including upper and lower case, multiple numbers and special characters (minimum of 5)
2. Files and directories must have its owner for managing permissions
3. Follow the principle of least privilege, only allowing the minimal permissions for designated users or groups
4. System monitoring tools like logging should always be available for the system administrator only

Task 2



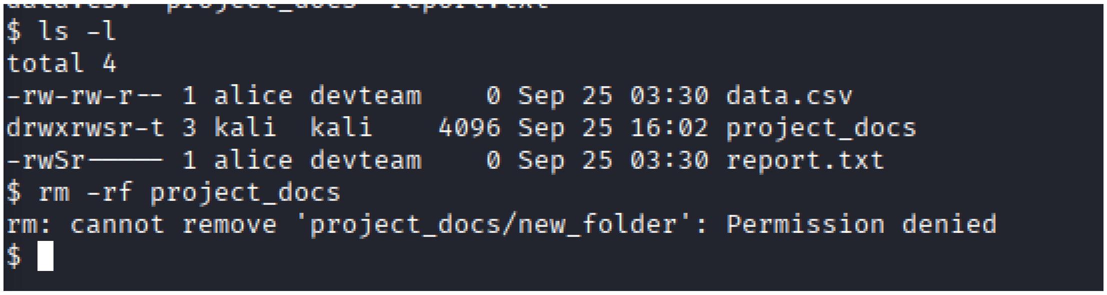
```
┌──(kali㉿kali)-[~]
└─$ mkdir ~/lab_files

┌──(kali㉿kali)-[~]
└─$ cd ./lab_files

┌──(kali㉿kali)-[~/lab_files]
└─$ touch report.txt data.csv

┌──(kali㉿kali)-[~/lab_files]
└─$ mkdir project_docs

┌──(kali㉿kali)-[~/lab_files]
└─$ ls -l
total 4
-rw-rw-r-- 1 kali kali    0 Sep 25 03:30 data.csv
drwxrwxr-x 2 kali kali 4096 Sep 25 03:31 project_docs
-rw-rw-r-- 1 kali kali    0 Sep 25 03:30 report.txt

┌──(kali㉿kali)-[~/lab_files]
└─$ chmod 640 report.txt

┌──(kali㉿kali)-[~/lab_files]
└─$ sudo chown alice:devteam data.csv

┌──(kali㉿kali)-[~/lab_files]
└─$ ls -l
total 4
-rw-rw-r-- 1 alice devteam    0 Sep 25 03:30 data.csv
drwxrwxr-x 2 kali  kali    4096 Sep 25 03:31 project_docs
-rw-r----- 1 kali  kali       0 Sep 25 03:30 report.txt

┌──(kali㉿kali)-[~/lab_files]
└─$ 
```

Task 3



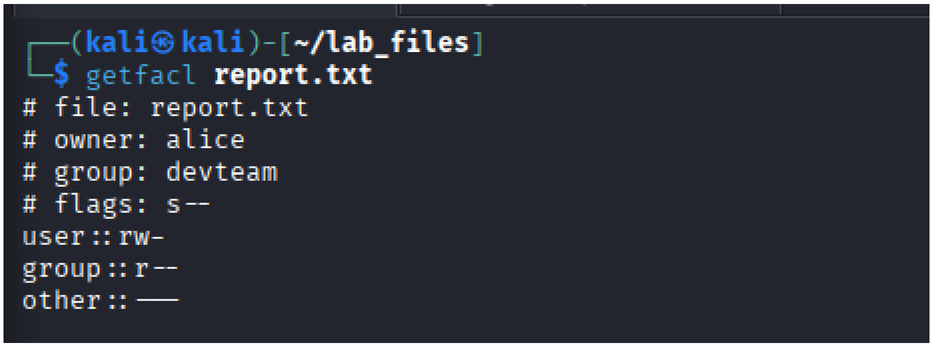
```
┌──(kali㉿kali)-[~/lab_files]
└─$ mkdir project_docs

┌──(kali㉿kali)-[~/lab_files]
└─$ sudo chmod u+s report.txt
[sudo] password for kali:

┌──(kali㉿kali)-[~/lab_files]
└─$ ls -l report.txt
-rwSr----- 1 alice devteam 0 Sep 25 03:30 report.txt

┌──(kali㉿kali)-[~/lab_files]
└─$ sudo chmod g+s project_docs

┌──(kali㉿kali)-[~/lab_files]
└─$ mkdir project_docs/new_folder

┌──(kali㉿kali)-[~/lab_files]
└─$ ls -ld project_docs/new_folder
drwxrwsr-x 2 kali kali 4096 Sep 25 16:02 project_docs/new_folder

┌──(kali㉿kali)-[~/lab_files]
└─$ sudo chmod +t project_docs

┌──(kali㉿kali)-[~/lab_files]
└─$ ls -ld project_docs/new_folder
drwxrwsr-x 2 kali kali 4096 Sep 25 16:02 project_docs/new_folder

┌──(kali㉿kali)-[~/lab_files]
└─$ ls -ld project_docs
drwxrwsr-t 3 kali kali 4096 Sep 25 16:02 project_docs

┌──(kali㉿kali)-[~/lab_files]
└─$ 
```

From Alice's account:

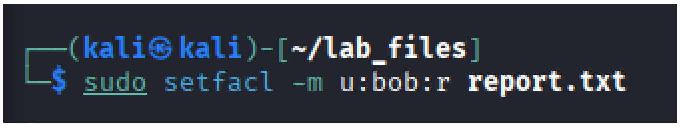


```
data.csv  project_docs  report.txt
$ ls -l
total 4
-rw-rw-r-- 1 alice devteam    0 Sep 25 03:30 data.csv
drwxrwsr-t 3 kali  kali    4096 Sep 25 16:02 project_docs
-rwSr----- 1 alice devteam    0 Sep 25 03:30 report.txt
$ rm -rf project_docs
rm: cannot remove 'project_docs/new_folder': Permission denied
$ 
```

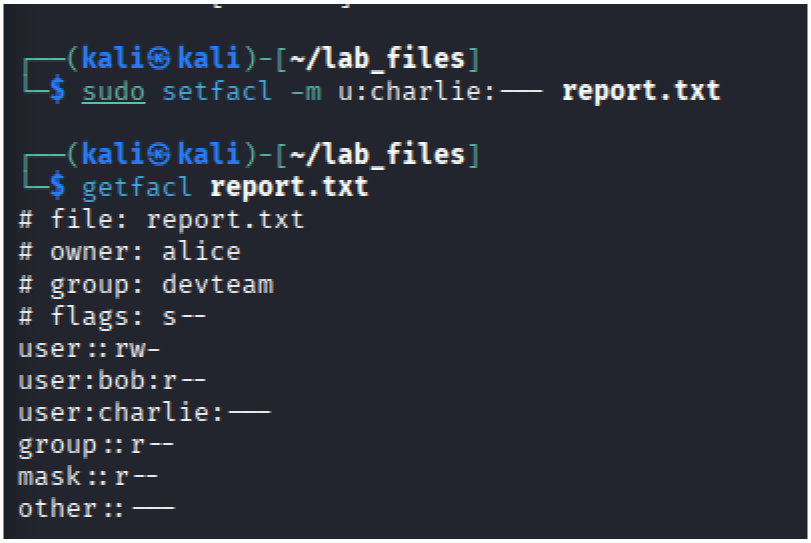
Task 4



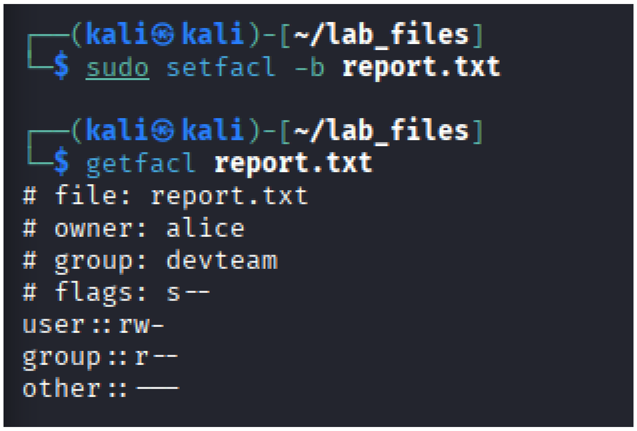
```
┌──(kali㉿kali)-[~/lab_files]
└─$ getfacl report.txt
# file: report.txt
# owner: alice
# group: devteam
# flags: s--
user::rw-
group::r--
other::---
```



```
┌──(kali㉿kali)-[~/lab_files]
└─$ sudo setfacl -m u:bob:r report.txt
```

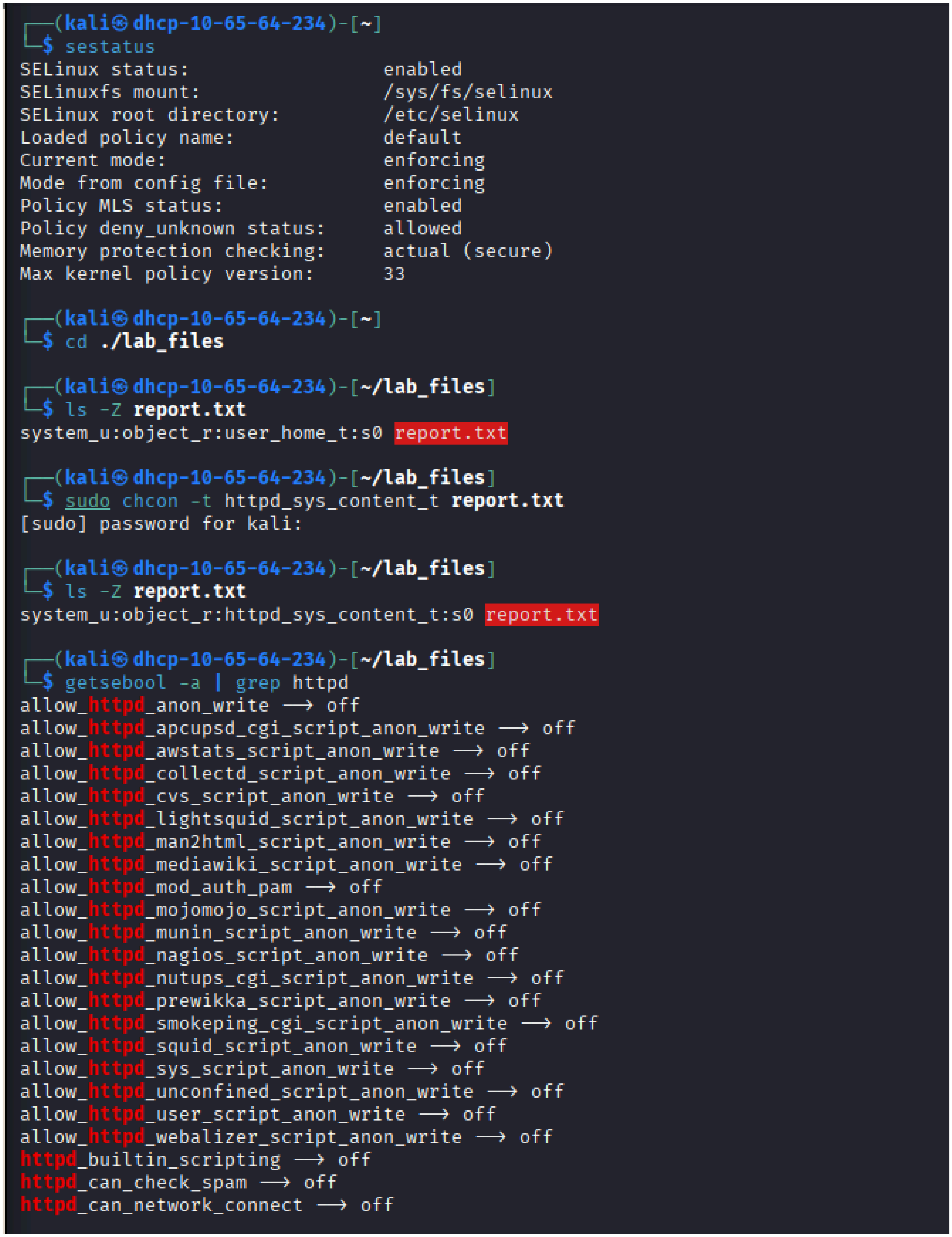


```
┌──(kali㉿kali)-[~/lab_files]
└─$ sudo setfacl -m u:charlie:--- report.txt

┌──(kali㉿kali)-[~/lab_files]
└─$ getfacl report.txt
# file: report.txt
# owner: alice
# group: devteam
# flags: s--
user::rw-
user:bob:r--
user:charlie:---
group::r--
mask::r--
other::---
```

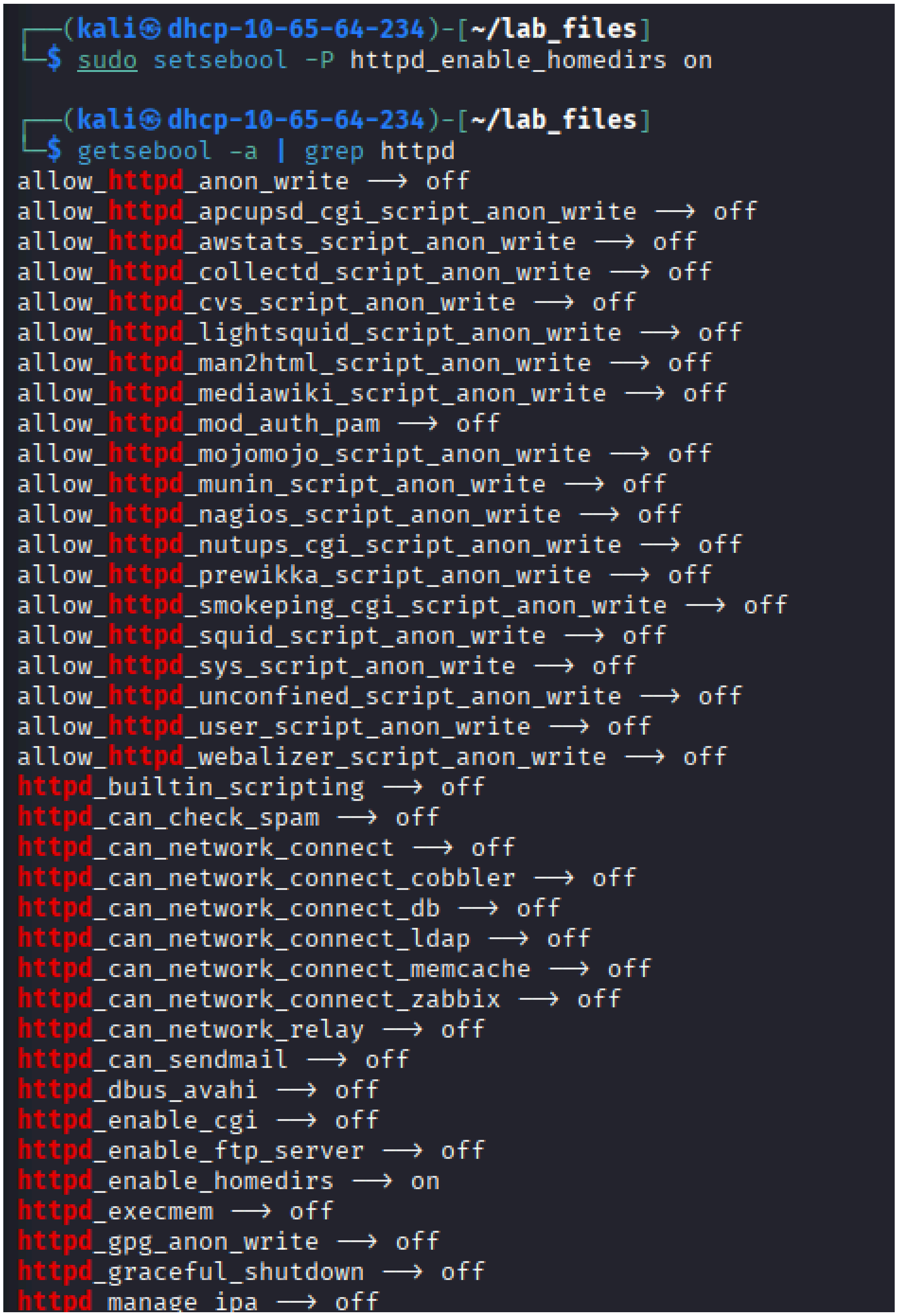


```
┌──(kali㉿kali)-[~/lab_files]
└─$ sudo setfacl -b report.txt

┌──(kali㉿kali)-[~/lab_files]
└─$ getfacl report.txt
# file: report.txt
# owner: alice
# group: devteam
# flags: s--
user::rw-
group::r--
other::---
```

Task 5



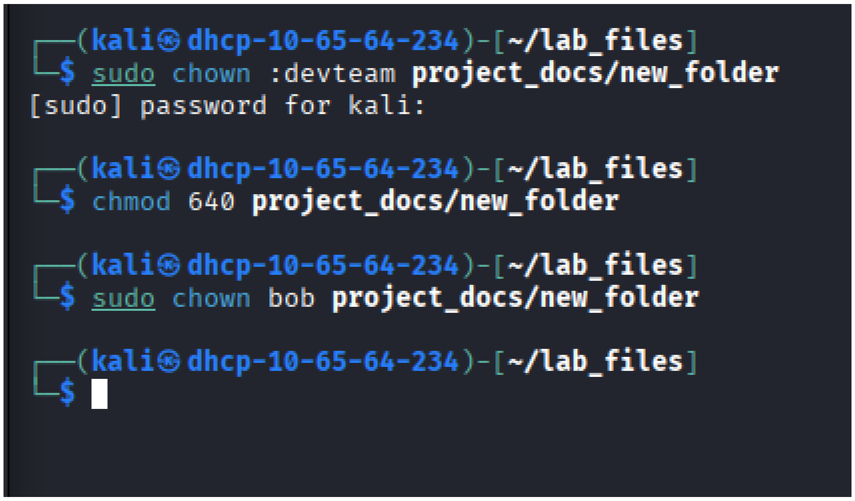
```
┌──(kali㉿dhcp-10-65-64-234)-[~]
└─$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

┌──(kali㉿dhcp-10-65-64-234)-[~]
└─$ cd ./lab_files

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ ls -Z report.txt
system_u:object_r:user_home_t:s0 report.txt

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ sudo chcon -t httpd_sys_content_t report.txt
[sudo] password for kali:

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ ls -Z report.txt
system_u:object_r:httpd_sys_content_t:s0 report.txt

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ getsebool -a | grep httpd
allow_httpd_anon_write ⟶ off
allow_httpd_apcupsd_cgi_script_anon_write ⟶ off
allow_httpd_awstats_script_anon_write ⟶ off
allow_httpd_collectd_script_anon_write ⟶ off
allow_httpd_cvs_script_anon_write ⟶ off
allow_httpd_lightsquid_script_anon_write ⟶ off
allow_httpd_man2html_script_anon_write ⟶ off
allow_httpd_mediawiki_script_anon_write ⟶ off
allow_httpd_mod_auth_pam ⟶ off
allow_httpd_mojomojo_script_anon_write ⟶ off
allow_httpd_munin_script_anon_write ⟶ off
allow_httpd_nagios_script_anon_write ⟶ off
allow_httpd_nutups_cgi_script_anon_write ⟶ off
allow_httpd_prewikka_script_anon_write ⟶ off
allow_httpd_smokeping_cgi_script_anon_write ⟶ off
allow_httpd_squid_script_anon_write ⟶ off
allow_httpd_sys_script_anon_write ⟶ off
allow_httpd_unconfined_script_anon_write ⟶ off
allow_httpd_user_script_anon_write ⟶ off
allow_httpd_webalizer_script_anon_write ⟶ off
httpd_builtin_scripting ⟶ off
httpd_can_check_spam ⟶ off
httpd_can_network_connect ⟶ off
```



```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ sudo setsebool -P httpd_enable_homedirs on

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ getsebool -a | grep httpd
allow_httpd_anon_write --> off
allow_httpd_apcupsd_cgi_script_anon_write --> off
allow_httpd_awstats_script_anon_write --> off
allow_httpd_collectd_script_anon_write --> off
allow_httpd_cvs_script_anon_write --> off
allow_httpd_lightsquid_script_anon_write --> off
allow_httpd_man2html_script_anon_write --> off
allow_httpd_mediawiki_script_anon_write --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_mojomojo_script_anon_write --> off
allow_httpd_munin_script_anon_write --> off
allow_httpd_nagios_script_anon_write --> off
allow_httpd_nutups_cgi_script_anon_write --> off
allow_httpd_prewikka_script_anon_write --> off
allow_httpd_smokeping_cgi_script_anon_write --> off
allow_httpd_squid_script_anon_write --> off
allow_httpd_sys_script_anon_write --> off
allow_httpd_unconfined_script_anon_write --> off
allow_httpd_user_script_anon_write --> off
allow_httpd_webalizer_script_anon_write --> off
httpd_builtin_scripting --> off
httpd_can_check_spam --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_connect_ldap --> off
httpd_can_network_connect_memcache --> off
httpd_can_network_connect_zabbix --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> off
httpd_enable_cgi --> off
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> on
httpd_execmem --> off
httpd_gpg_anon_write --> off
httpd_graceful_shutdown --> off
httpd_manage_ipa --> off
```

Task 6

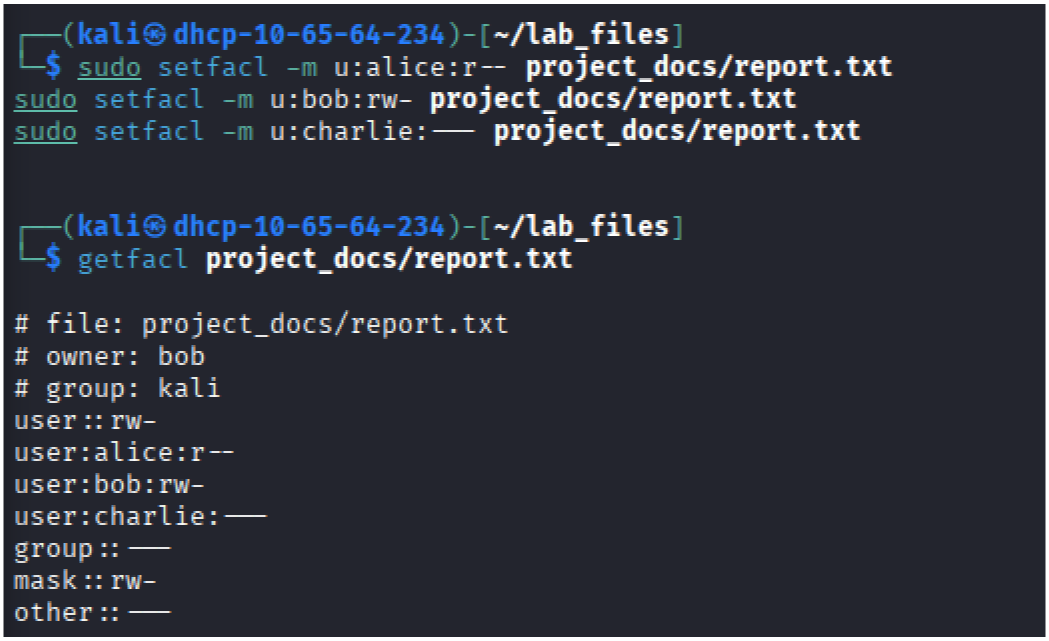
Standard permission



```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ sudo chown :devteam project_docs/new_folder
[sudo] password for kali:

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ chmod 640 project_docs/new_folder

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ sudo chown bob project_docs/new_folder

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ █
```

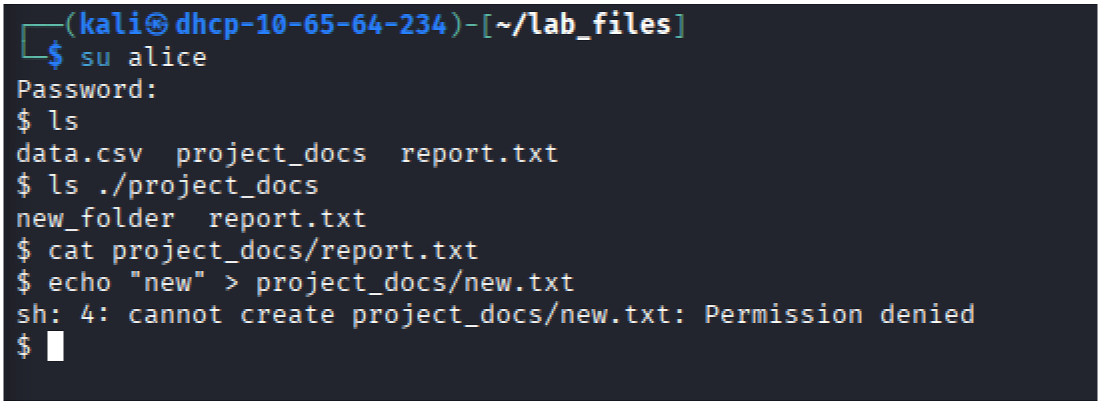
Change permission to 640, read write for owner, read for group, change bob to the owner and chown devteam to the folder.

ACL



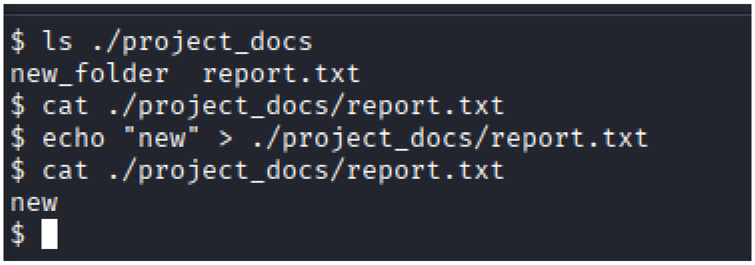
```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ sudo setfacl -m u:alice:r-- project_docs/report.txt
sudo setfacl -m u:bob:rw- project_docs/report.txt
sudo setfacl -m u:charlie:--- project_docs/report.txt


┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ getfacl project_docs/report.txt

# file: project_docs/report.txt
# owner: bob
# group: kali
user::rw-
user:alice:r--
user:bob:rw-
user:charlie:---
group::---
mask::rw-
other::---
```

Alice



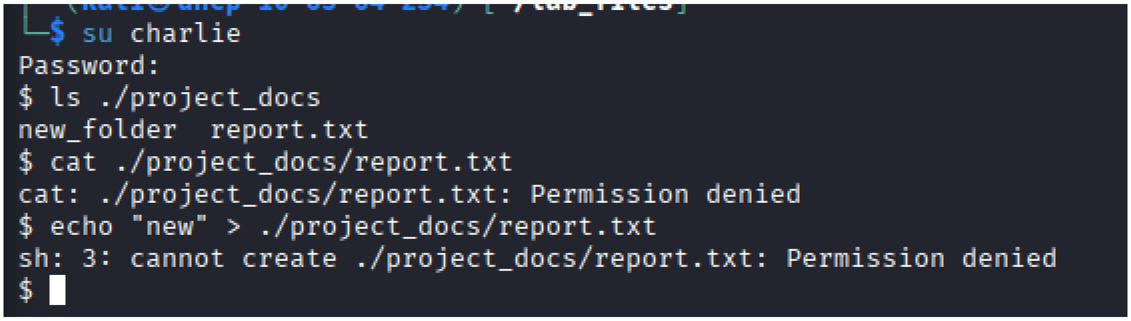
```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ su alice
Password:
$ ls
data.csv  project_docs  report.txt
$ ls ./project_docs
new_folder  report.txt
$ cat project_docs/report.txt
$ echo "new" > project_docs/new.txt
sh: 4: cannot create project_docs/new.txt: Permission denied
$ 
```

Bob



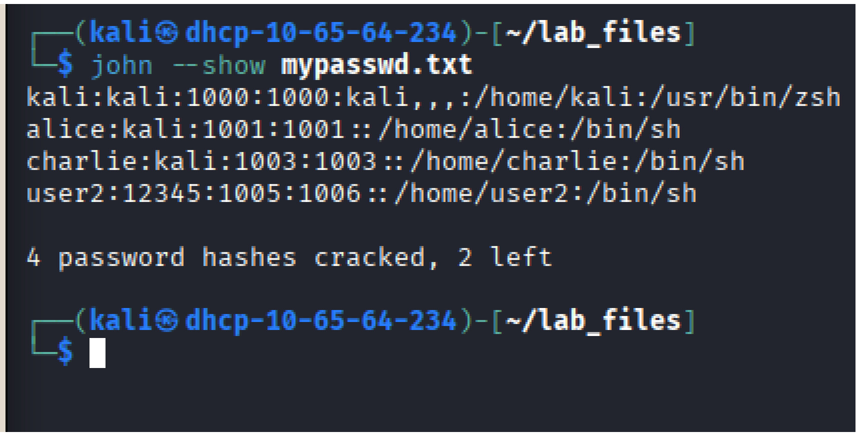
```
$ ls ./project_docs
new_folder  report.txt
$ cat ./project_docs/report.txt
$ echo "new" > ./project_docs/report.txt
$ cat ./project_docs/report.txt
new
$ 
```

Charlie

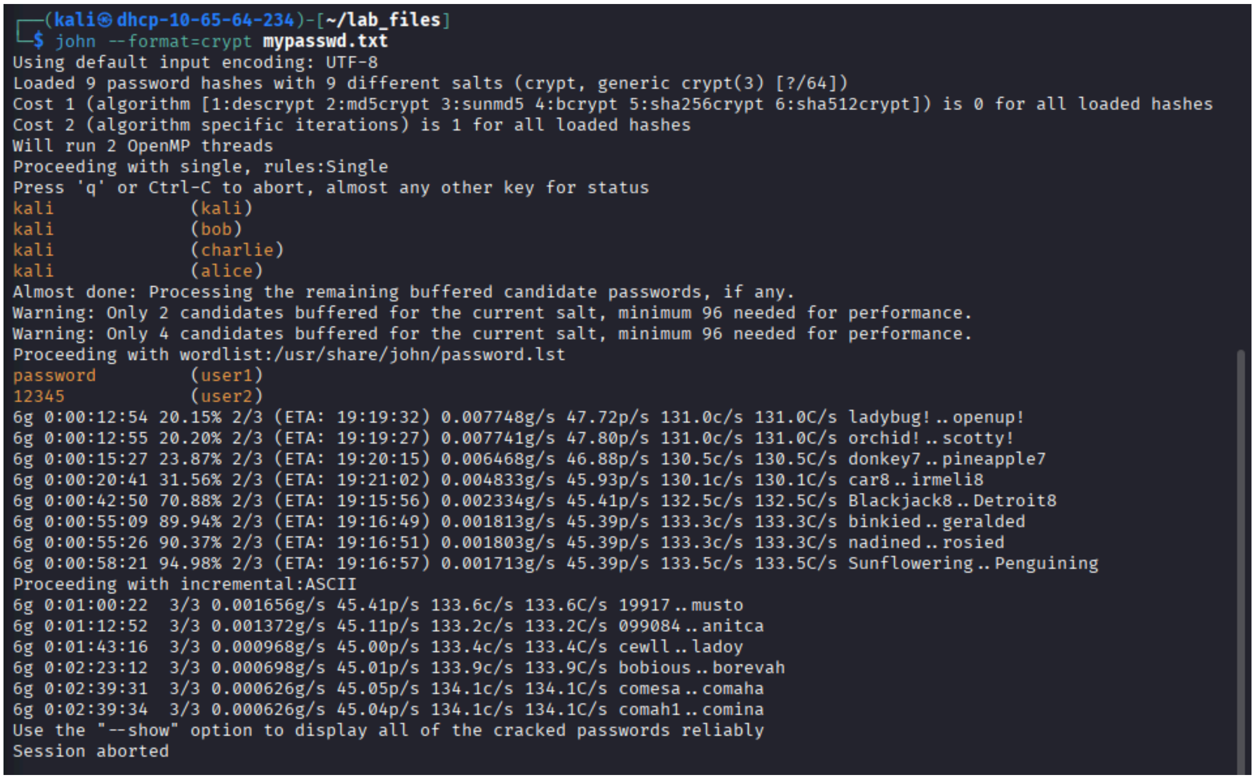


```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ su charlie
Password:
$ ls ./project_docs
new_folder  report.txt
$ cat ./project_docs/report.txt
cat: ./project_docs/report.txt: Permission denied
$ echo "new" > ./project_docs/report.txt
sh: 3: cannot create ./project_docs/report.txt: Permission denied
$ 
```

Task 7

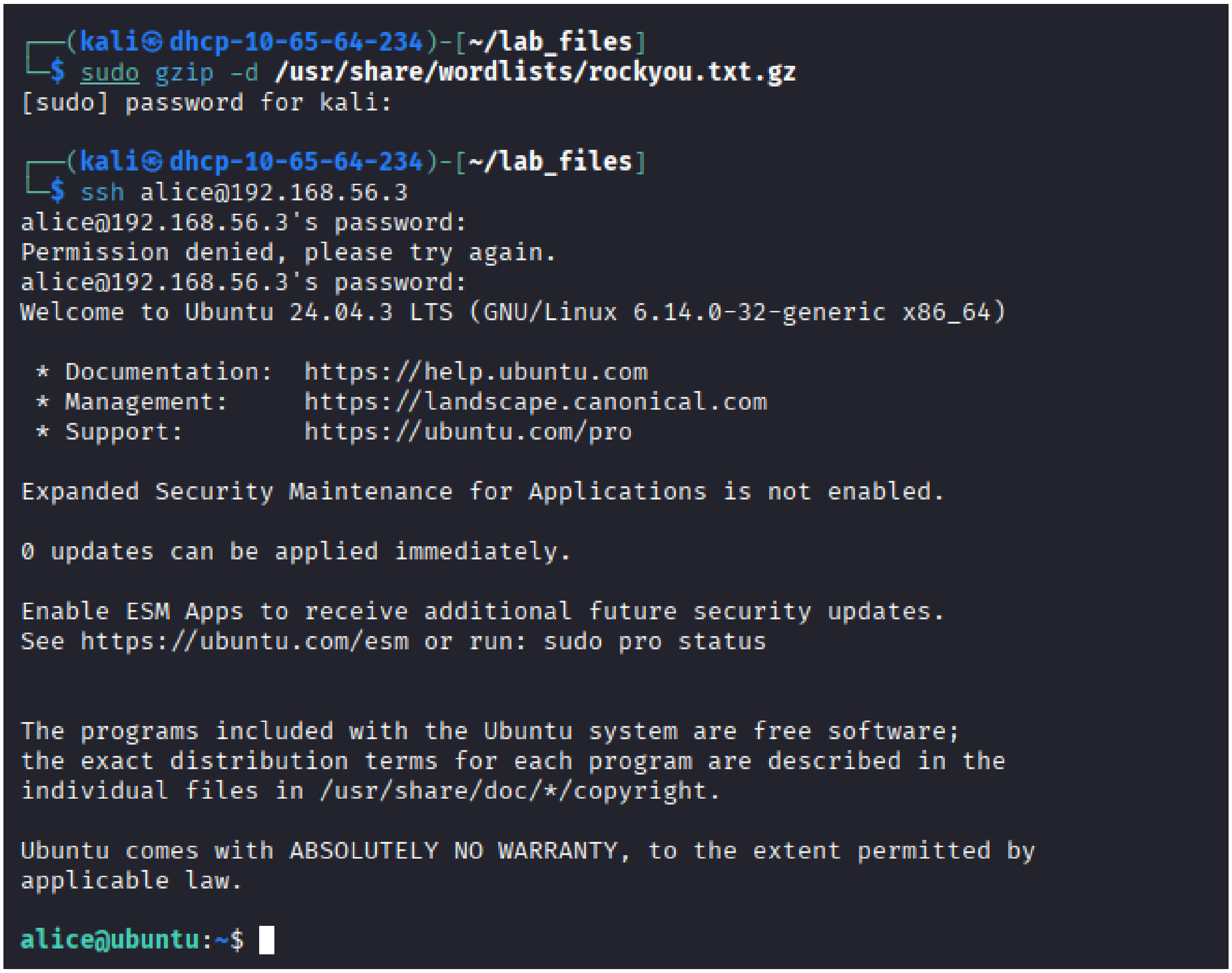


```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ john --show mypasswd.txt
kali:kali:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
alice:kali:1001:1001::/home/alice:/bin/sh
charlie:kali:1003:1003::/home/charlie:/bin/sh
user2:12345:1005:1006::/home/user2:/bin/sh

4 password hashes cracked, 2 left

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ 
```

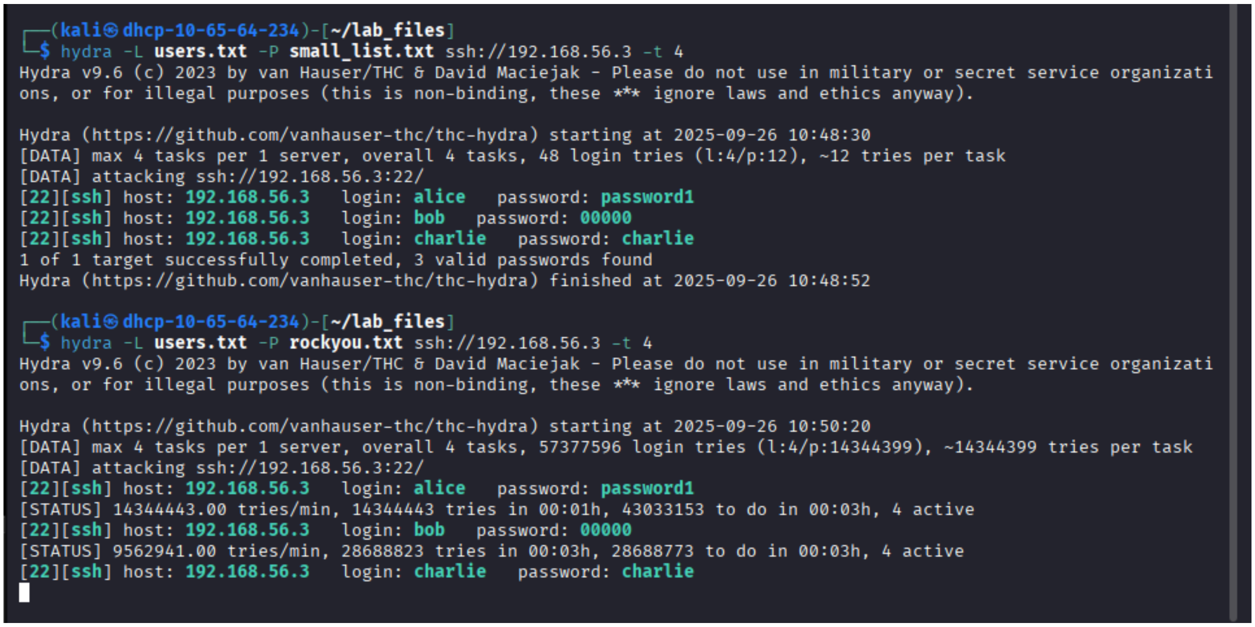


```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ john --format=crypt mypasswd.txt
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali             (kali)
kali             (bob)
kali             (charlie)
kali             (alice)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 2 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
password         (user1)
12345            (user2)
6g 0:00:12:54 20.15% 2/3 (ETA: 19:19:32) 0.007748g/s 47.72p/s 131.0c/s 131.0C/s ladybug!..openup!
6g 0:00:12:55 20.20% 2/3 (ETA: 19:19:27) 0.007741g/s 47.80p/s 131.0c/s 131.0C/s orchid!..scotty!
6g 0:00:15:27 23.87% 2/3 (ETA: 19:20:15) 0.006468g/s 46.88p/s 130.5c/s 130.5C/s donkey7..pineapple7
6g 0:00:20:41 31.56% 2/3 (ETA: 19:21:02) 0.004833g/s 45.93p/s 130.1c/s 130.1C/s car8..irmeli8
6g 0:00:42:50 70.88% 2/3 (ETA: 19:15:56) 0.002334g/s 45.41p/s 132.5c/s 132.5C/s Blackjack8..Detroit8
6g 0:00:55:09 89.94% 2/3 (ETA: 19:16:49) 0.001813g/s 45.39p/s 133.3c/s 133.3C/s binkied..geralded
6g 0:00:55:26 90.37% 2/3 (ETA: 19:16:51) 0.001803g/s 45.39p/s 133.3c/s 133.3C/s nadined..rosied
6g 0:00:58:21 94.98% 2/3 (ETA: 19:16:57) 0.001713g/s 45.39p/s 133.5c/s 133.5C/s Sunflowering..Penguining
Proceeding with incremental:ASCII
6g 0:01:00:22  3/3 0.001656g/s 45.41p/s 133.6c/s 133.6C/s 19917..musto
6g 0:01:12:52  3/3 0.001372g/s 45.11p/s 133.2c/s 133.2C/s 099084..anitca
6g 0:01:43:16  3/3 0.000968g/s 45.00p/s 133.4c/s 133.4C/s cewll..ladoy
6g 0:02:23:12  3/3 0.000698g/s 45.01p/s 133.9c/s 133.9C/s bobious..borevah
6g 0:02:39:31  3/3 0.000626g/s 45.05p/s 134.1c/s 134.1C/s comesa..comaha
6g 0:02:39:34  3/3 0.000626g/s 45.04p/s 134.1c/s 134.1C/s comah1..comina
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Task 8



```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ ssh alice@192.168.56.3
alice@192.168.56.3's password:
Permission denied, please try again.
alice@192.168.56.3's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

alice@ubuntu:~$ █
```



```
┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ hydra -L users.txt -P small_list.txt ssh://192.168.56.3 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-26 10:48:30
[DATA] max 4 tasks per 1 server, overall 4 tasks, 48 login tries (l:4/p:12), ~12 tries per task
[DATA] attacking ssh://192.168.56.3:22/
[22][ssh] host: 192.168.56.3   login: alice   password: password1
[22][ssh] host: 192.168.56.3   login: bob   password: 00000
[22][ssh] host: 192.168.56.3   login: charlie   password: charlie
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-26 10:48:52

┌──(kali㉿dhcp-10-65-64-234)-[~/lab_files]
└─$ hydra -L users.txt -P rockyou.txt ssh://192.168.56.3 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-26 10:50:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 57377596 login tries (l:4/p:14344399), ~14344399 tries per task
[DATA] attacking ssh://192.168.56.3:22/
[22][ssh] host: 192.168.56.3   login: alice   password: password1
[STATUS] 14344443.00 tries/min, 14344443 tries in 00:01h, 43033153 to do in 00:03h, 4 active
[22][ssh] host: 192.168.56.3   login: bob   password: 00000
[STATUS] 9562941.00 tries/min, 28688823 tries in 00:03h, 28688773 to do in 00:03h, 4 active
[22][ssh] host: 192.168.56.3   login: charlie   password: charlie
█
```

All accounts are successfully cracked; it took less than 10 minutes with rockyou.txt. Using my own small wordlist would be faster, as I am testing it with the knowledge of knowing the password and putting it in. But in trades of in real world scenario it would mean less accurate and will miss more valid common passwords, using rockyou.txt is more suitable as it is brute forcing with large dictionary list.

1. Victim IP: 192.168.56.3
2. Username Tested: alice, bob, charlie
3. Password list used: rockyou.txt and my small wordlist
4. Accounts cracked: all of them
5. Observations/Notes: Weak passwords are common in dictionary attacks, which are more vulnerable and easier to crack.