Lab Assignment 4: Password Cracking

Course Code:	CYB301
Course Name:	Security, Defence, and Response
Time:	75+ minutes in class
Student Name	Saiprasad Raman
Student ID	23074624

Materials and Resources

Textbooks:	N/A
Software:	N/A
Websites:	• NPR Link • Vice Link • Openwall Yescrypt • Openwall: John the Ripper's Command Line Syntax • Openwall: John the Ripper's Cracking Modes • Wordlist 1 • Wordlist 2
Videos:	N/A
Other:	N/A

Assignment Description

One of the biggest takeaways from Verizon's 2020 Data Breach Investigations Report (DBIR) was that over 80 percent of hacking-related breaches involve brute force or the use of stolen credentials.
Although they are not the best choice for authentication and gaining remote access to systems and networks, passwords (things you know) are still more heavily used than security tokens, key fobs, or smart cards (things you have) and biometrics (something you are).

Attackers can use a technique called password guessing in which they manually enter passwords at a login prompt to gain access to an account when they have a valid username. In fact, this is exactly what happened with two Major League Baseball teams in 2013, when a St. Louis Cardinals executive guessed the password of a former co-worker who used to work for the Cardinals but moved on to the Houston Astros. This led to considerable confidential information about players, potential trades, and scouting reports getting into the hands of a rival executive. The information was publicly dumped and wound up embarrassing numerous players and teams. Read about it at these links:

- NPR Link
- Vice Link

There are two steps in this Dictionary Attack: create user accounts and crack them, and then using rockyou.txt attempt to crack password hashes.

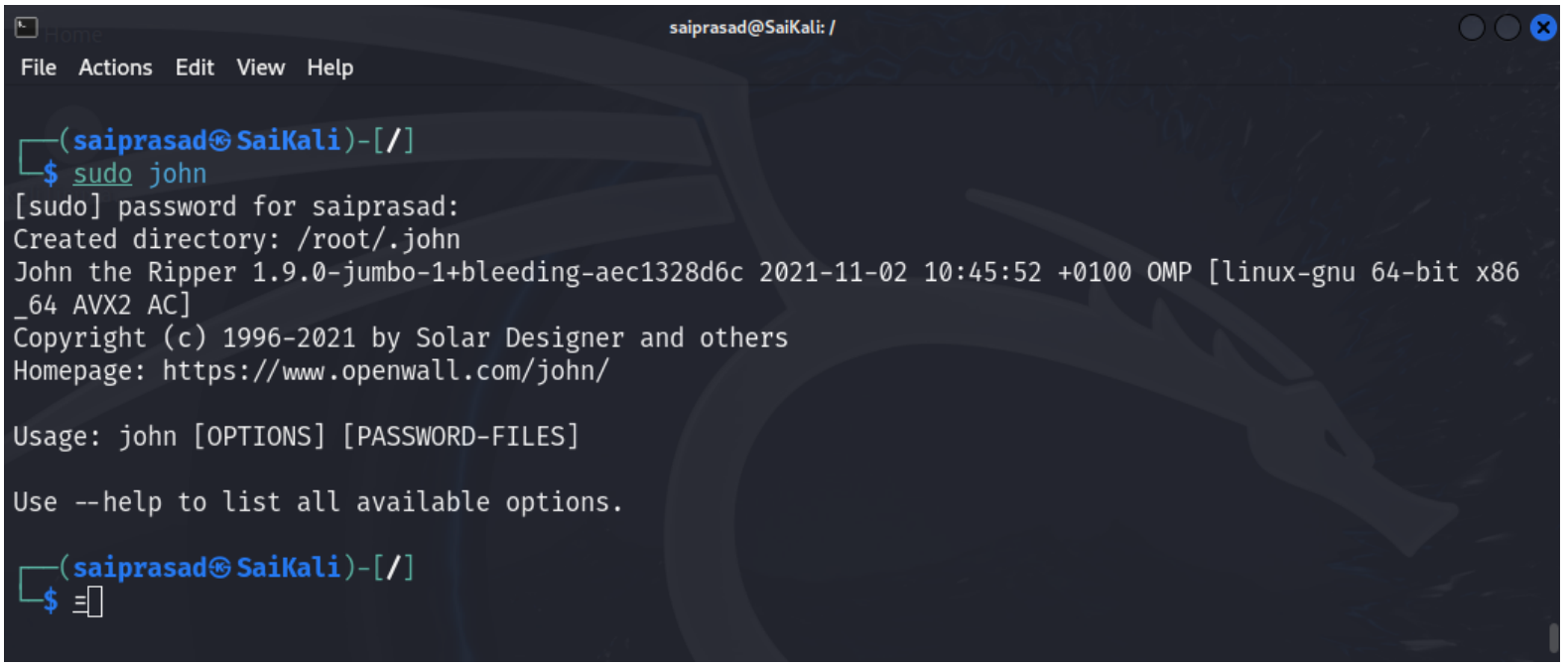
Assignment Steps

In previous labs, you may have created different user accounts. For cleaner output and the ability to focus on this lab's activities and user accounts, delete each of those user accounts (as well as any other users you created, except for the first user created with the Kali Linux installation—the account you are logged in with now) with the deluser command.

- Launch your Kali Linux VM and open a terminal. Press ENTER after each command.

STEP 1: Create user accounts and crack them with the default wordlist that comes with John the Ripper, as well as metadata GECOS information.

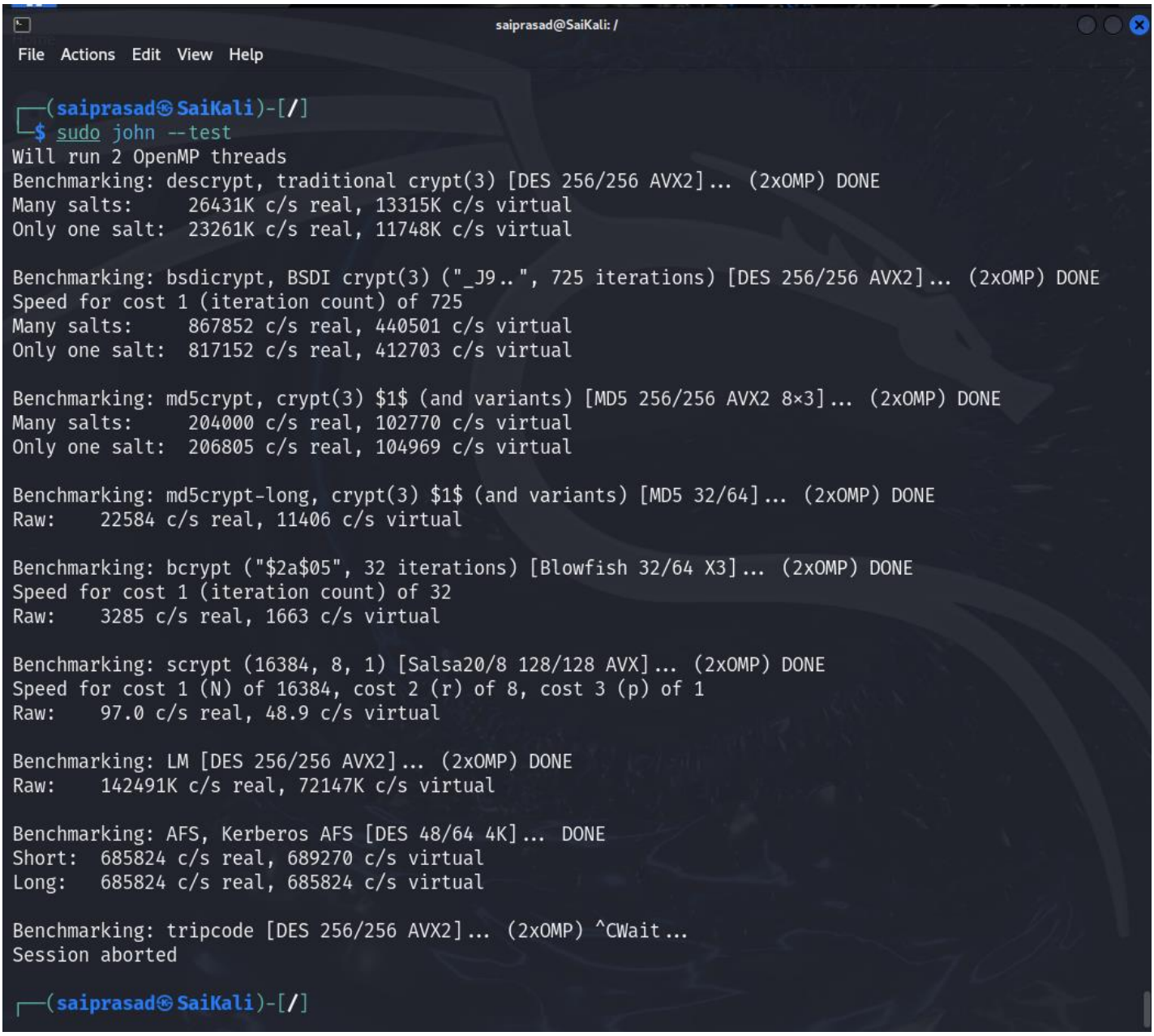
a) Display usage help for John the Ripper, a password-cracking program:
sudo john
Provide your password if prompted now and throughout this lab.



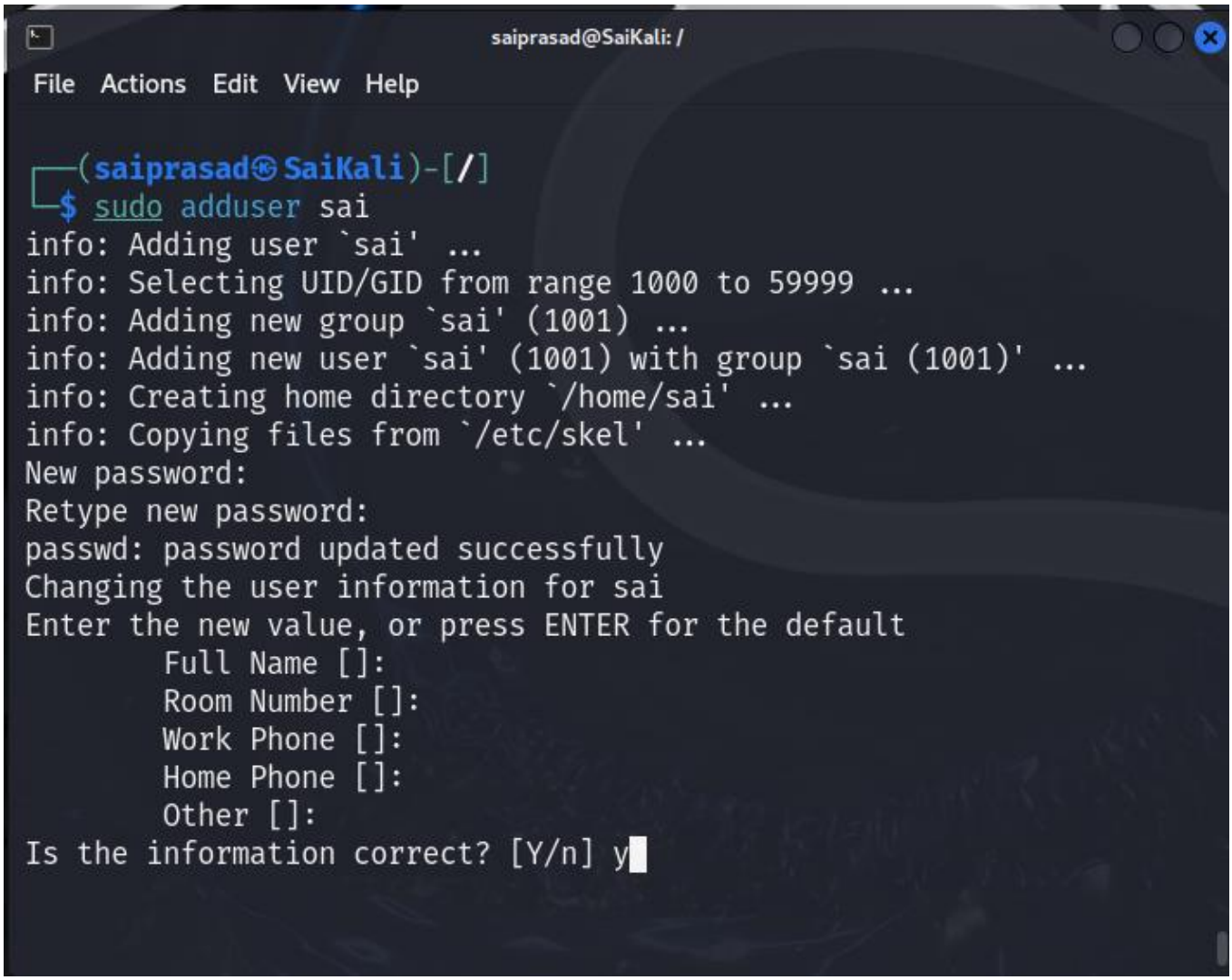
b) See the man page entry for John the Ripper:
man john

c) Enter the following command to get an idea of how long it will take John the Ripper to crack passwords based on various cryptographic schemes based on your current system:

sudo john --test

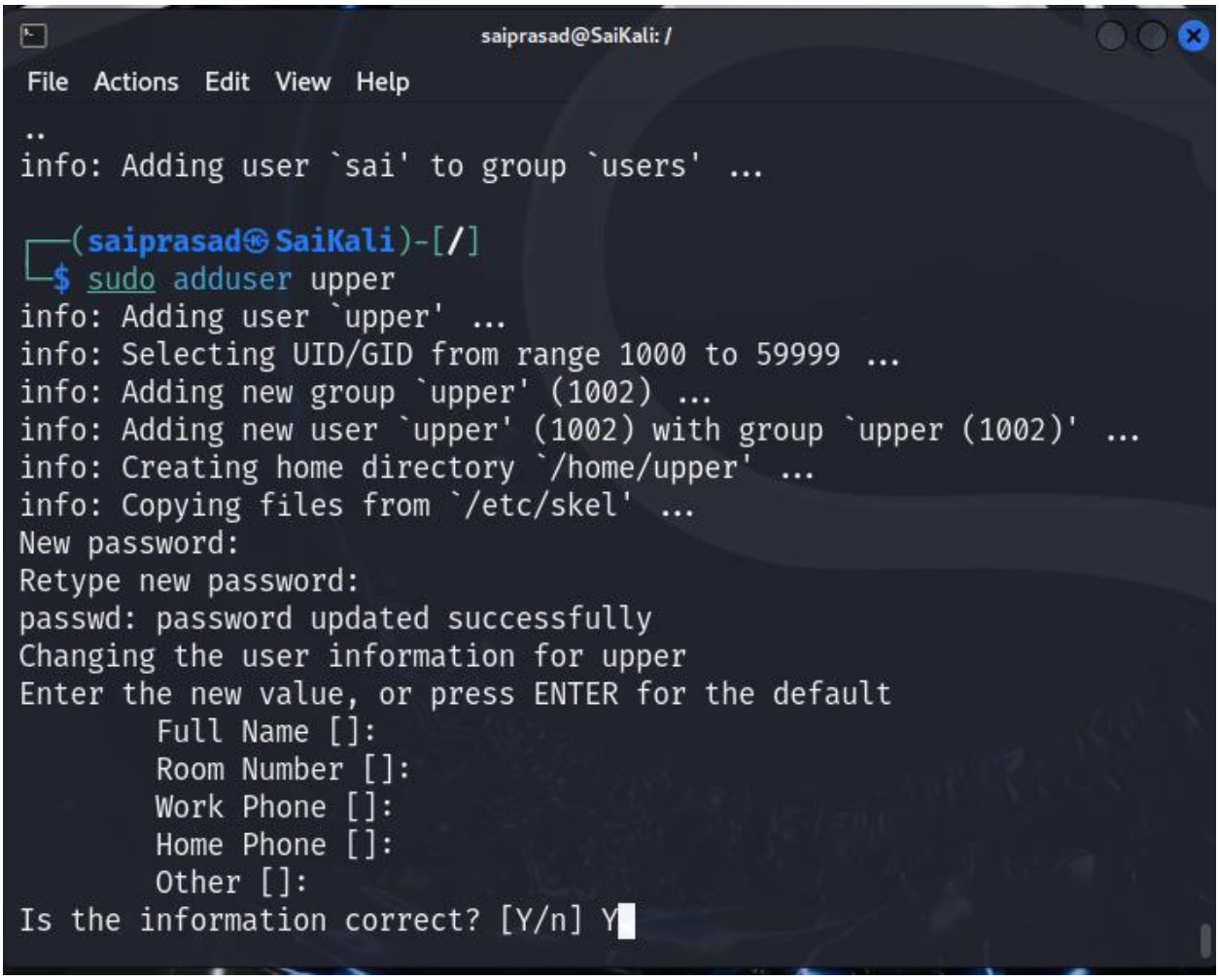


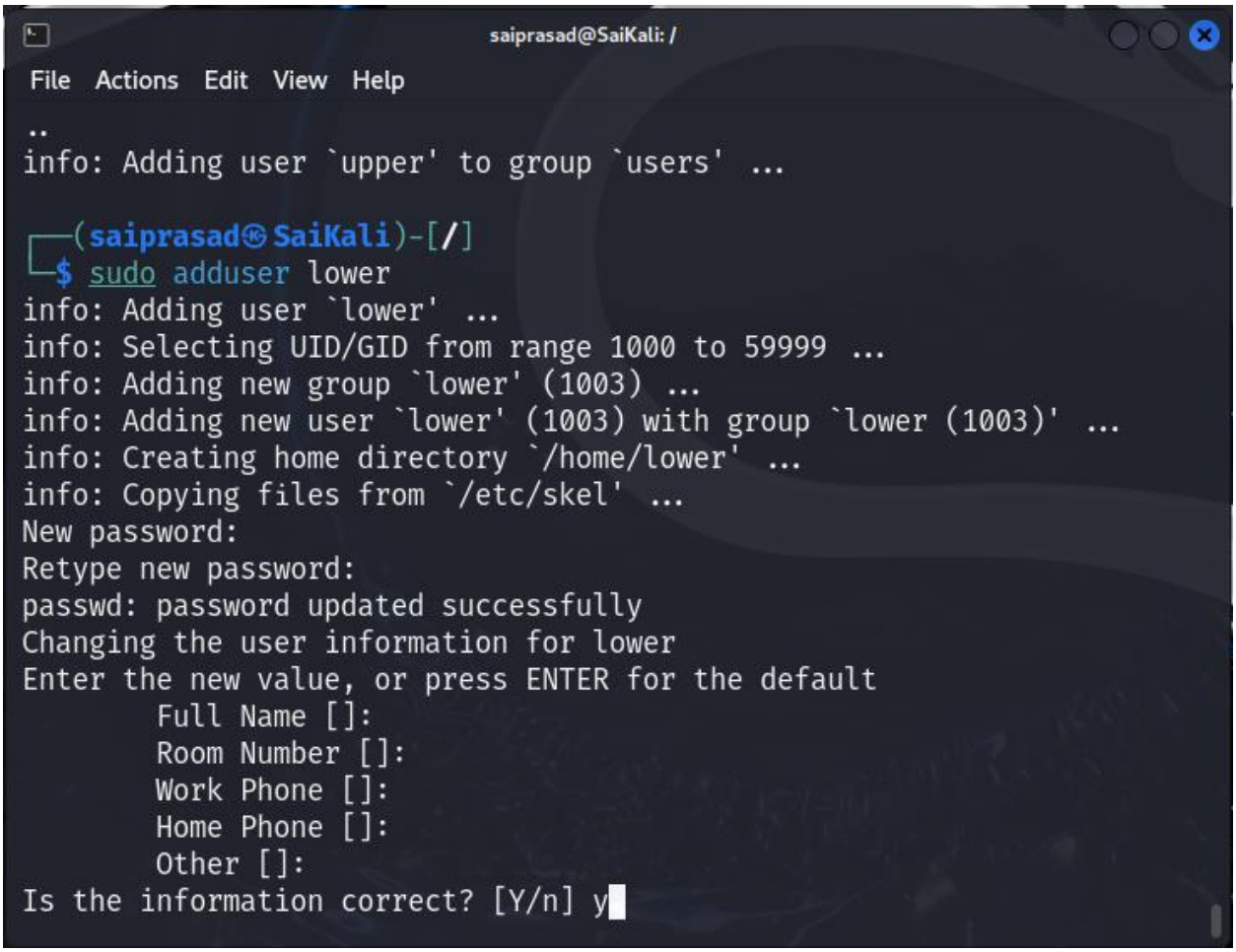
d) Enter the following command to create a user namd *[Your First Name]*:
sudo adduser muhammad

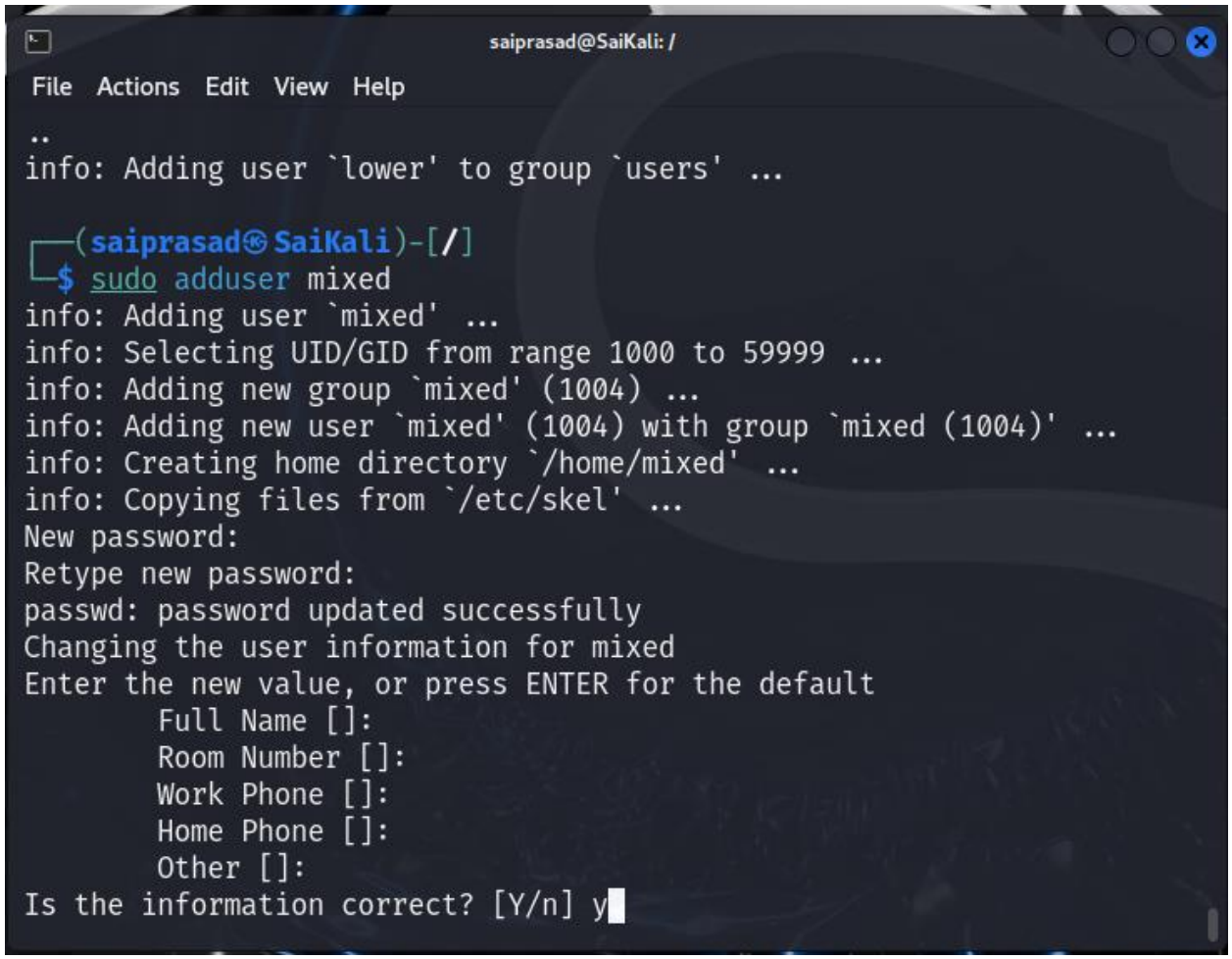


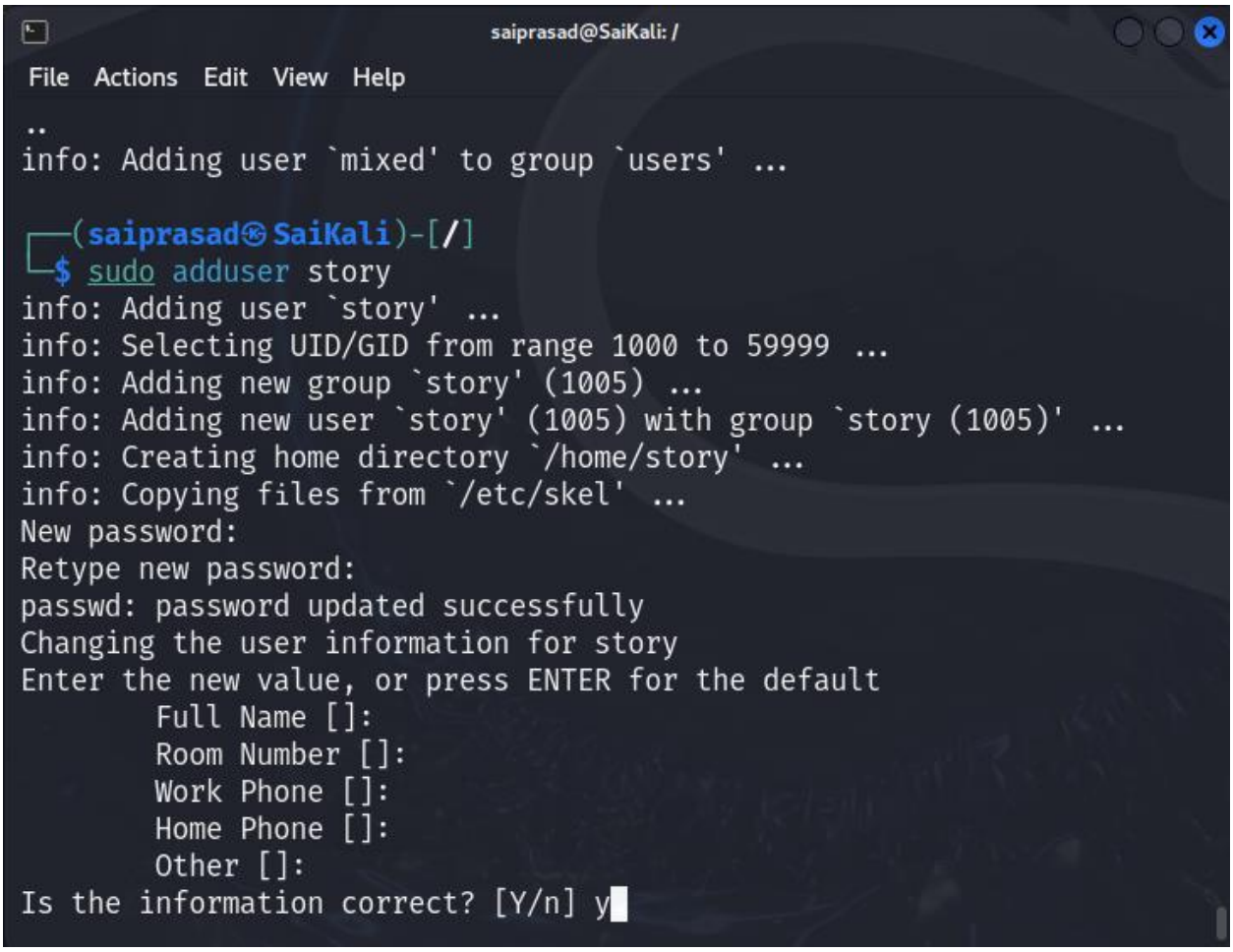
e) Add these additional username/password combinations, paying close attention to case:

Username	Password
upper	PASSWORD
lower	password
mixed	Password
story	3bears




saiprasad@SaiKali: /
File Actions Edit View Help
..
info: Adding user `upper' to group `users' ...
(saiprasad㉿SaiKali)-[/]
$ sudo adduser lower
info: Adding user `lower' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `lower' (1003) ...
info: Adding new user `lower' (1003) with group `lower (1003)' ...
info: Creating home directory `/home/lower' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lower
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

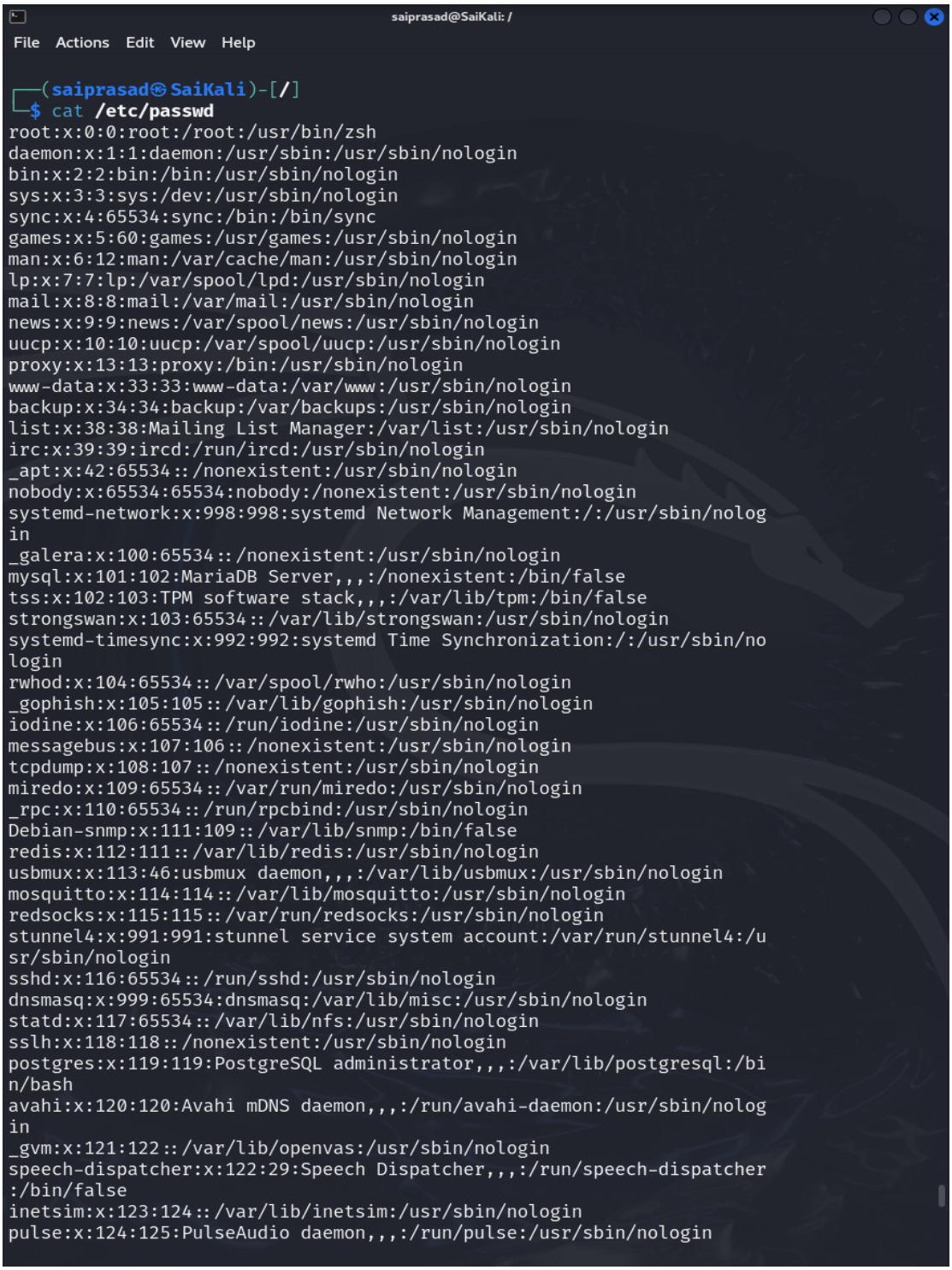

saiprasad@SaiKali: /
File Actions Edit View Help
..
info: Adding user `lower' to group `users' ...
┌──(saiprasad㉿SaiKali)-[/]
└─$ sudo adduser mixed
info: Adding user `mixed' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `mixed' (1004) ...
info: Adding new user `mixed' (1004) with group `mixed (1004)' ...
info: Creating home directory `/home/mixed' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mixed
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


saiprasad@SaiKali: /
File Actions Edit View Help
..
info: Adding user `mixed' to group `users' ...
(saiprasad㉿SaiKali)-[/]
$ sudo adduser story
info: Adding user `story' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `story' (1005) ...
info: Adding new user `story' (1005) with group `story (1005)' ...
info: Creating home directory `/home/story' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for story
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

f) Explore the /etc/passwd and /etc/shadow files with the cat command

cat /etc/passwd

sudo cat /etc/shadow




saiprasad@SaiKali: /
File Actions Edit View Help
story:x:1005:1005:,,,:/home/story:/bin/bash
(saiprasad㉿SaiKali)-[/]
$ sudo cat /etc/shadow
root:!:19972:0:99999:7:::
daemon:*:19972:0:99999:7:::
bin:*:19972:0:99999:7:::
sys:*:19972:0:99999:7:::
sync:*:19972:0:99999:7:::
games:*:19972:0:99999:7:::
man:*:19972:0:99999:7:::
lp:*:19972:0:99999:7:::
mail:*:19972:0:99999:7:::
news:*:19972:0:99999:7:::
uucp:*:19972:0:99999:7:::
proxy:*:19972:0:99999:7:::
www-data:*:19972:0:99999:7:::
backup:*:19972:0:99999:7:::
list:*:19972:0:99999:7:::
irc:*:19972:0:99999:7:::
_apt:*:19972:0:99999:7:::
nobody:*:19972:0:99999:7:::
systemd-network:!*:19972::::::
_galera:!:19972::::::
mysql:!:19972::::::
tss:!:19972::::::
strongswan:!:19972::::::
systemd-timesync:!*:19972::::::
rwhod:!:19972::::::
_gophish:!:19972::::::
iodine:!:19972::::::
messagebus:!:19972::::::
tcpdump:!:19972::::::
miredo:!:19972::::::
_rpc:!:19972::::::
Debian-snmp:!:19972::::::
redis:!:19972::::::
usbmux:!:19972::::::
mosquitto:!:19972::::::
redsocks:!:19972::::::
stunnel4:!*:19972::::::
sshd:!:19972::::::
dnsmasq:!:19972::::::
statd:!:19972::::::
sslh:!:19972::::::
postgres:!:19972::::::
avahi:!:19972::::::
_gvm:!:19972::::::
speech-dispatcher:!:19972::::::
inetsim:!:19972::::::
pulse:!:19972::::::
geoclue:!:19972::::::
lightdm:!:19972::::::
saned:!:19972::::::
polkitd:!*:19972::::::
rtkit:!:19972::::::
colord:!:19972::::::
nm-openvpn:!:19972::::::
nm-openconnect:!:19972::::::
saiprasad:yj9T$wKb9M7QsDO7ATrrx7AbkL/$eYCW2ZfZYm95u5.iIPtLua1ncxA0cWf7/2xKiS3BTr3:19972:0:99999:7:::
sai:yj9T$tzK6cntweFedfnwws1W7q.$Hn4jr6XEgF2fCoEydl6ALkmSkQq/oenZgf14kxxGAf3:19981:0:99999:7:::
upper:yj9T$WmaoLj1SLTHus00gLAj960$.aIGes3NnnQ3yFTWh/t7J1D21nau/qsERlV1xe7OZCB:19981:0:99999:7:::
lower:yj9T$XbvlnEU2Vlko8k7OBNtjx/$UEz1hsuz2gFZ3FJCZ5i5JIEji3LgakUCKgFmcKn0ZOC:19981:0:99999:7:::
mixed:yj9T$3UnXv0U8BLhbmYNRUiwqT.$ExQPqjXYpRb1PM7uqEANtJ6FDunHISq/b9QnmcQy43D:19981:0:99999:7:::
story:yj9T$isEwmLYxGpodfKle0O4FH1$/uPPLh69CpXRW1pJJi0JSLRY.9NG3NgeQU41lhFq/y4:19981:0:99999:7:::

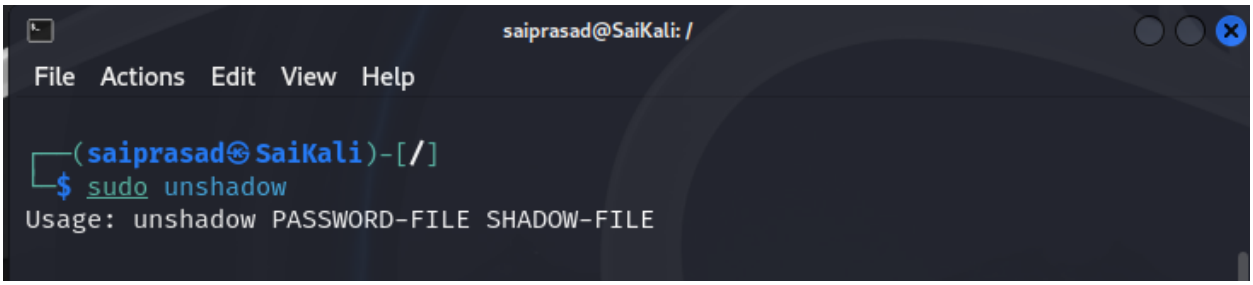
g) The **unshadow** utility combines the /etc/passwd and /etc/shadow files. This is done so John the Ripper can attempt to crack the password with information from both files, using a single file.

Enter the following command to see the man page entry for unshadow:

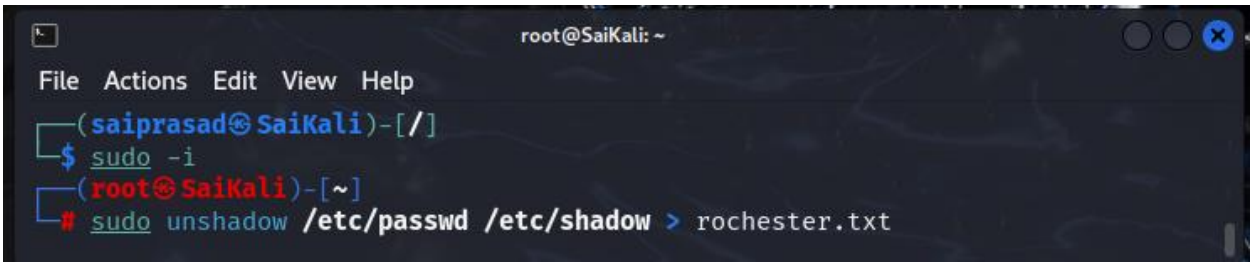
man unshadow

Type **q** to quit.

h) To see the usage of the unshadow utility, type the following command:
sudo unshadow

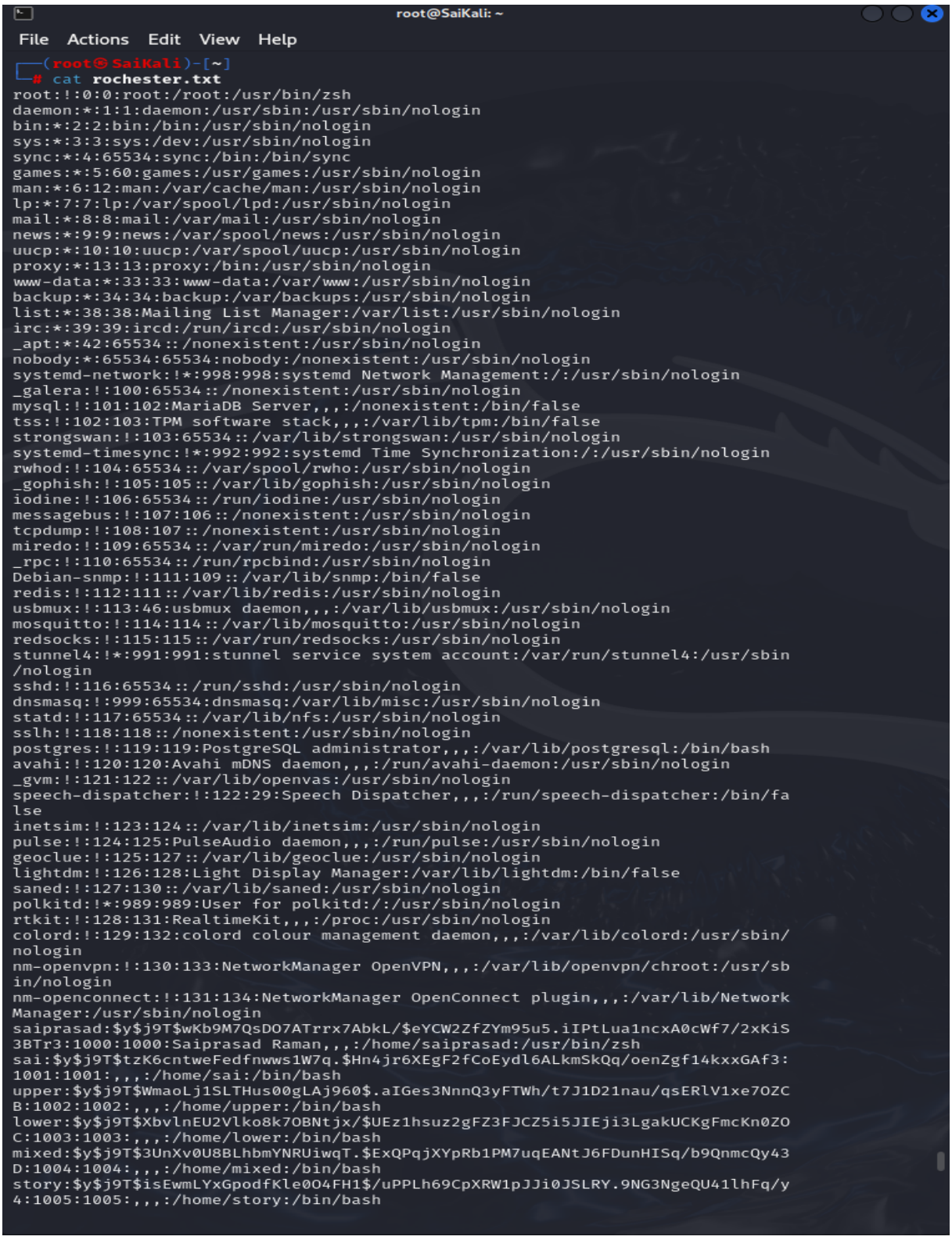


i) Enter the following command to merge the /etc/passwd and /etc/shadow files into a file called rochester.txt for John the Ripper:
sudo unshadow /etc/passwd /etc/shadow > rochester.txt



j) Type the following command to display the rochester.txt file:

cat rochester.txt



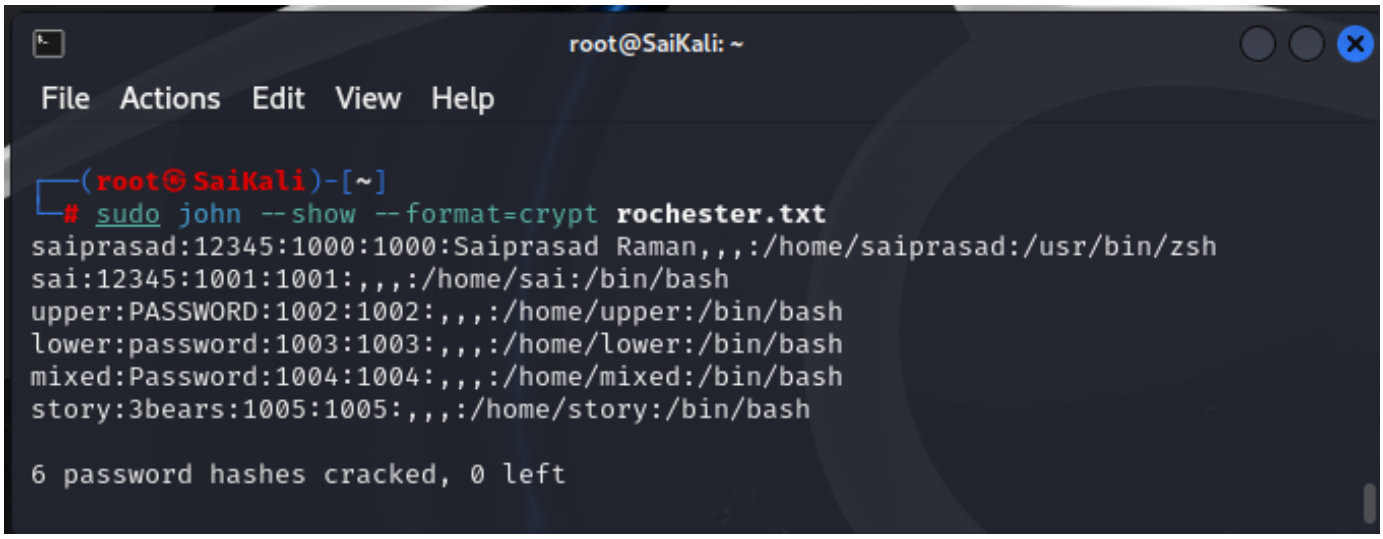
k) Using a wordlist that comes with John the Ripper(/usr/share/john/password.lst), crack as many passwords as possible from the merged file (rochester.txt):

sudo john --wordlist=/usr/share/john/password.lst --format=crypt rochester.txt

At the point of cracking, the passwords and usernames appear on the screen.

If your regular user account's password is in the password.lst file, it will be shown as well.

l) **sudo john --show --format=crypt rochester.txt**

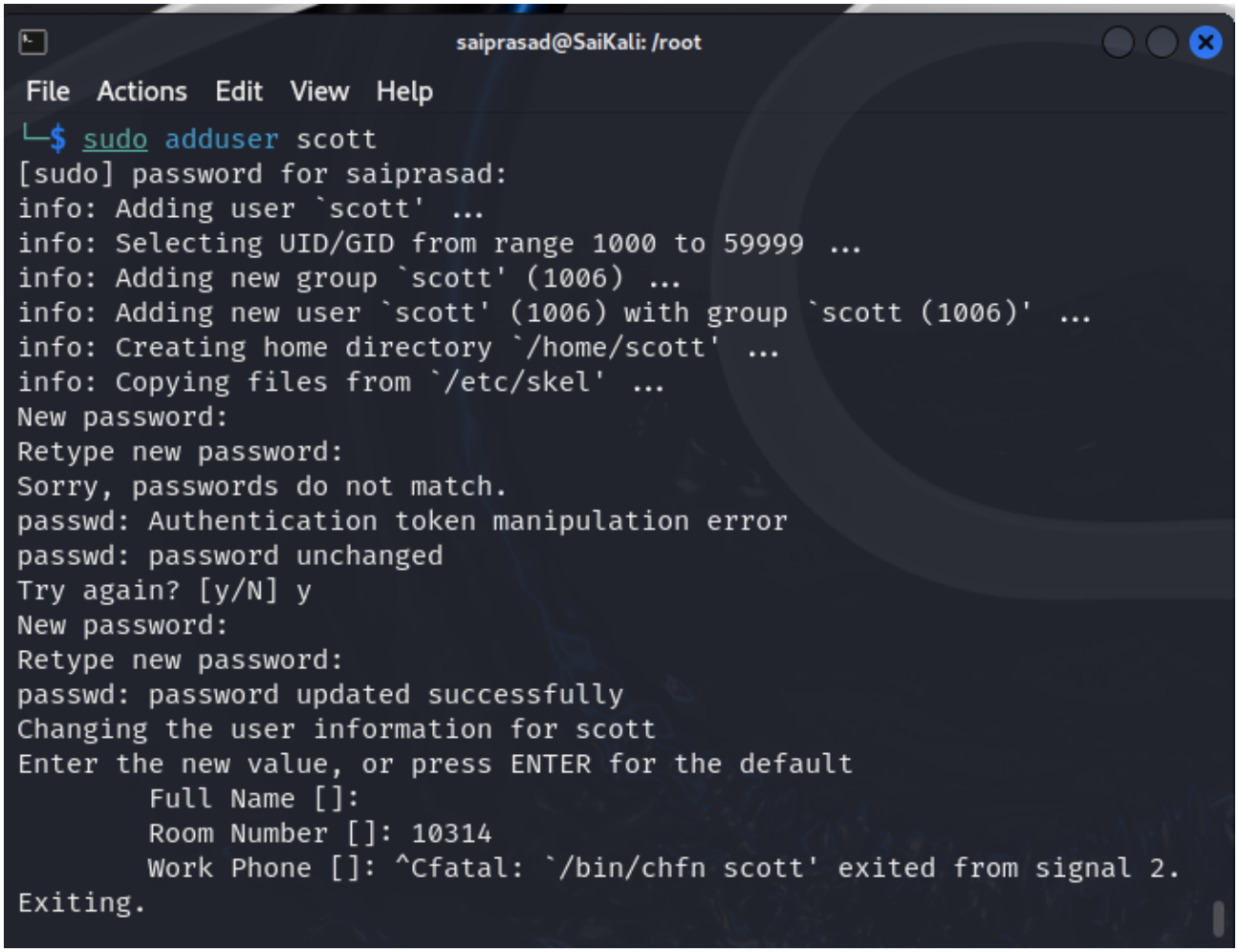


m) To remove all remembered cracked passwords from John the Ripper, delete the john.pot file, located in /root/.john:

sudo rm /root/.john/john.pot

n) Create a new user called scott:

sudo adduser scott

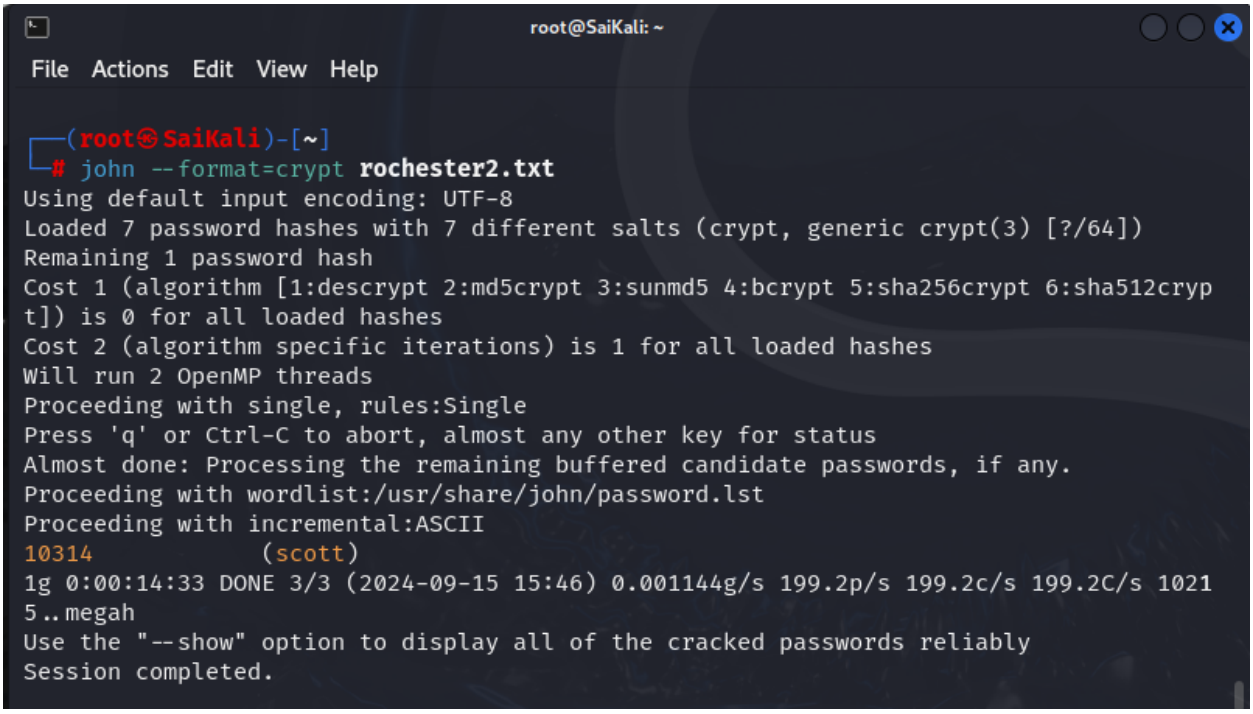


o) Create a new unshadow file called rochester2.txt, updated with the new user (scott):

sudo unshadow /etc/passwd /etc/shadow > rochester2.txt

p) Run John the Ripper, but this time without a wordlist:

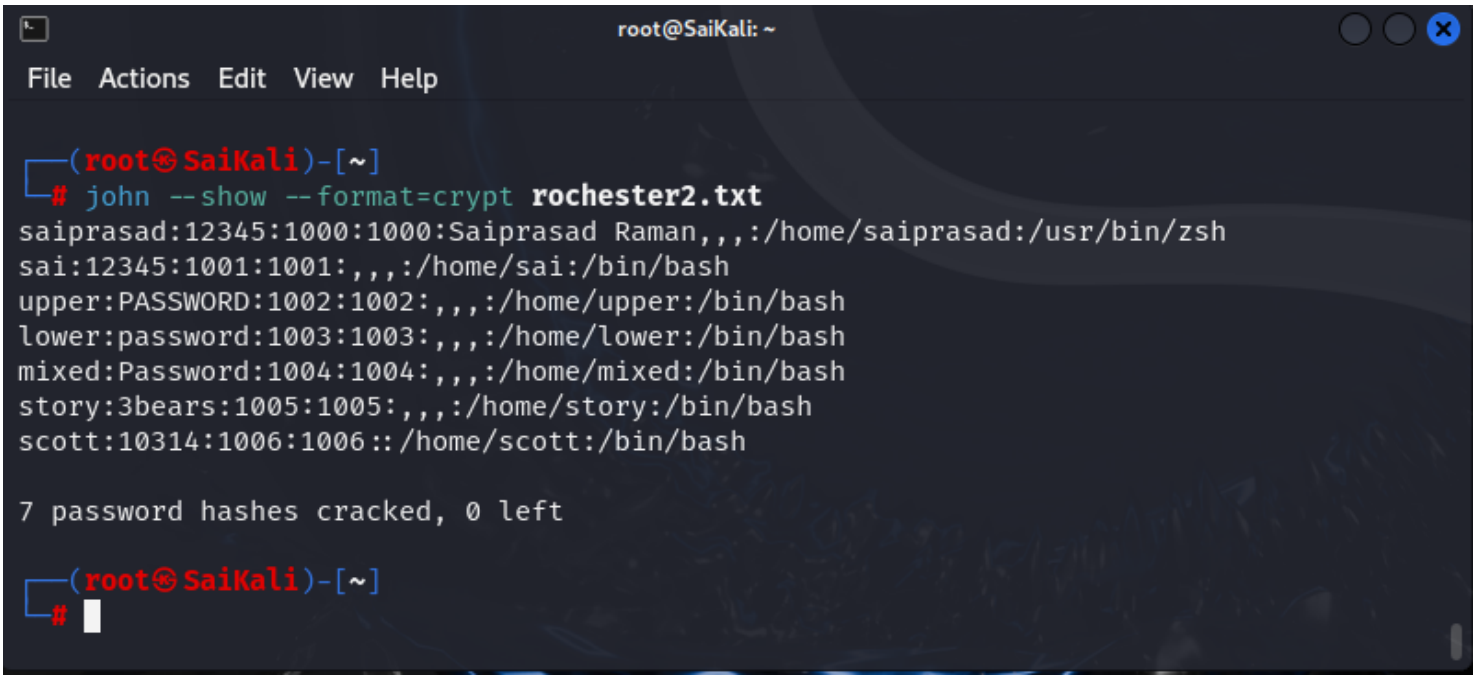
sudo john --format=crypt rochester2.txt



q) Enter the following command to see all cracked passwords, including the latest one:

sudo john --show --format=crypt rochester2.txt

STEP 2: The wordlist that comes with John the Ripper is not really that great, due to its small number of words. The more words in a wordlist, the greater your odds of successfully cracking passwords. **Take a screenshot.**



a) Copy the compressed rockyou.txt file to the current directory (the dot at the end of the command represents the current directory):

cp /usr/share/wordlists/rockyou.txt.gz .

b) Decompress (-d) the file using the gzip utility.

gzip -d rockyou.txt.gz

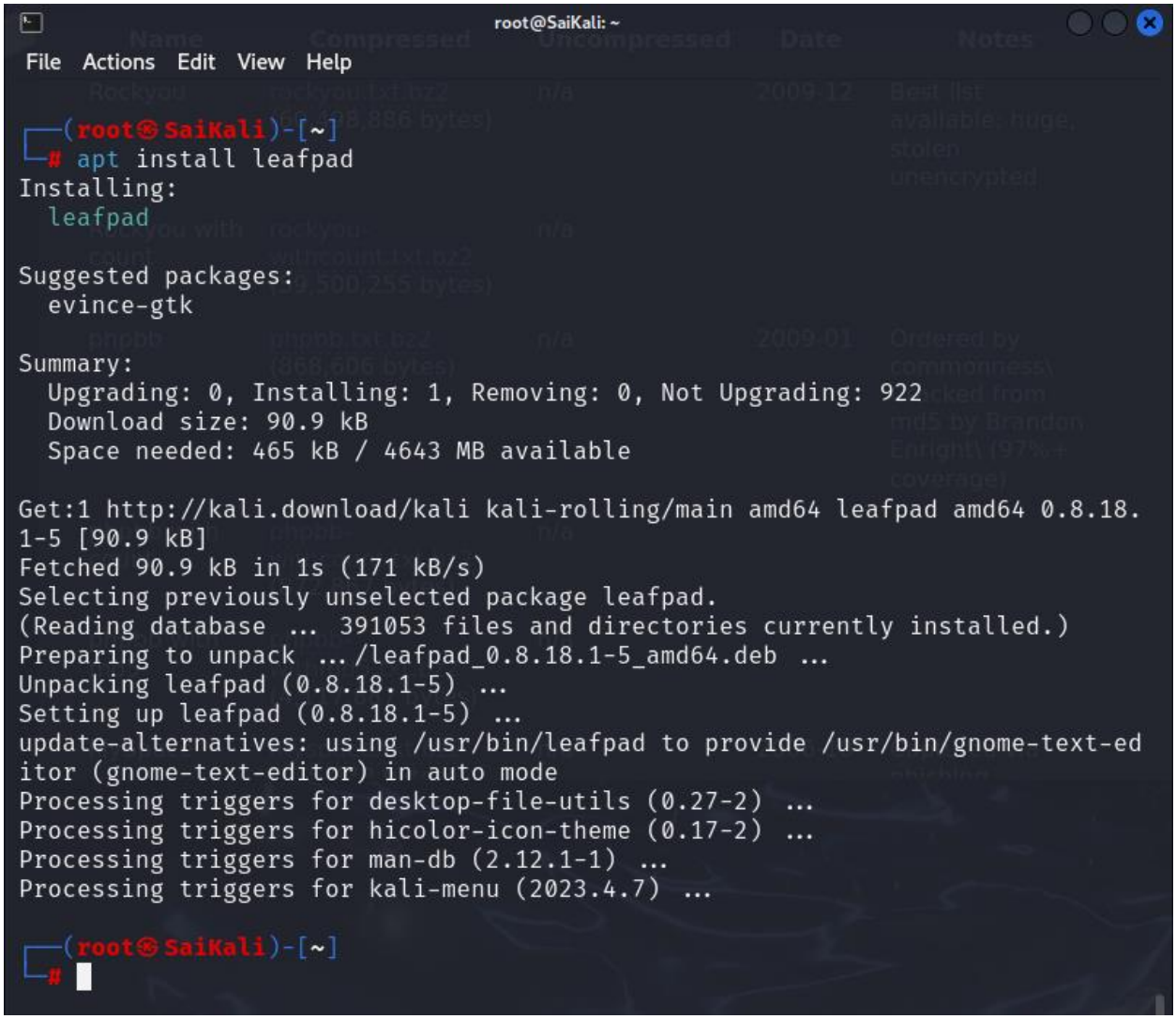
c) Compare the size of the John the Ripper password wordlist file (26325 bytes or 26.325 KB) to the size of rockyou.txt (139921507 bytes or 139.921507 MB).

ls -l /usr/share/john/password.lst

ls -l rockyou.txt

d) Enter the following command to install Leafpad:
sudo apt install leafpad

Leafpad is a text editor that does not come by default with Kali Linux.



e) Compare the contents of the wordlists. Display the contents through the terminal first:

cat /usr/share/john/password.lst

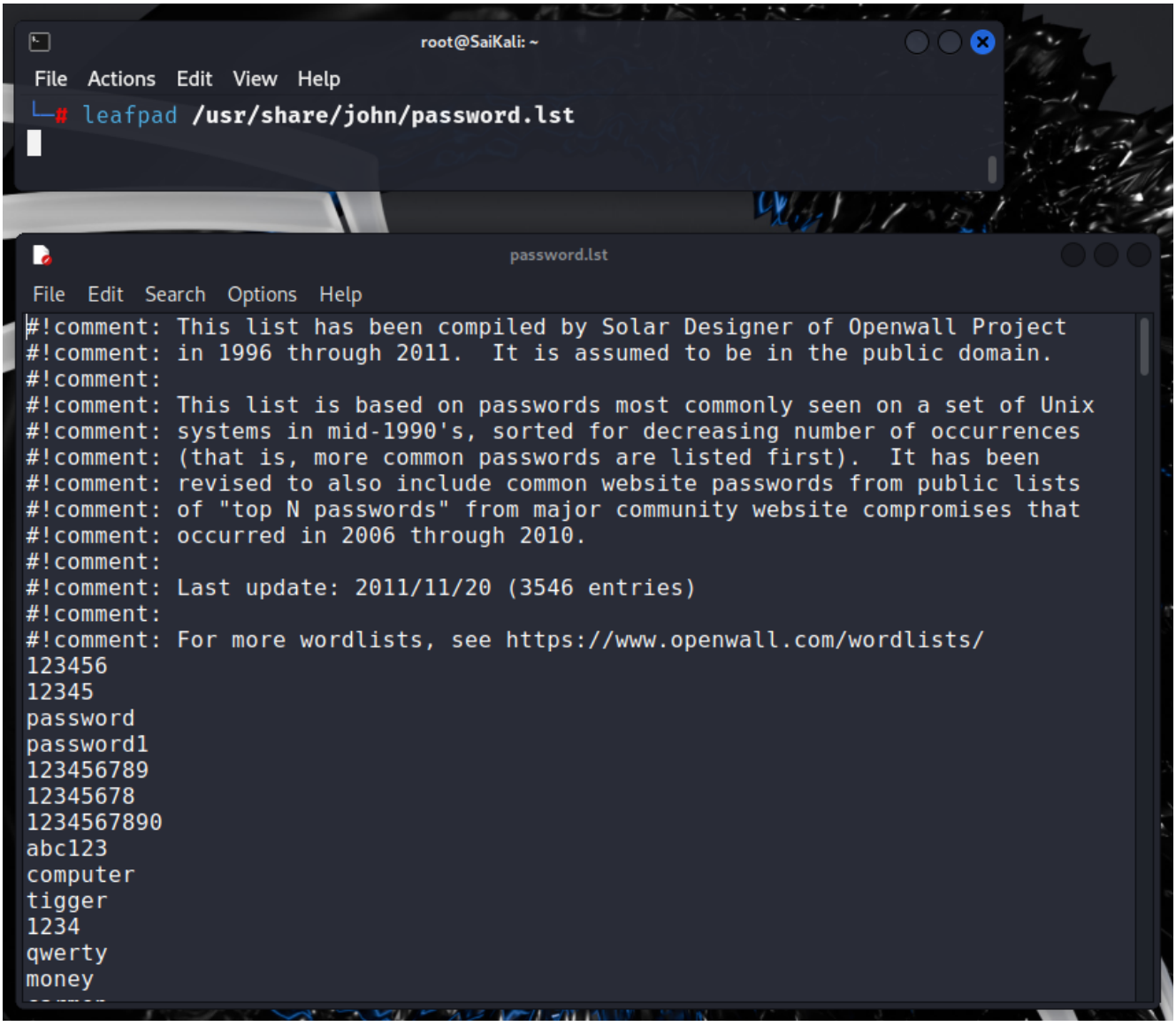
cat rockyou.txt

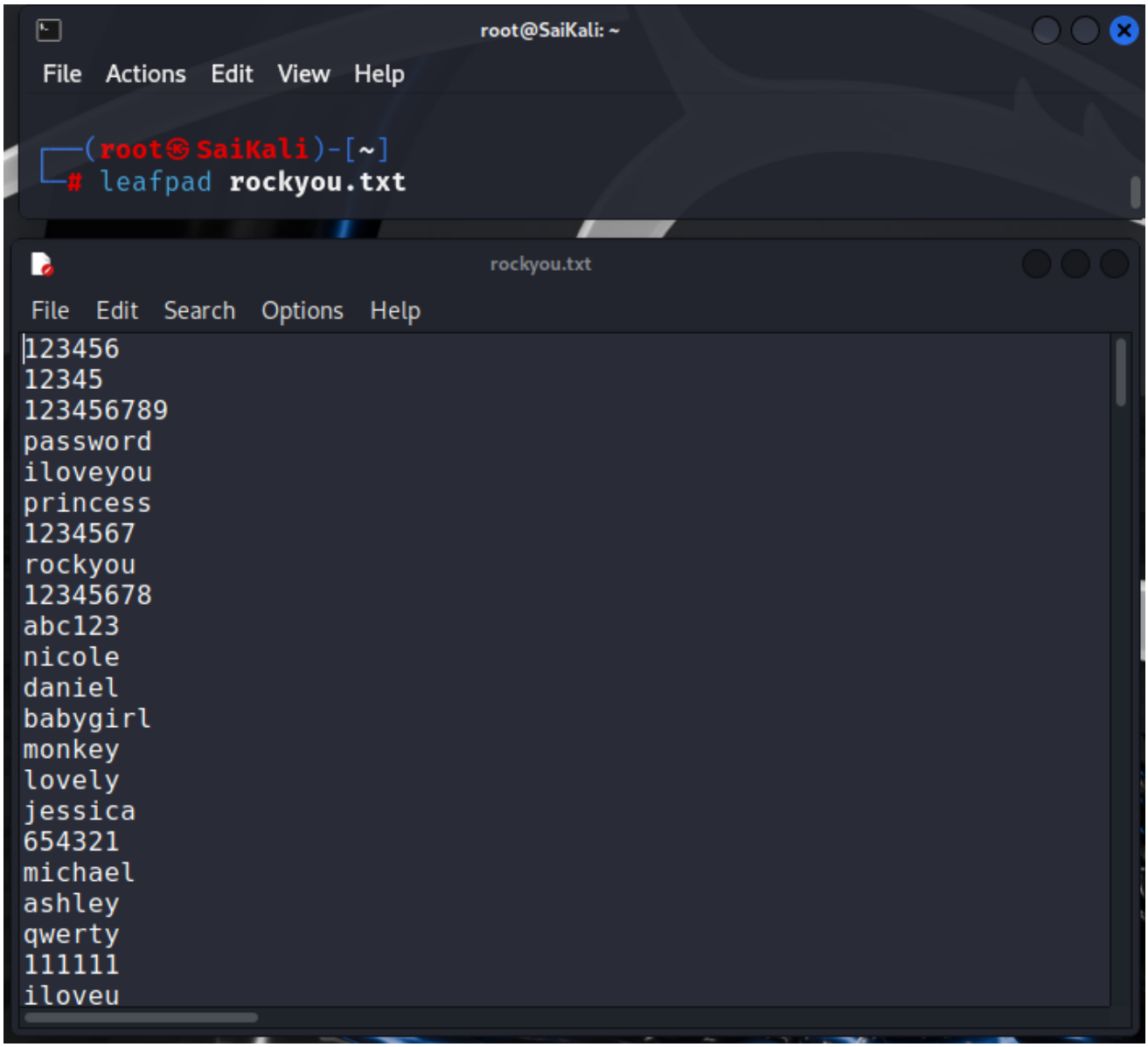

root@SaiKali: ~
File Actions Edit View Help
(root㉿SaiKali)-[~]
cat rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends

f) Look at the contents of the files through Leafpad:

leafpad /usr/share/john/password.lst

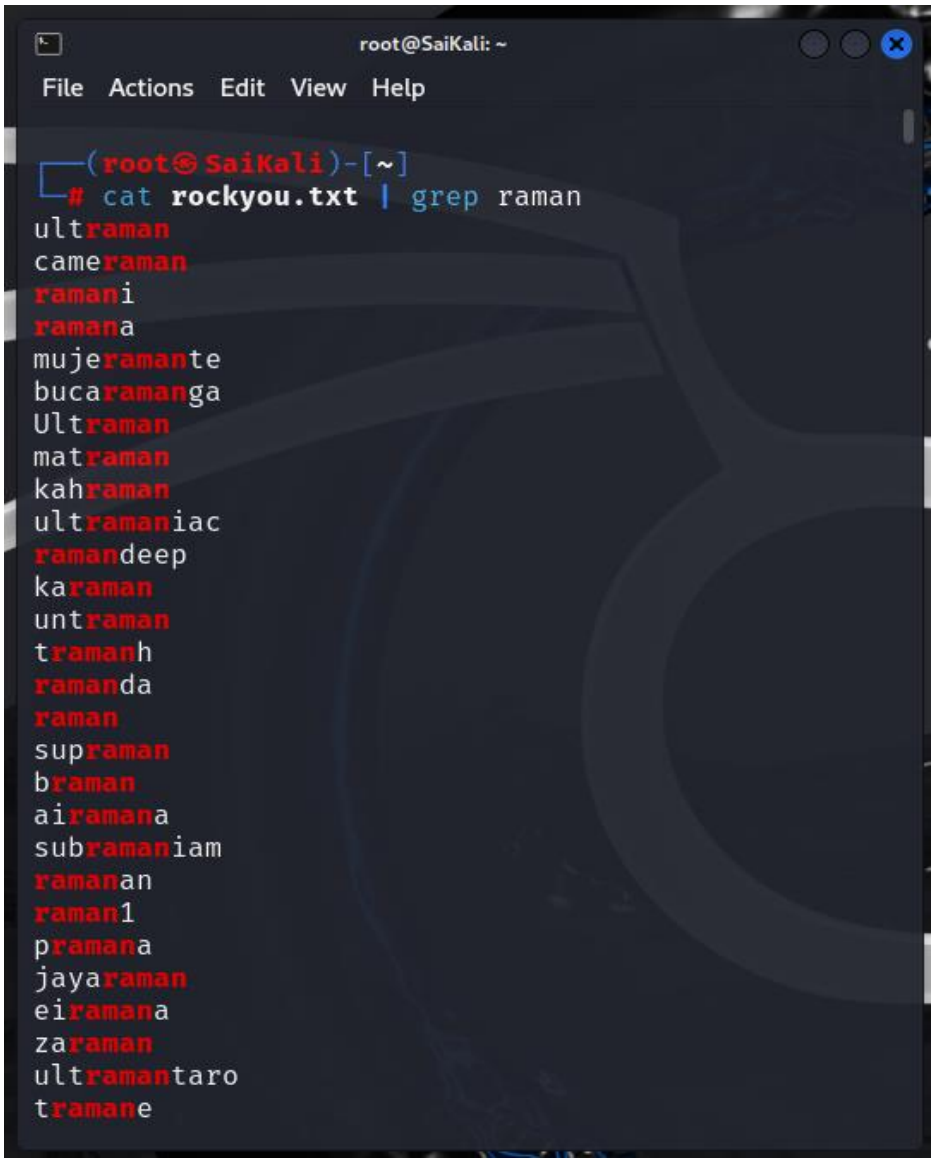
leafpad rockyou.txt




root@SaiKali: ~
File Actions Edit View Help
(root㉿SaiKali)-[~]
leafpad rockyou.txt
rockyou.txt
File Edit Search Options Help
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu

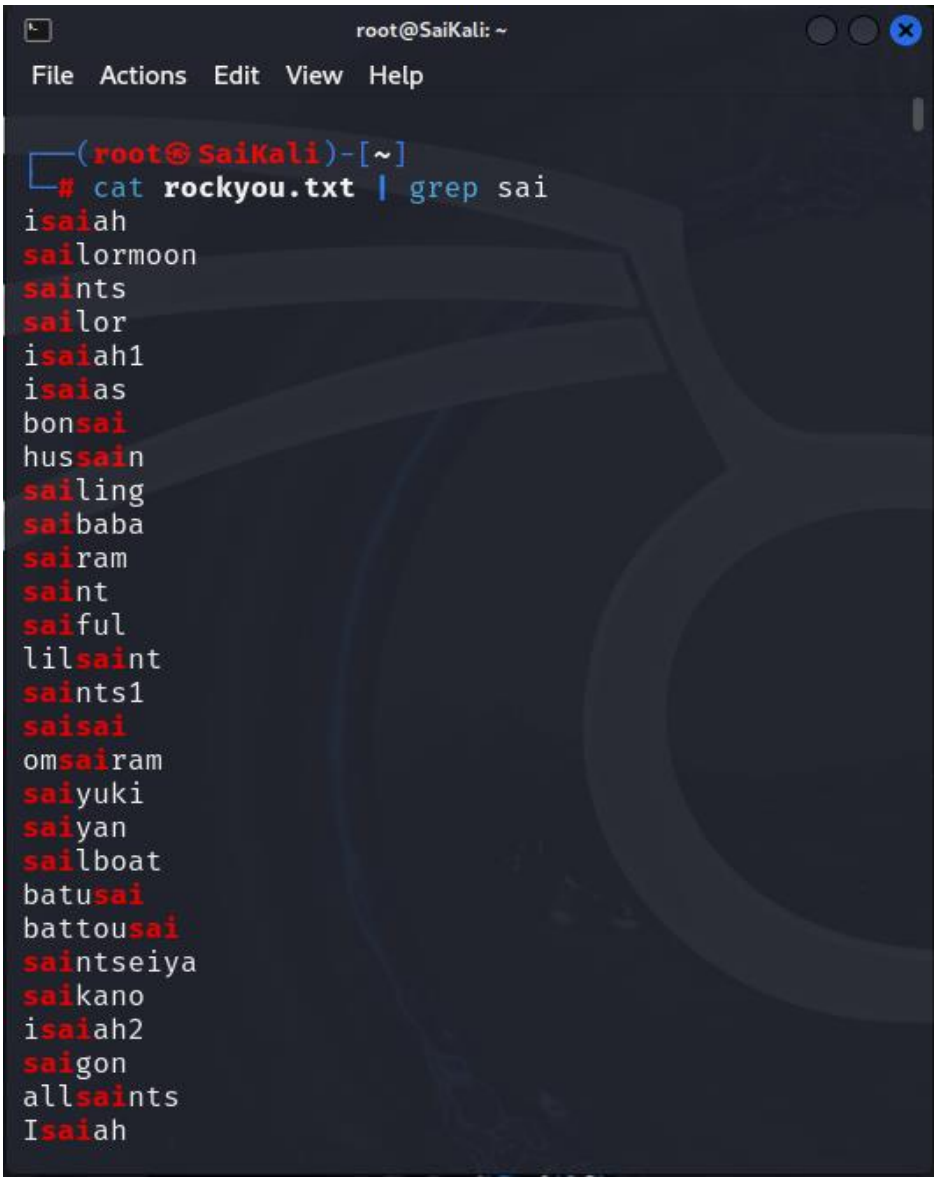
g) Display all entries in rockyou.txt that have the string *[Your Last Name]*:

cat rockyou.txt | grep siddiqui | less

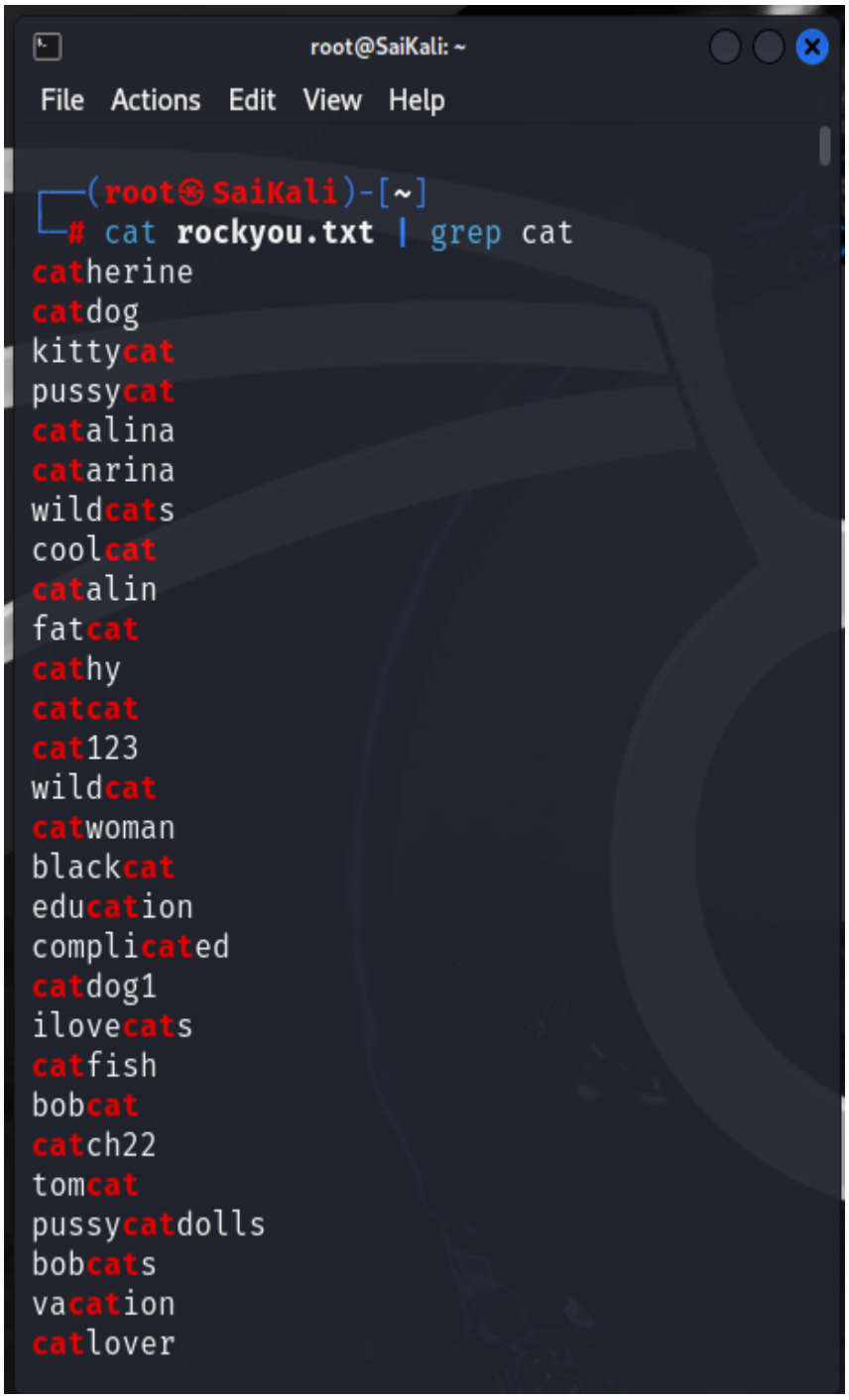


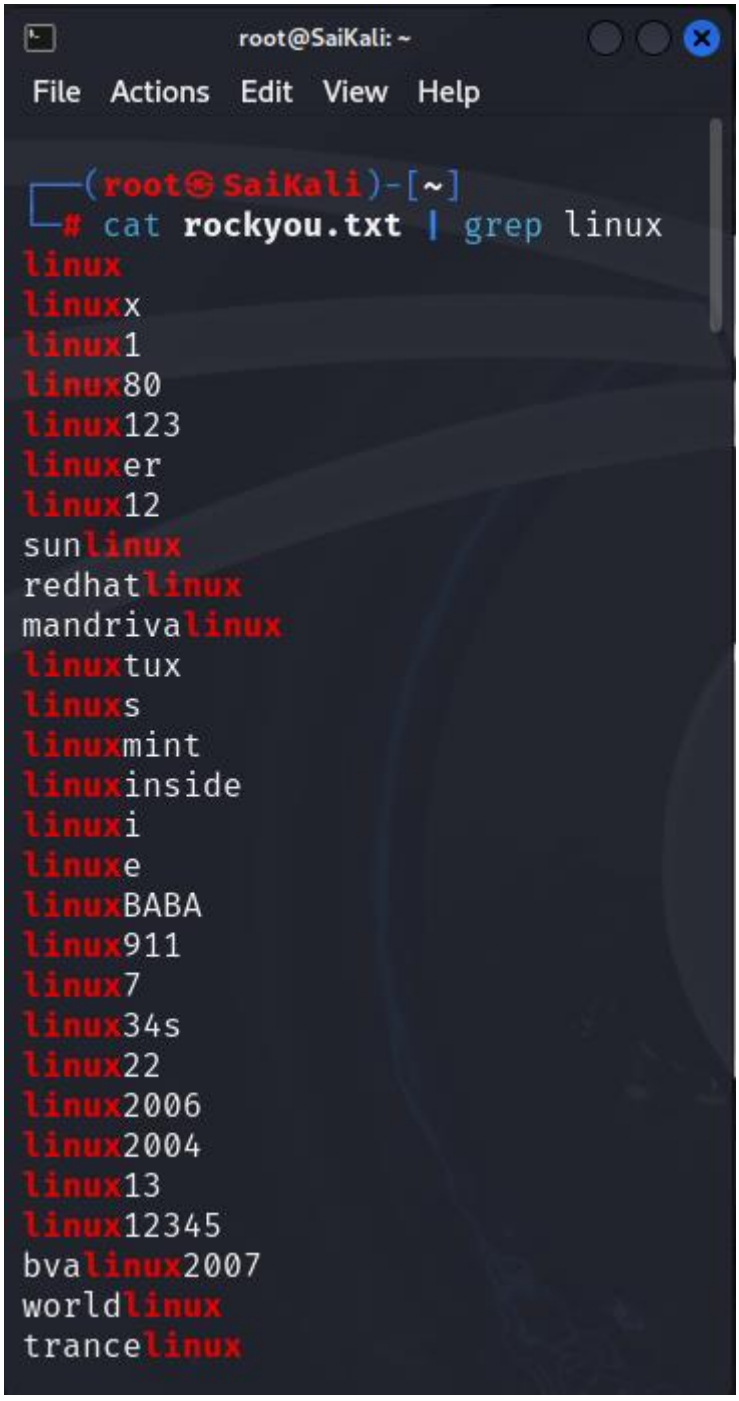
h) Display all entries in rockyou.txt that have the string *[Your First Name]*:

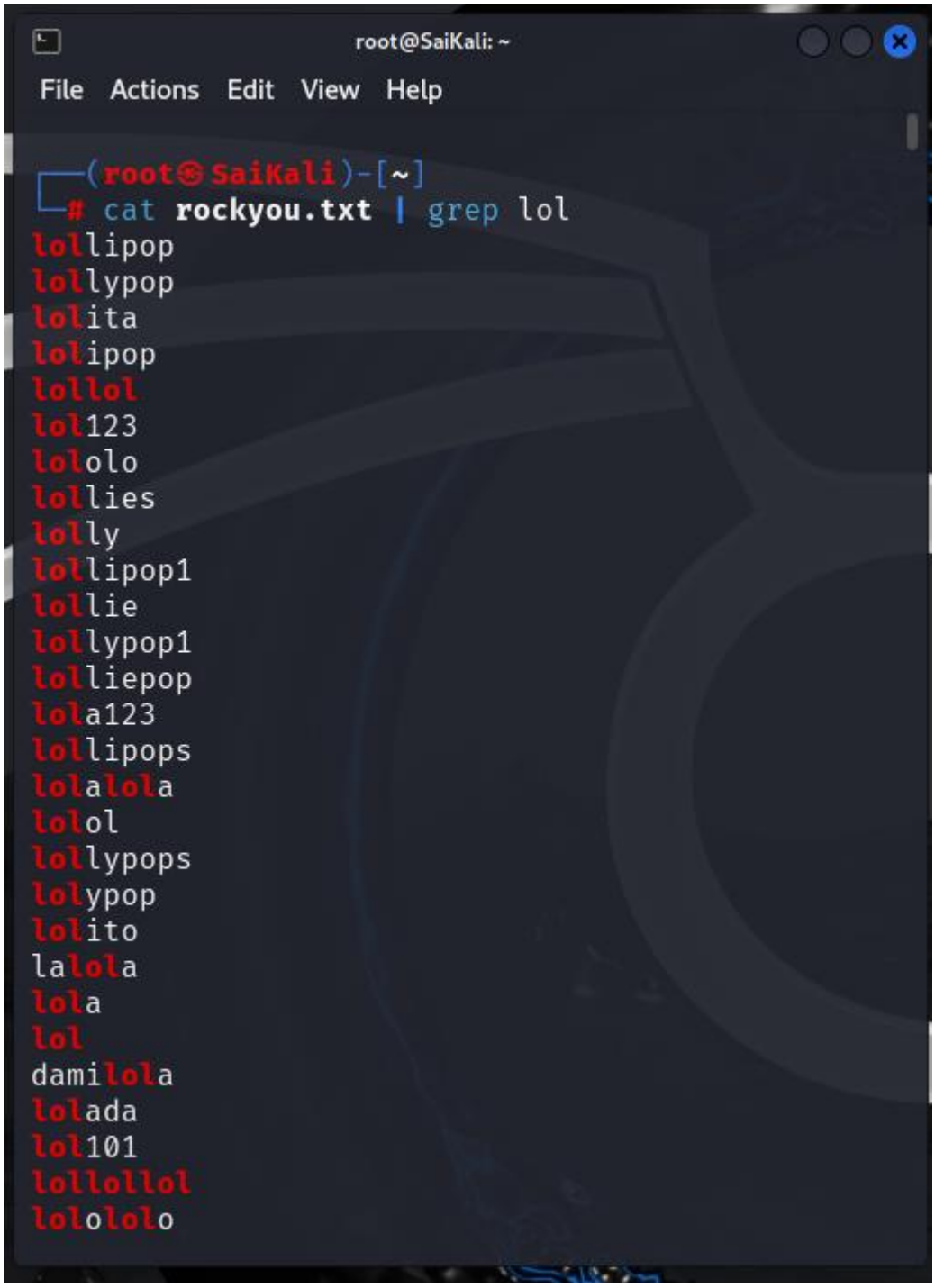
cat rockyou.txt | grep muhammad



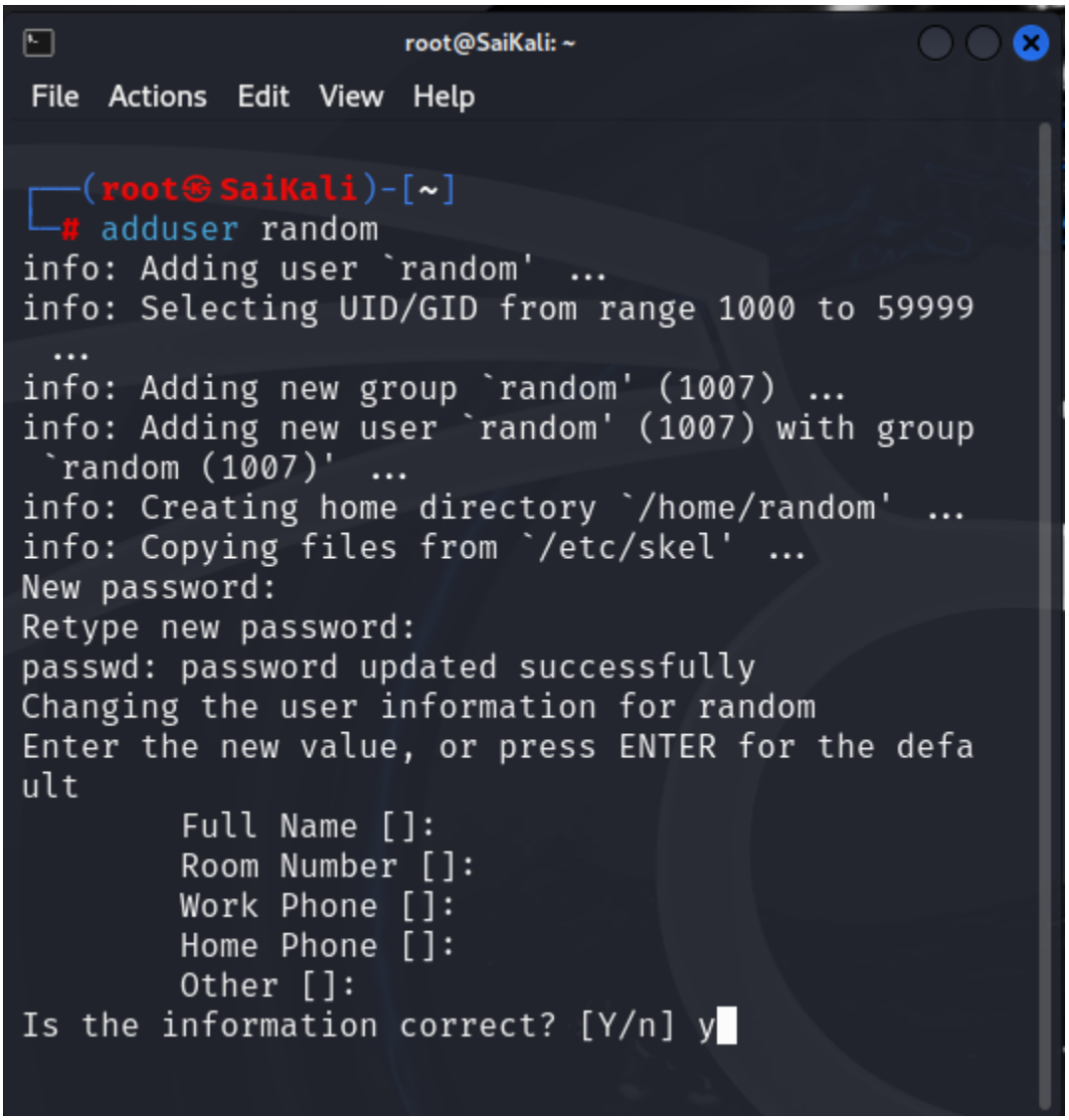
i) Search rockyou.txt for three strings of your choice to see how many passwords have those strings in them.

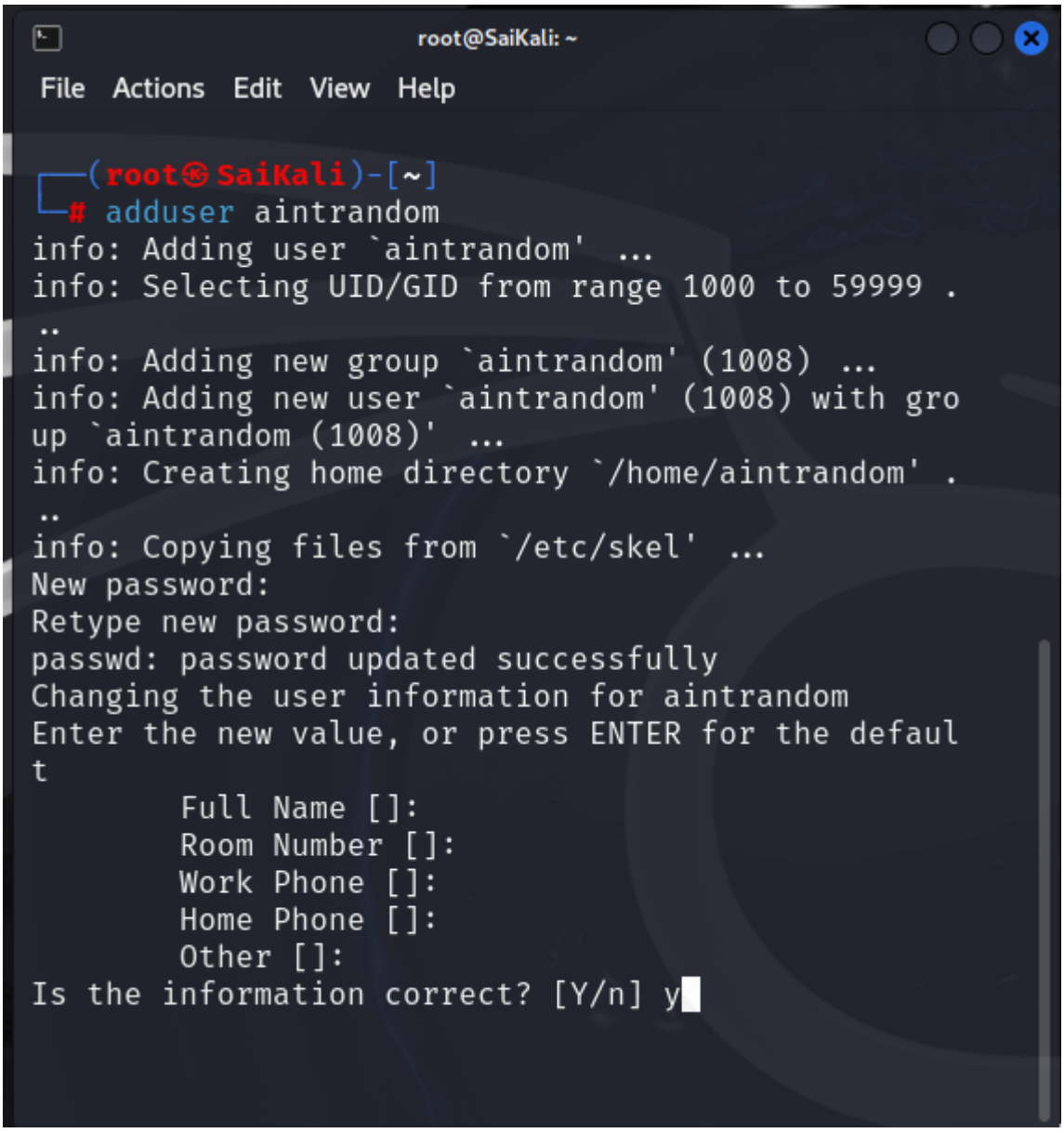


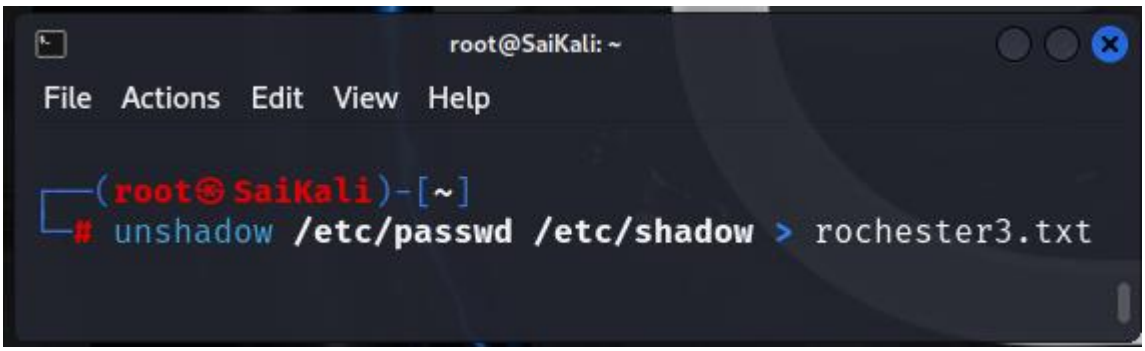

root@SaiKali: ~
File Actions Edit View Help
(root㉿SaiKali)-[~]
cat rockyou.txt | grep linux
linux
linuxx
linux1
linux80
linux123
linuxer
linux12
sunlinux
redhatlinux
mandrivalinux
linuxtux
linuxs
linuxmint
linuxinside
linuxi
linuxe
linuxBABA
linux911
linux7
linux34s
linux22
linux2006
linux2004
linux13
linux12345
bvalinux2007
worldlinux
trancelinux


root@SaiKali: ~
File Actions Edit View Help
(root㉿SaiKali)-[~]
cat rockyou.txt | grep lol
lollipop
lollypop
lolita
lolipop
lollol
lol123
lololo
lollies
lolly
lollipop1
lollie
lollypop1
lolliepop
lola123
lollipops
lolalola
lolol
lollypops
lolypop
lolito
lalola
lola
lol
damilola
lolada
lol101
lollollol
lolololo

j) Generate two more users with passwords that are more complex than the ones used in this lab exercise so far and make a new unshadow file called rochester3.txt.




root@SaiKali: ~
File Actions Edit View Help
┌──(root㉿SaiKali)-[~]
└─# adduser aintrandom
info: Adding user `aintrandom' ...
info: Selecting UID/GID from range 1000 to 59999 .
..
info: Adding new group `aintrandom' (1008) ...
info: Adding new user `aintrandom' (1008) with gro
up `aintrandom (1008)' ...
info: Creating home directory `/home/aintrandom' .
..
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for aintrandom
Enter the new value, or press ENTER for the defaul
t
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y


root@SaiKali: ~
File Actions Edit View Help
┌──(root㉿SaiKali)-[~]
└─# unshadow /etc/passwd /etc/shadow > rochester3.txt

k) **sudo john --wordlist=rockyou.txt --format=crypt rochester3.txt**