

Step 1:

- Creating 6 users and passwords

```
(jessica@kali)-[~]
└─$ sudo passwd John
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo useradd John2
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo passwd John2
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo useradd John3
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo passwd John3
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo useradd John4
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo passwd John4
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo useradd John5
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo passwd John5
New password:
Retype new password:
passwd: password updated successfully
```

```
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo useradd John6
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$ sudo passwd John6
New password:
Retype new password:
passwd: password updated successfully

(jessica@kali)-[~]
└─$
```

Step 2:

- Locate the rockyou.txt file
- Use the “pwd” command to print the current working directory
- Copy the file to the current directory
- use the long listing command

```
(jessica@kali)-[~]
└─$ locate rockyou.txt.gz
/usr/share/wordlists/rockyou.txt.gz

(jessica@kali)-[~]
└─$ pwd
/home/jessica

(jessica@kali)-[~]
└─$ sudo cp /usr/share/wordlists/rockyou.txt.gz /home/jessica/

(jessica@kali)-[~]
└─$ ls -l
total 188840
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 270
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 CYSE
drwxr-xr-x 7 jessica jessica 4096 Oct  7 15:50 Desktop
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Downloads
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Downloads
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Music
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Pictures
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Public
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Templates
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Videos
-rw-r--r-- 1 jessica jessica 5578 Sep 22 15:05 copyright
-rw-r--r-- 1 jessica jessica 5578 Sep 20 21:01 copyright_cyse270
drwxrwxr-x 2 jessica jessica 4096 Sep  9 18:57 data
-rw-rw-r-- 1 jessica games 0 Sep 23 15:31 demo.txt
-rw-rw-r-- 1 jessica jessica 51 Sep  9 15:37 error_log.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:25 jfrim001.hash.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:56 jfrim001hash.txt
-rw-r-- 1 jessica jessica 2 Sep 16 15:13 nano.1456847.save
-rw-rw-r-- 1 jessica jessica 46 Sep 18 11:38 practice.txt
-rw-r--r-- 1 jessica jessica 139921507 Oct  7 11:55 rockyou.txt
-rw-r--r-- 1 root root 53357329 Oct 11 17:13 rockyou.txt.gz
-rw-r-- 1 root root 2354 Oct  7 11:56 shadow
-rw-rw-r-- 1 jessica jessica 1760 Oct  2 15:51 test.txt
-rw-rw-r-- 1 jessica newtest 0 Oct  2 11:58 test2file.txt
```

Step 3:

- Gunzip the file
- Use the long listing command

```
(jessica@kali)-[~]
└─$ gunzip rockyou.txt.gz
gzip: rockyou.txt already exists; do you wish to overwrite (y or n)? y
(jessica@kali)-[~]
└─$ ls -l
total 136732
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 270
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 CYSE
drwxr-xr-x 7 jessica jessica 4096 Oct  7 15:50 Desktop
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Documents
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Downloads
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Music
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Pictures
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Public
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Templates
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Videos
-rw-r--r-- 1 jessica jessica 5578 Sep 22 15:05 copyright
-rw-r--r-- 1 jessica jessica 5578 Sep 20 21:01 copyright_cyse270
drwxrwxr-x 2 jessica jessica 4096 Sep  9 18:57 data
-rw-rw-r-- 1 jessica games 0 Sep 23 15:31 demo.txt
-rw-rw-r-- 1 jessica jessica 51 Sep  9 15:37 error_log.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:25 jfrim001.hash.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:56 jfrim001hash.txt
-rw-r--r-- 1 jessica jessica 2 Sep 16 15:13 nano.1456847.save
-rw-rw-r-- 1 jessica jessica 46 Sep 18 11:38 practice.txt
-rw-r--r-- 1 jessica jessica 139921507 Oct 11 17:13 rockyou.txt
-rw-r--r-- 1 root root 2354 Oct  7 11:56 shadow
-rw-rw-r-- 1 jessica jessica 1760 Oct  2 15:51 test.txt
-rw-rw-r-- 1 jessica newtest 0 Oct  2 11:58 test2file.txt
```

Step 4:

- Use the “cat” command to see 10 lines from the file
- Copy shadow to the current directory
- Then use the long listing command to print.

```
(jessica@kali)-[~]
└─$ cat rockyou.txt | head -10
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
(jessica@kali)-[~]
└─$ sudo cp /etc/shadow /home/jessica/
(jessica@kali)-[~]
└─$ ls -l
total 136732
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 270
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 CYSE
drwxr-xr-x 7 jessica jessica 4096 Oct  7 15:50 Desktop
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Documents
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Downloads
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Music
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Pictures
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Public
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Templates
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Videos
-rw-r--r-- 1 jessica jessica 5578 Sep 22 15:05 copyright
-rw-r--r-- 1 jessica jessica 5578 Sep 20 21:01 copyright_cyse270
drwxrwxr-x 2 jessica jessica 4096 Sep  9 18:57 data
-rw-rw-r-- 1 jessica games 0 Sep 23 15:31 demo.txt
-rw-rw-r-- 1 jessica jessica 51 Sep  9 15:37 error_log.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:25 jfrim001.hash.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:56 jfrim001hash.txt
-rw-r--r-- 1 jessica jessica 2 Sep 16 15:13 nano.1456847.save
-rw-rw-r-- 1 jessica jessica 46 Sep 18 11:38 practice.txt
-rw-r--r-- 1 jessica jessica 139921507 Oct 11 17:13 rockyou.txt
-rw-r--r-- 1 root root 2975 Oct 11 17:16 shadow
-rw-rw-r-- 1 jessica jessica 1760 Oct  2 15:51 test.txt
-rw-rw-r-- 1 jessica newtest 0 Oct  2 11:58 test2file.txt
```

Step 5:

- Save the shadow file content into the new file created
- Using the long listing command to verify the content is there.

```
(jessica@kali)-[~]
└─$ sudo cat shadow > jfrim001.hash.file

(jessica@kali)-[~]
└─$ ls -l
total 136736
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 270
drwxrwxr-x 2 jessica jessica 4096 Sep  4 15:48 CYSE
drwxr-xr-x 7 jessica jessica 4096 Oct  7 15:50 Desktop
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Documents
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Downloads
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Music
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Pictures
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Public
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Templates
drwxr-xr-x 2 jessica jessica 4096 Aug 26 17:33 Videos
-rw-r--r-- 1 jessica jessica 5578 Sep 22 15:05 copyright
-rw-r--r-- 1 jessica jessica 5578 Sep 20 21:01 copyright_cyse270
drwxrwxr-x 2 jessica jessica 4096 Sep  9 18:57 data
-rw-rw-r-- 1 jessica games 0 Sep 23 15:31 demo.txt
-rw-rw-r-- 1 jessica jessica 51 Sep  9 15:37 error_log.txt
-rw-rw-r-- 1 jessica jessica 2975 Oct 11 17:17 jfrim001.hash.file
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:25 jfrim001.hash.txt
-rw-rw-r-- 1 jessica jessica 2354 Oct  7 11:56 jfrim001hash.txt
-rw----- 1 jessica jessica 2 Sep 16 15:13 nano.1456847.save
-rw-rw-r-- 1 jessica jessica 46 Sep 18 11:38 practice.txt
-rw-r--r-- 1 jessica jessica 139921507 Oct 11 17:13 rockyou.txt
-rw-r----- 1 root root 2975 Oct 11 17:16 shadow
-rw-rw-r-- 1 jessica jessica 1760 Oct  2 15:51 test.txt
-rw-rw-r-- 1 jessica newtest 0 Oct  2 11:58 test2file.txt
```

Step 7:

- Reveal the content of the file

```
(jessica@kali)-[~]
└─$ cat jfrim001.hash.file
root:!:19961:0:99999:7:::
daemon:!:19961:0:99999:7:::
bin:!:19961:0:99999:7:::
sys:!:19961:0:99999:7:::
sync:!:19961:0:99999:7:::
games:!:19961:0:99999:7:::
man:!:19961:0:99999:7:::
lp:!:19961:0:99999:7:::
mail:!:19961:0:99999:7:::
news:!:19961:0:99999:7:::
uucp:!:19961:0:99999:7:::
proxy:!:19961:0:99999:7:::
www-data:!:19961:0:99999:7:::
backup:!:19961:0:99999:7:::
list:!:19961:0:99999:7:::
irc:!:19961:0:99999:7:::
_apt:!:19961:0:99999:7:::
```

Step 8:

- Using john the ripper password cracking for 10 minutes

- Three passwords were only cracked out of six

```
(jessica@kali)-[~]
└─$ sudo john --format=crypt jfrim001.hash.file --wordlist=/home/jessica/rockyou.txt
Using default input encoding: UTF-8
Loaded 16 password hashes with 16 different salts (crypt, generic crypt(3) [?/64])
Remaining 15 password hashes with 15 different salts
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234      (John)
blue      (John2)
green5    (John5)
3g 0:00:11:50 0.11% (ETA: 2024-10-19 04:39) 0.004224g/s 26.63p/s 344.5c/s 344.5C/s sukses..garuda
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```