

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:	<ul style="list-style-type: none"> • 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.

```
Home saiprasad@SaiKali: /  
File Actions Edit View Help  
  
└─(saiprasad@SaiKali)-[/]  
└─$ sudo john  
[sudo] password for saiprasad:  
Created directory: /root/.john  
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]  
Copyright (c) 1996-2021 by Solar Designer and others  
Homepage: https://www.openwall.com/john/  
  
Usage: john [OPTIONS] [PASSWORD-FILES]  
  
Use --help to list all available options.  
  
└─(saiprasad@SaiKali)-[/]  
└─$ =[]
```

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

man john

```

saiprasad@SaiKali: / 
File Actions Edit View Help
JOHN(8) System Manager's Manual JOHN(8)
NAME
john - a tool to find weak passwords of your users

SYNOPSIS
john [options] password-files

DESCRIPTION
This manual page documents briefly the john command. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. john, better known as John the Ripper, is a tool to find weak passwords of users in a server. John can use a dictionary or some search pattern as well as a password file to check for passwords. John supports different cracking modes and understands many ciphertext formats, like several DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows NT passwords.

USAGE
To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental". Once John finds a password, it will be printed to the terminal and saved into a file called ~/.john/john.pot. John will read this file when it restarts so it doesn't try to crack already done passwords.

To see the cracked passwords, use
john -show passwd

Important: do this under the same directory where the password was cracked (when using the cronjob, /var/lib/john), otherwise it won't work.

While cracking, you can press any key for status, or Ctrl+C to abort the session, saving point information to a file (~/.john/john.rec by default). By the way, if you press Ctrl+C twice John will abort immediately without saving. The point information is also saved every 10 minutes (configurable in the configuration file, ~/.john/john.ini or ~/.john/john.conf) in case of a crash.

To continue an interrupted session, run:
john -restore

Now, you may notice that many accounts have a disabled shell, you can make John ignore these (assume that shell is called /etc/expired):
john -show -shells:-/etc/expired passwd

You might want to mail all the users who got weak passwords, to tell them to change the passwords. It's not always a good idea though (unfortunately, lots of people seem to ignore such mail, it can be used as a hint for crackers, etc), but anyway, I'll assume you know what you're doing. Get a copy of the 'mailer' script supplied with John, so you won't change anything that's under /usr/sbin; edit the message it sends, and possibly the mail command inside it (especially if the password file is from a different box than you got John running on). Then run:
./mailer passwd

Manual page john(8) line 1/189 29% (press h for help or q to quit)

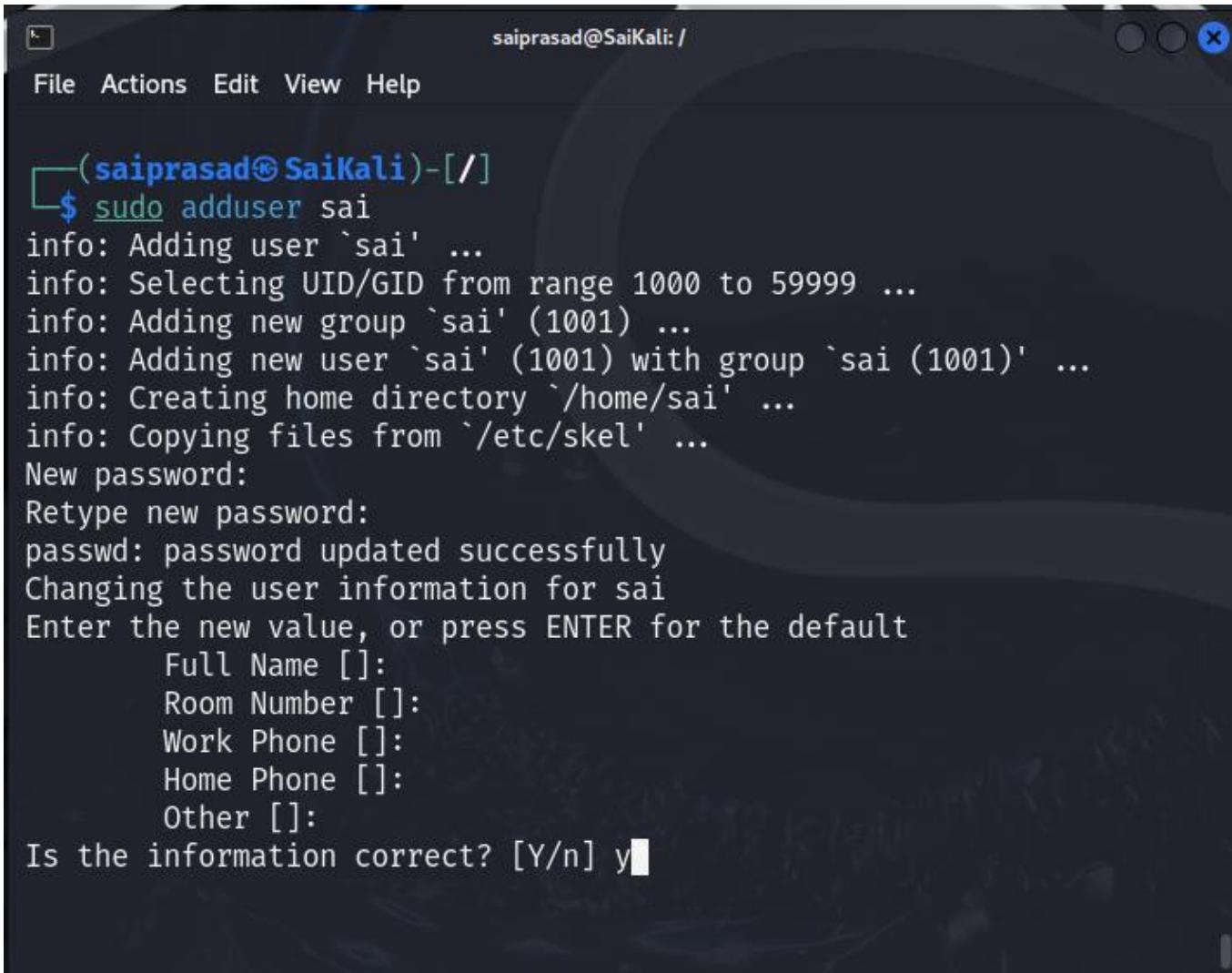
```

- 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

```
saiprasad@SaiKali: /  
File Actions Edit View Help  
└─(saiprasad@SaiKali)-[ /]  
$ sudo john --test  
Will run 2 OpenMP threads  
Benchmarking: decrypt, traditional crypt(3) [DES 256/256 AVX2] ... (2xOMP) DONE  
Many salts: 26431K c/s real, 13315K c/s virtual  
Only one salt: 23261K c/s real, 11748K c/s virtual  
  
Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 256/256 AVX2] ... (2xOMP) DONE  
Speed for cost 1 (iteration count) of 725  
Many salts: 867852 c/s real, 440501 c/s virtual  
Only one salt: 817152 c/s real, 412703 c/s virtual  
  
Benchmarking: md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3] ... (2xOMP) DONE  
Many salts: 204000 c/s real, 102770 c/s virtual  
Only one salt: 206805 c/s real, 104969 c/s virtual  
  
Benchmarking: md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64] ... (2xOMP) DONE  
Raw: 22584 c/s real, 11406 c/s virtual  
  
Benchmarking: bcrypt ("$2a$05", 32 iterations) [Blowfish 32/64 X3] ... (2xOMP) DONE  
Speed for cost 1 (iteration count) of 32  
Raw: 3285 c/s real, 1663 c/s virtual  
  
Benchmarking: scrypt (16384, 8, 1) [Salsa20/8 128/128 AVX] ... (2xOMP) DONE  
Speed for cost 1 (N) of 16384, cost 2 (r) of 8, cost 3 (p) of 1  
Raw: 97.0 c/s real, 48.9 c/s virtual  
  
Benchmarking: LM [DES 256/256 AVX2] ... (2xOMP) DONE  
Raw: 142491K c/s real, 72147K c/s virtual  
  
Benchmarking: AFS, Kerberos AFS [DES 48/64 4K] ... DONE  
Short: 685824 c/s real, 689270 c/s virtual  
Long: 685824 c/s real, 685824 c/s virtual  
  
Benchmarking: tripcode [DES 256/256 AVX2] ... (2xOMP) ^CWait...  
Session aborted  
└─(saiprasad@SaiKali)-[ /]
```

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



```
saiprasad@SaiKali: /  
File Actions Edit View Help  
└─(saiprasad@SaiKali)-[ /]  
$ sudo adduser sai  
info: Adding user `sai' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `sai' (1001) ...  
info: Adding new user `sai' (1001) with group `sai (1001)' ...  
info: Creating home directory `/home/sai' ...  
info: Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for sai  
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
```

- 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 `sai' to group `users' ...

[saiprasad@SaiKali ~] $ sudo adduser upper
info: Adding user `upper' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `upper' (1002) ...
info: Adding new user `upper' (1002) with group `upper (1002)' ...
info: Creating home directory `/home/upper' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for upper
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 `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█
```

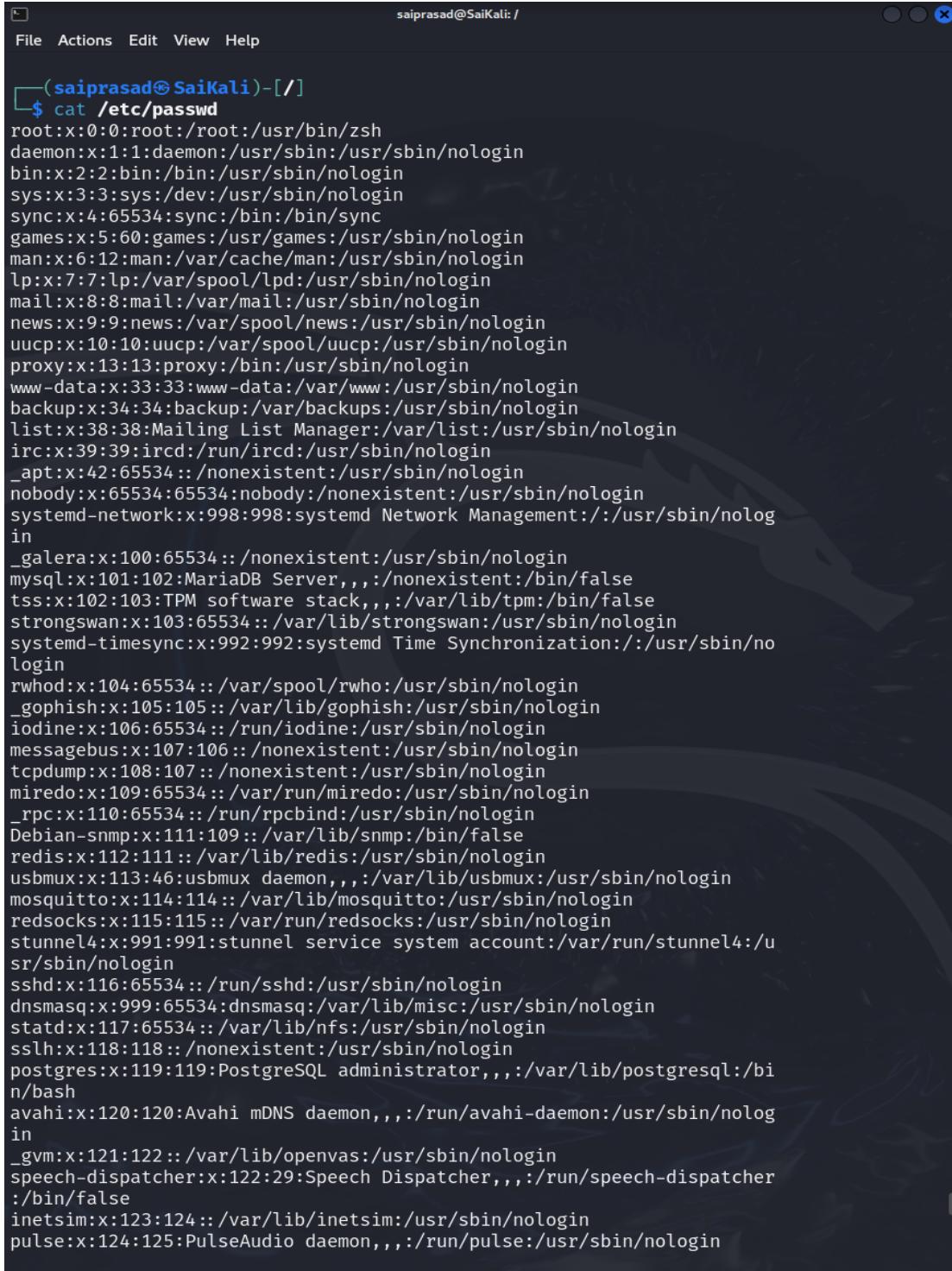
```
saiprasad@SaiKali: /  
File Actions Edit View Help  
..  
info: Adding user `lower' to group `users' ...  
  
[saiprasad@SaiKali ~]$ sudo adduser mixed  
info: Adding user `mixed' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `mixed' (1004) ...  
info: Adding 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█
```

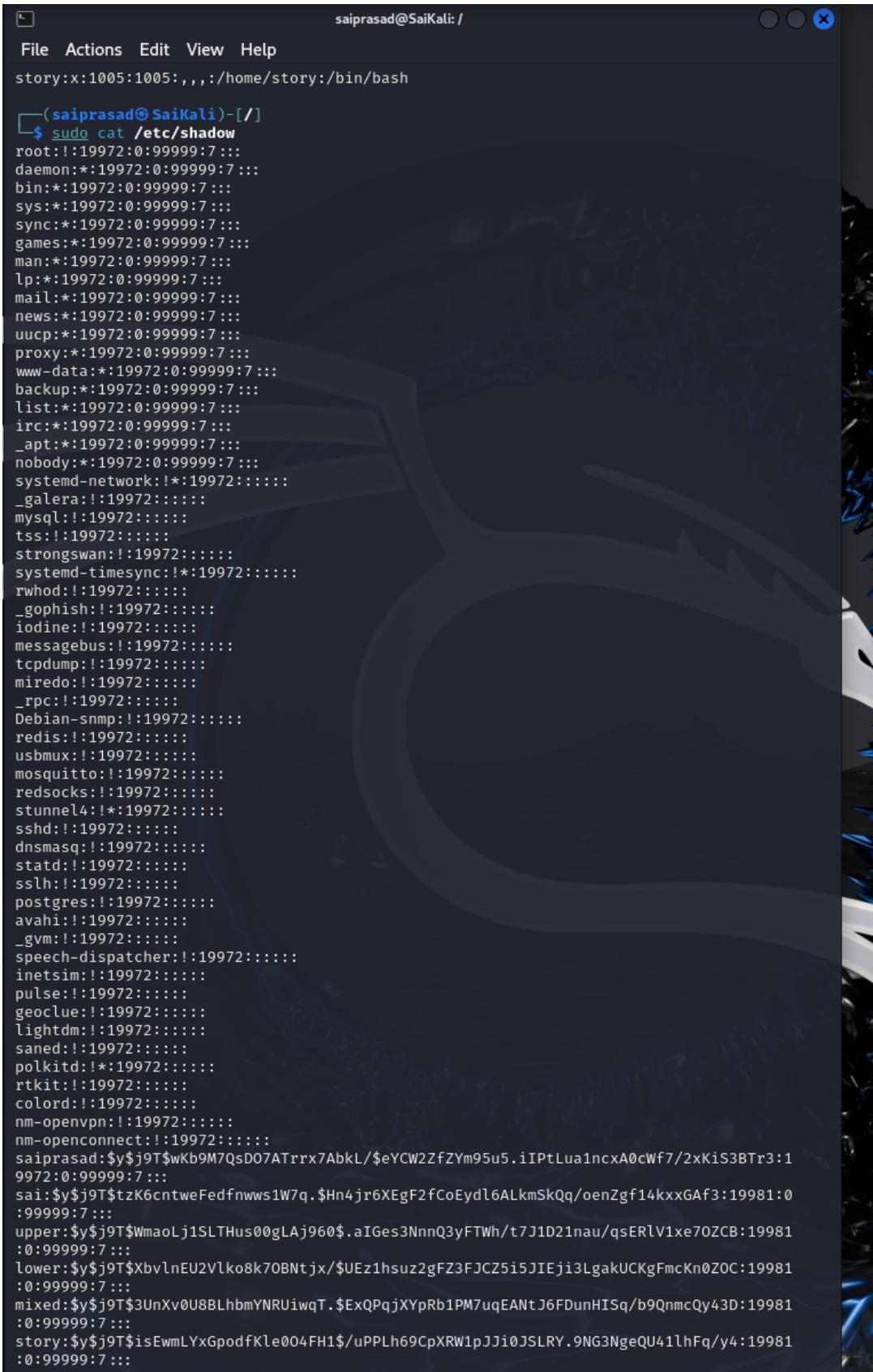
- f) Explore the /etc/passwd and /etc/shadow files with the cat command

cat /etc/passwd

sudo cat /etc/shadow



```
(saiprasad@saiKali)-[~]
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
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:/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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_in
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/no
login
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:105:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:106:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:107:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:108:107::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:110:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:111:109::/var/lib/snmp:/bin/false
redis:x:112:111::/var/lib/redis:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:114:114::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:115:115::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/u
sr/sbin/nologin
sshd:x:116:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
sslh:x:118:118::/nonexistent:/usr/sbin/nologin
postgres:x:119:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bi
n/bash
avahi:x:120:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nolog
in
_gvm:x:121:122::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:122:29:Speech Dispatcher,,,:/run/speech-dispatcher
:/bin/false
inetsim:x:123:124::/var/lib/inetsim:/usr/sbin/nologin
pulse:x:124:125:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
```



```

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:$y$j9T$wKb9M7QsD07ATrrx7AbkL/$eYCwZfZYm95u5.iIPtLua1ncxA0cWf7/2xKiS3BTr3:1
9972:0:99999:7:::
sai:$y$j9T$tzK6cntweFedfnwws1W7q.$Hn4jr6X EgF2fCoEydl6ALkmSkQq/oenZgf14kxxGaf3:19981:0
:99999:7:::
upper:$y$j9T$WmaoLj1SLTHus00gLAj960$.aIGes3NnnQ3yFTWh/t7J1D21nau/qsERlV1xe70ZCB:19981
:0:99999:7:::
lower:$y$j9T$XbvlnEU2Vlko8k70BNtjx/$UEz1hsuz2gFZ3FJCZ5i5JIEji3LgakUCKgFmcKn0ZOC:19981
:0:99999:7:::
mixed:$y$j9T$3UnXv0U8BLhbhYNRUiwqT.$ExQPqjXYpRb1PM7uqEANtJ6FDunHISq/b9QnmcQy43D:19981
:0:99999:7:::
story:$y$j9T$isEwmLYxGpodfKle004FH1$/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.

File Actions Edit View Help

UNSHADOW(8) System Manager's Manual UNSHADOW(8)

NAME
unshadow - combines passwd and shadow files

SYNOPSIS
unshadow *password-file* *shadow-file*

DESCRIPTION
This manual page documents briefly the **unshadow** command, which is part of the **john** package. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. **john**, better known as John the Ripper, is a tool to find weak passwords of users in a server.

The **unshadow** tool combines the *passwd* and *shadow* files so **John** can use them. You might need this since if you only used your *shadow* file, the GECOS information wouldn't be used by the "single crack" mode, and also you wouldn't be able to use the '-shells' option. On a normal system you'll need to run **unshadow** as root to be able to read the *shadow* file.

SEE ALSO
john(8), **mailer**(8), **unafs**(8), **unique**(8).

The programs are documented fully by **John**'s documentation, which should be available in */usr/share/doc/john* or other location, depending on your system.

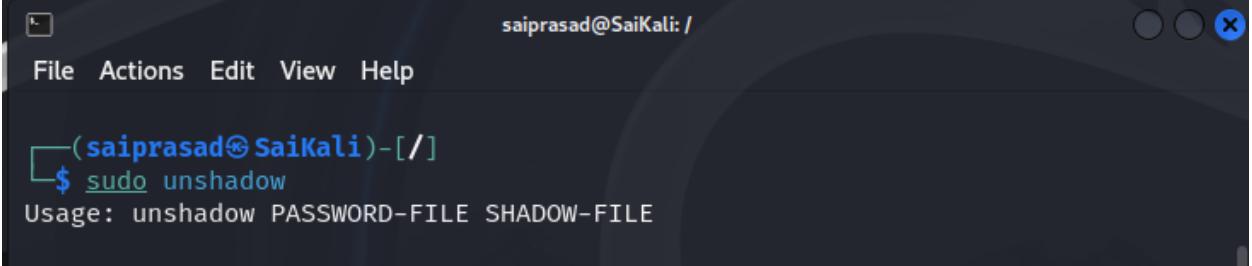
AUTHOR
This manual page was written by Jordi Mallach <jordi@debian.org>, for the Debian GNU/Linux system (but may be used by others).
John the Ripper and **mailer** were written by Solar Designer <solar@openwall.com>. The complete list of contributors can be found in the CREDITS file in the documentation directory.

john June 03, 2004 UNSHADOW(8)

Manual page unshadow(8) line 1/34 (END) (press h for help or q to quit) █

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

sudo unshadow

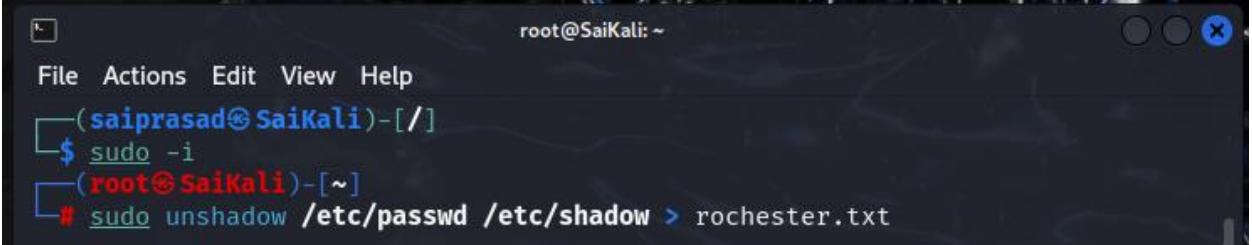


```
saiprasad@SaiKali: /  
File Actions Edit View Help  
└─(saiprasad@SaiKali)-[ ]  
└─$ sudo unshadow  
Usage: unshadow PASSWORD-FILE SHADOW-FILE
```

A screenshot of a terminal window titled "saiprasad@SaiKali: /". The window has a dark theme with white text. The title bar shows the user's name and the host. Below the title bar is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal shows a command prompt "(saiprasad@SaiKali)-[]". The user has typed "sudo unshadow" and is seeing the usage information for the command.

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



```
root@SaiKali: ~  
File Actions Edit View Help  
└─(saiprasad@SaiKali)-[ ]  
└─$ sudo -i  
└─(root@SaiKali)-[~]  
└─# sudo unshadow /etc/passwd /etc/shadow > rochester.txt
```

A screenshot of a terminal window titled "root@SaiKali: ~". The window has a dark theme with white text. The title bar shows the user's name and the host. Below the title bar is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal shows a command prompt "(root@SaiKali)-[~]". The user has typed "# sudo unshadow /etc/passwd /etc/shadow > rochester.txt" and is executing the command.

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

cat rochester.txt

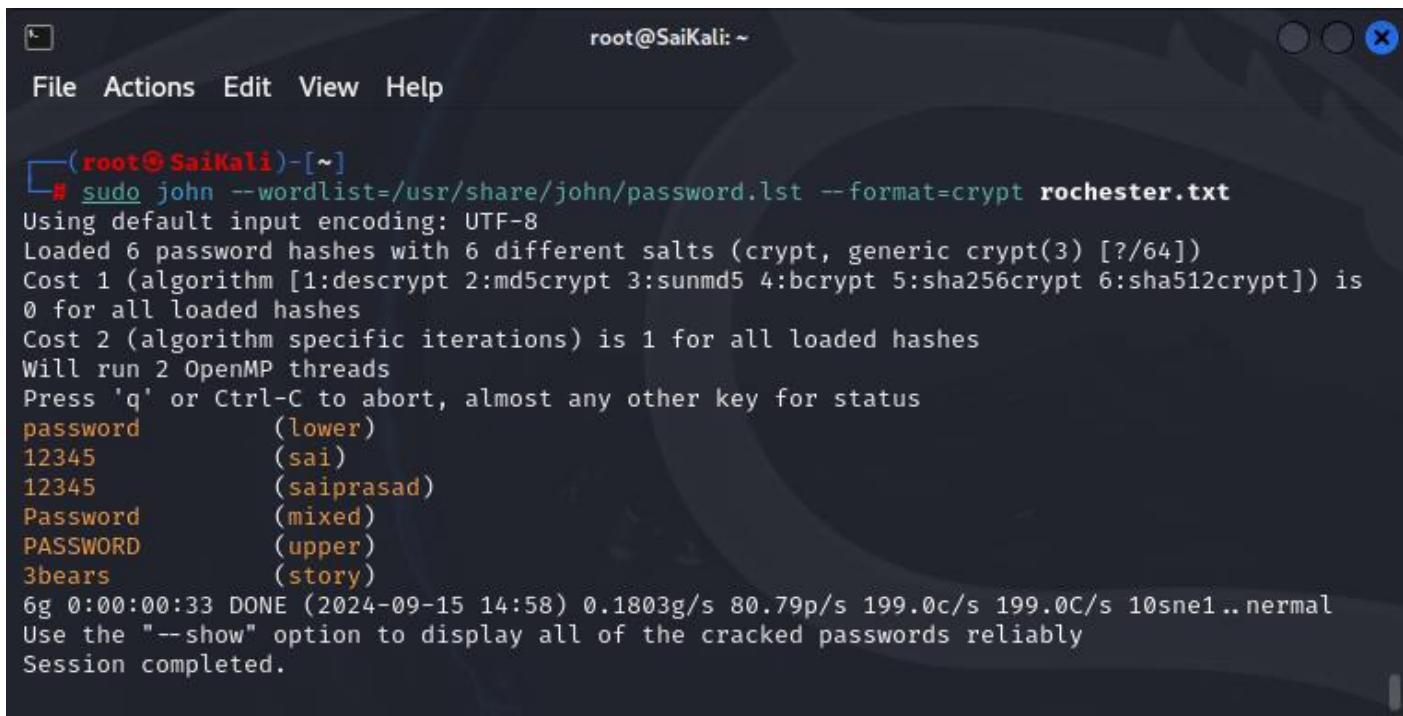
```
root@SaiKali:~#
File Actions Edit View Help
[root@SaiKali] ~
# cat rochester.txt
root::!:0:0:root:/root:/usr/bin/zsh
daemon:*:1::daemon:/usr/sbin:/usr/sbin/nologin
bin::2::bin:/bin:/usr/sbin/nologin
sys::3::sys:/dev:/usr/sbin/nologin
sync::4:65534::sync:/bin.sync
games::5:60:games:/usr/games:/usr/sbin/nologin
man::6:12:man:/var/cache/man:/usr/sbin/nologin
lp::7:lp:/var/spool/lpd:/usr/sbin/nologin
mail::8:8:mail:/var/mail:/usr/sbin/nologin
news::9:9:news:/var/spool/news:/usr/sbin/nologin
uucp::10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy::13:13:proxy:/bin:/usr/sbin/nologin
www-data::33:33:www-data:/var/www:/usr/sbin/nologin
backup::34:34:backup:/var/backups:/usr/sbin/nologin
list::38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc::39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt::42:65534::/nonexistent:/usr/sbin/nologin
nobody::65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network::998:998:systemd Network Management:/usr/sbin/nologin
_galera::100:65534::/nonexistent:/usr/sbin/nologin
mysql::101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss::102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan::103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync::992:992:systemd Time Synchronization:/usr/sbin/nologin
rwhod::104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish::105:105::/var/lib/gophish:/usr/sbin/nologin
iodine::106:65534::/run/iodine:/usr/sbin/nologin
messagebus::107:106::/nonexistent:/usr/sbin/nologin
tcpdump::108:107::/nonexistent:/usr/sbin/nologin
miredo::109:65534::/var/run/miredo:/usr/sbin/nologin
_rpc::110:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp::111:109::/var/lib/snmp:/bin/false
redis::112:111::/var/lib/redis:/usr/sbin/nologin
usbmux::113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto::114:114::/var/lib/mosquitto:/usr/sbin/nologin
redsocks::115:115::/var/run/redsocks:/usr/sbin/nologin
stunnel4::991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin
/nologin
sshd::116:65534::/run/sshd:/usr/sbin/nologin
dnsmasq::999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
statd::117:65534::/var/lib/nfs:/usr/sbin/nologin
sslh::118:118::/nonexistent:/usr/sbin/nologin
postgres::119:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi::120:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
_gvm::121:122::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher::122:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/fa
lse
inetsim::123:124::/var/lib/inetsim:/usr/sbin/nologin
pulse::124:125:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
geoclue::125:127::/var/lib/geoclue:/usr/sbin/nologin
lightdm::126:128:Light Display Manager:/var/lib/lightdm:/bin/false
saned::127:130::/var/lib/saned:/usr/sbin/nologin
polkitd::989:989:User for polkitd::/usr/sbin/nologin
rtkit::128:131:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord::129:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin
/nologin
nm-openvpn::130:133:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sb
in/nologin
nm-openconnect::131:134:NetworkManager OpenConnect plugin,,,:/var/lib/Network
Manager:/usr/sbin/nologin
saiprasad:$j9T$wKb9M7qsD07ATrrx7AbkL$/eYCW2ZfZYm95u5.iIPtLua1ncxA0cWf7/2xKiS
3BTr3:1000:1000:Saiprasad Raman,,,:/home/saiprasad:/usr/bin/zsh
sai:$y$j9T$tzK6cntweFedfnwzs1W7q.$Hn4jr6xEgF2fCoEydl6ALkmSkQq/oenZgf14kxxGAF3:
1001:1001:,,,,:/home/sai:/bin/bash
upper:$y$j9T$WmaoLj1SLThus00gLAj960$.aIGes3NnnQ3yFTWh/t7J1D21nau/qzERlV1xe70ZC
B:1002:1002:,,,,:/home/upper:/bin/bash
lower:$y$j9T$XbvlxEU2Vlk08k7OBNtjx/$UEz1hsuz2gFZ3FJCZ5i5JIEji3LgakUCKgFmcKn0ZO
C:1003:1003:,,,,:/home/lower:/bin/bash
mixed:$y$j9T$3UnXv0U8BLhbhYNRUiwqT.$ExQPqjXYpRb1PM7uqEANtJ6FDunHISq/b9QnmcQy43
D:1004:1004:,,,,:/home/mixed:/bin/bash
story:$y$j9T$isEwmLYxGpofKle004FH1$/uPPLh69CpXRW1pJJi0JSLRY.9NG3NgeQU41lhFq/y
4:1005:1005:,,,,:/home/story:/bin/bash
```

- 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
```

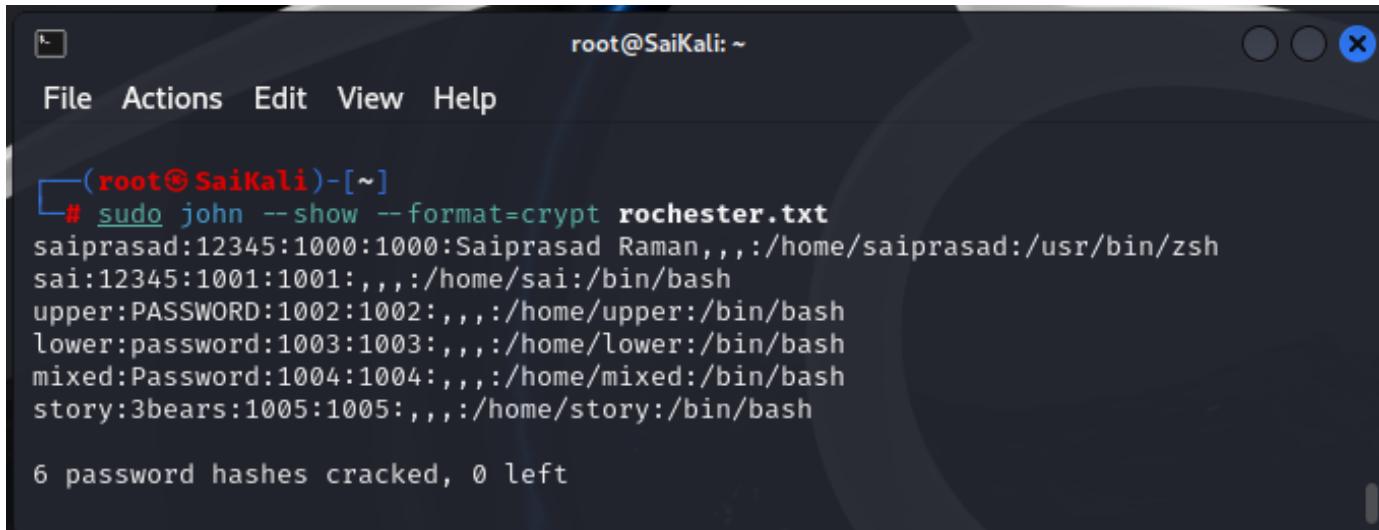
At the point of cracking, the passwords and usernames appear on the screen.

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



```
root@SaiKali: ~
File Actions Edit View Help
root@SaiKali:[~]
# sudo john --wordlist=/usr/share/john/password.lst --format=crypt rochester.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 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
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (lower)
12345        (sai)
12345        (saiprasad)
Password      (mixed)
PASSWORD      (upper)
3bears        (story)
6g 0:00:00:33 DONE (2024-09-15 14:58) 0.1803g/s 80.79p/s 199.0c/s 199.0C/s 10sne1..nrmal
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

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



```
root@SaiKali: ~
File Actions Edit View Help

└─(root@SaiKali)-[~]
  └─# sudo john --show --format=crypt rochester.txt
saiprasad:12345:1000:1000:Saiprasad Raman,,,,:/home/saiprasad:/usr/bin/zsh
sai:12345:1001:1001,,,,:/home/sai:/bin/bash
upper:PASSWORD:1002:1002:,,,,:/home/upper:/bin/bash
lower:password:1003:1003:,,,,:/home/lower:/bin/bash
mixed:Password:1004:1004:,,,,:/home/mixed:/bin/bash
story:3bears:1005:1005:,,,,:/home/story:/bin/bash

6 password hashes cracked, 0 left
```

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



```
root@SaiKali: ~
File Actions Edit View Help

└─(root@SaiKali)-[~]
  └─# rm /root/.john/john.pot
```

n) Create a new user called scott:

```
sudo adduser scott
```

```
saiprasad@SaiKali: /root
File Actions Edit View Help
└$ sudo adduser scott
[sudo] password for saiprasad:
info: Adding user `scott' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `scott' (1006) ...
info: Adding new user `scott' (1006) with group `scott (1006)' ...
info: Creating home directory `/home/scott' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for scott
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []: 10314
    Work Phone []: ^Cfatal: `/bin/chfn scott' exited from signal 2.
Exiting.
```

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

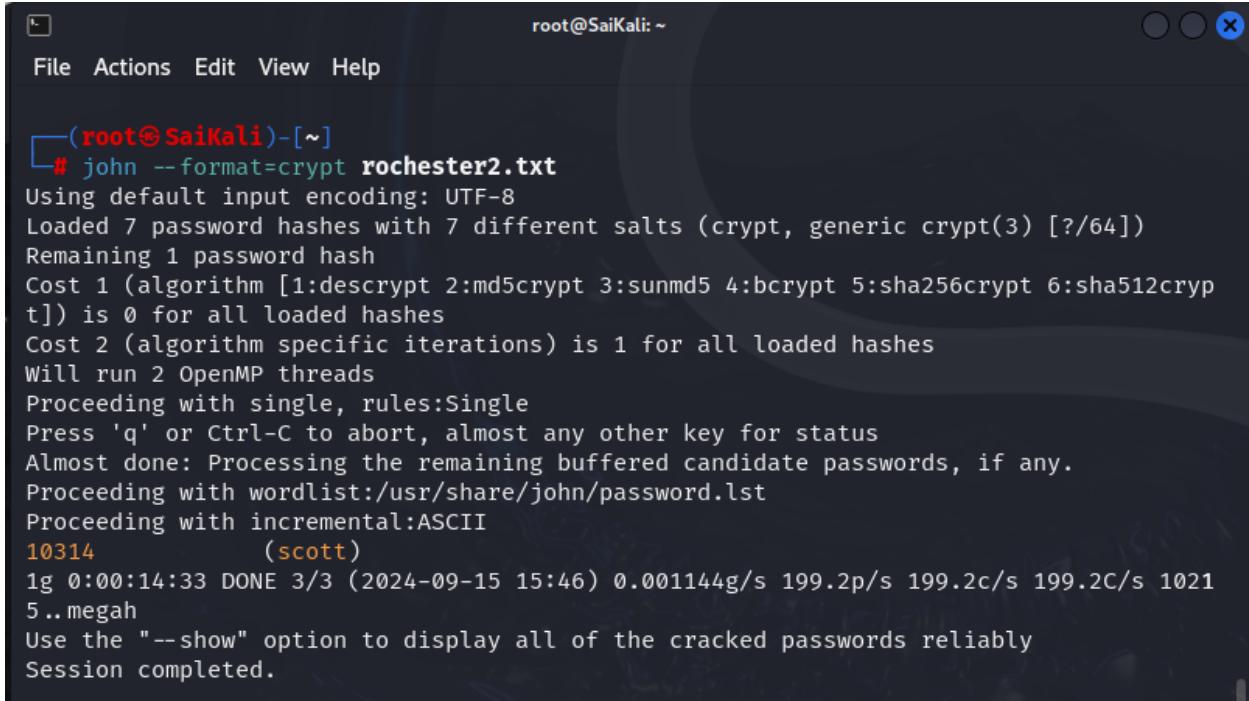
```
sudo unshadow /etc/passwd /etc/shadow > rochester2.txt
```



```
root@SaiKali: ~
File Actions Edit View Help
└─(root@SaiKali)-[~]
  # unshadow /etc/passwd /etc/shadow > rochester2.txt
└─(root@SaiKali)-[~]
  #
```

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

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

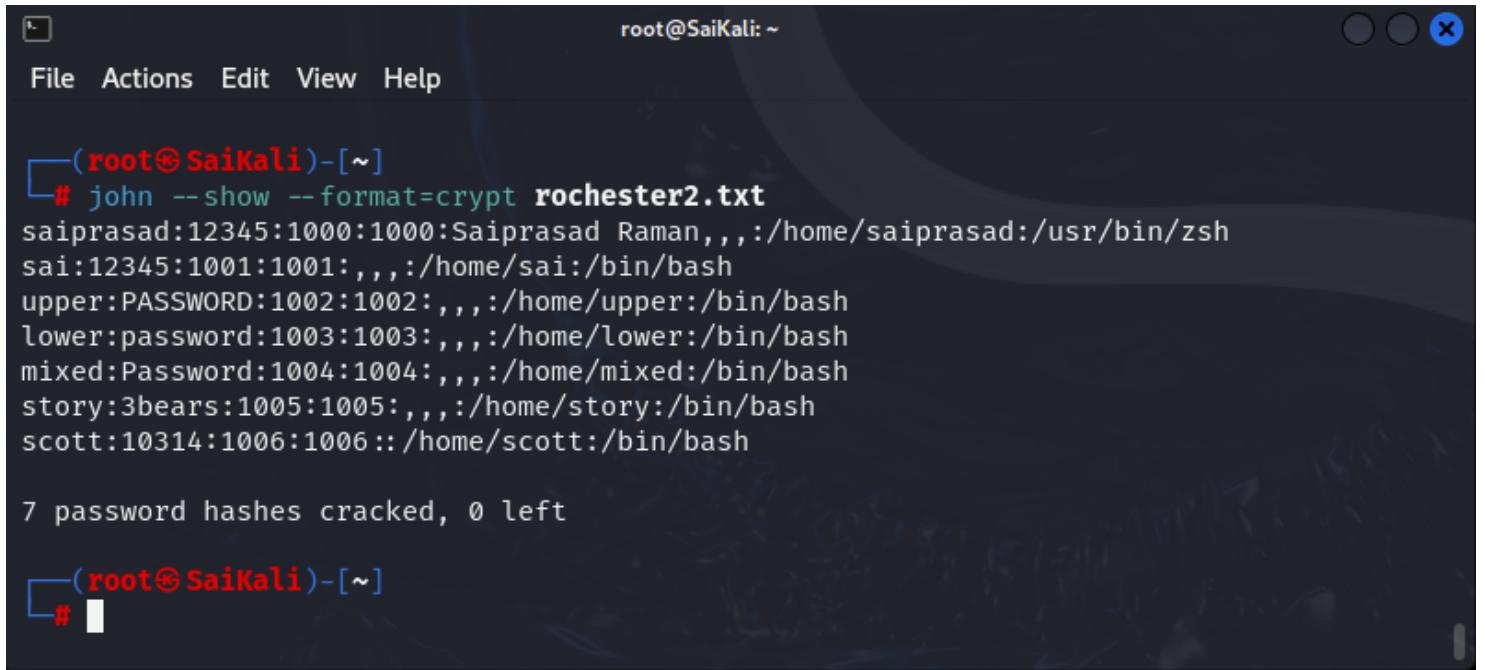


```
root@SaiKali: ~
File Actions Edit View Help
└─(root@SaiKali)-[~]
  # john --format=crypt rochester2.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
10314          (scott)
1g 0:00:14:33 DONE 3/3 (2024-09-15 15:46) 0.001144g/s 199.2p/s 199.2c/s 199.2C/s 1021
5..megah
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- 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.**



The screenshot shows a terminal window with the following content:

```
root@SaiKali: ~
File Actions Edit View Help
└──(root@SaiKali)-[~]
# john --show --format=crypt rochester2.txt
saiprasad:12345:1000:1000:Saiprasad Raman,,,,:/home/saiprasad:/usr/bin/zsh
sai:12345:1001:1001:,,,,:/home/sai:/bin/bash
upper:PASSWORD:1002:1002:,,,,:/home/upper:/bin/bash
lower:password:1003:1003:,,,,:/home/lower:/bin/bash
mixed:Password:1004:1004:,,,,:/home/mixed:/bin/bash
story:3bears:1005:1005:,,,,:/home/story:/bin/bash
scott:10314:1006:1006::/home/scott:/bin/bash

7 password hashes cracked, 0 left

└──(root@SaiKali)-[~]
#
```

- 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 .
```



A terminal window titled "root@SaiKali: ~". The command "cp /home/saiprasad/Downloads/rockyou.txt.tar.gz ." is entered and executed.

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

```
gzip -d rockyou.txt.gz
```

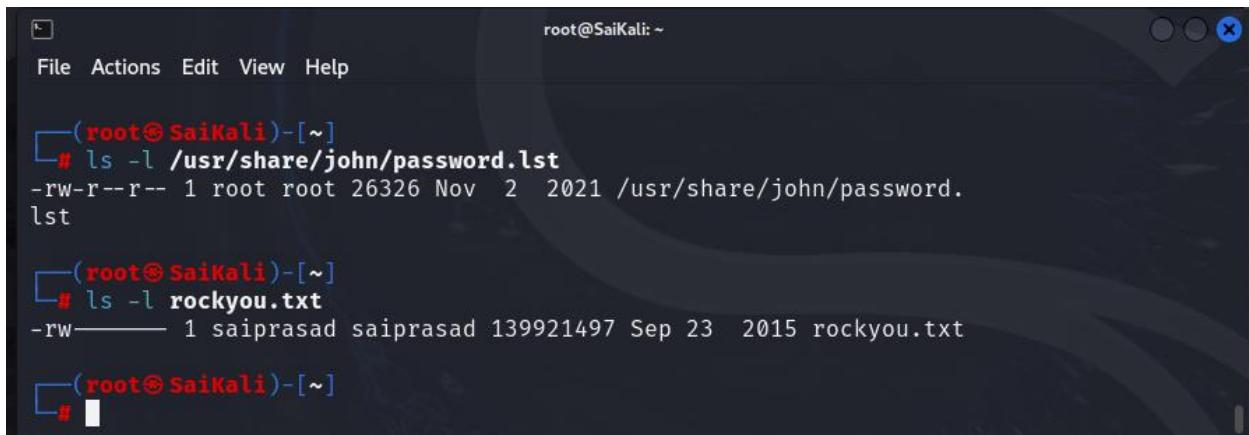


A terminal window titled "root@SaiKali: ~". The command "gzip -d rockyou.txt.tar.gz" is entered and executed.

- 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
```



A terminal window titled "root@SaiKali: ~". It shows two "ls -l" commands. The first command lists "/usr/share/john/password.lst" with a size of 26326 bytes. The second command lists "rockyou.txt" with a size of 139921497 bytes.

- 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.

```
root@SaiKali:~ Compressed Uncompressed Date Notes
File Actions Edit View Help
Rockyou rockyou.txt.bz2 n/a 2009-12 Best list
available; huge,
stolen
unencrypted
[root@SaiKali) ~] # apt install leafpad
Installing:
leafpad
Suggested packages:
evince-gtk
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 922
Download size: 90.9 kB
Space needed: 465 kB / 4643 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 1s (171 kB/s)
Selecting previously unselected package leafpad.
(Reading database ... 391053 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
update-alternatives: using /usr/bin/leafpad to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...

[root@SaiKali) ~] #
```

- 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)-[~]
# cat /usr/share/john/password.lst
#!/comment: This list has been compiled by Solar Designer of Openwall Project
#!/comment: in 1996 through 2011. It is assumed to be in the public domain.
#!/comment:
#!/comment: This list is based on passwords most commonly seen on a set of Uni
X
#!/comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!/comment: (that is, more common passwords are listed first). It has been
#!/comment: revised to also include common website passwords from public lists
#!/comment: of "top N passwords" from major community website compromises that
#!/comment: occurred in 2006 through 2010.
#!/comment:
#!/comment: Last update: 2011/11/20 (3546 entries)
#!/comment:
#!/comment: For more wordlists, see https://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
you
tigger
1234
qwerty
money
carmen
carmen
mickey
secret
summer
internet
a1b2c3
123
service
canada
hello
phpbb
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang
snoopy
buster
dragon
jordan
michael
michelle
mindy
patrick

  Name      Compressed    Uncompressed   Date       Notes
abc123      rockyou.txt.bz2      n/a        2009-12  Best list
computer     rockyou-          n/a        2009-12  available: huge,
you           withcount.txt.bz2      (60,498,886 bytes)  stolen
tigger        rockyou-          n/a        2009-12  unencrypted
1234          rockyou-          n/a        2009-12
qwerty         rockyou-          n/a        2009-12
money          rockyou-          n/a        2009-12
carmen         rockyou-          n/a        2009-12
carmen         rockyou-          n/a        2009-12
mickey         rockyou-          n/a        2009-12
secret         rockyou-          n/a        2009-12
summer         rockyou-          n/a        2009-01  Ordered by
internet      rockyou-          n/a        2009-01  commonness)
a1b2c3        rockyou-          n/a        2009-01  Cracked from
123            rockyou-          n/a        2009-01  md5 by Brandon
service        rockyou-          n/a        2009-01  Enright (97%+
canada         rockyou-          n/a        2009-01  coverage)

  Name      Compressed    Uncompressed   Date       Notes
hello          phpbb-           n/a        2009-01
phpbb          phpbb-           n/a        2009-01
ranger         phpbb-           n/a        2009-01
shadow         phpbb-           n/a        2009-01
baseball       phpbb-           n/a        2009-01
donald         phpbb-           n/a        2009-01
harley         phpbb-           n/a        2009-01
hockey         phpbb-           n/a        2009-01
letmein        phpbb-           n/a        2009-01
maggie         phpbb-           n/a        2009-01
mike           phpbb-           n/a        2009-01
mustang        phpbb-           n/a        2009-01
snoopy         phpbb-           n/a        2009-01
buster         phpbb-           n/a        2009-01
dragon         phpbb-           n/a        2009-01
jordan         phpbb-           n/a        2009-01
michael        phpbb-           n/a        2009-01
michelle       phpbb-           n/a        2009-01
mindy          phpbb-           n/a        2009-01
patrick        phpbb-           n/a        2009-01

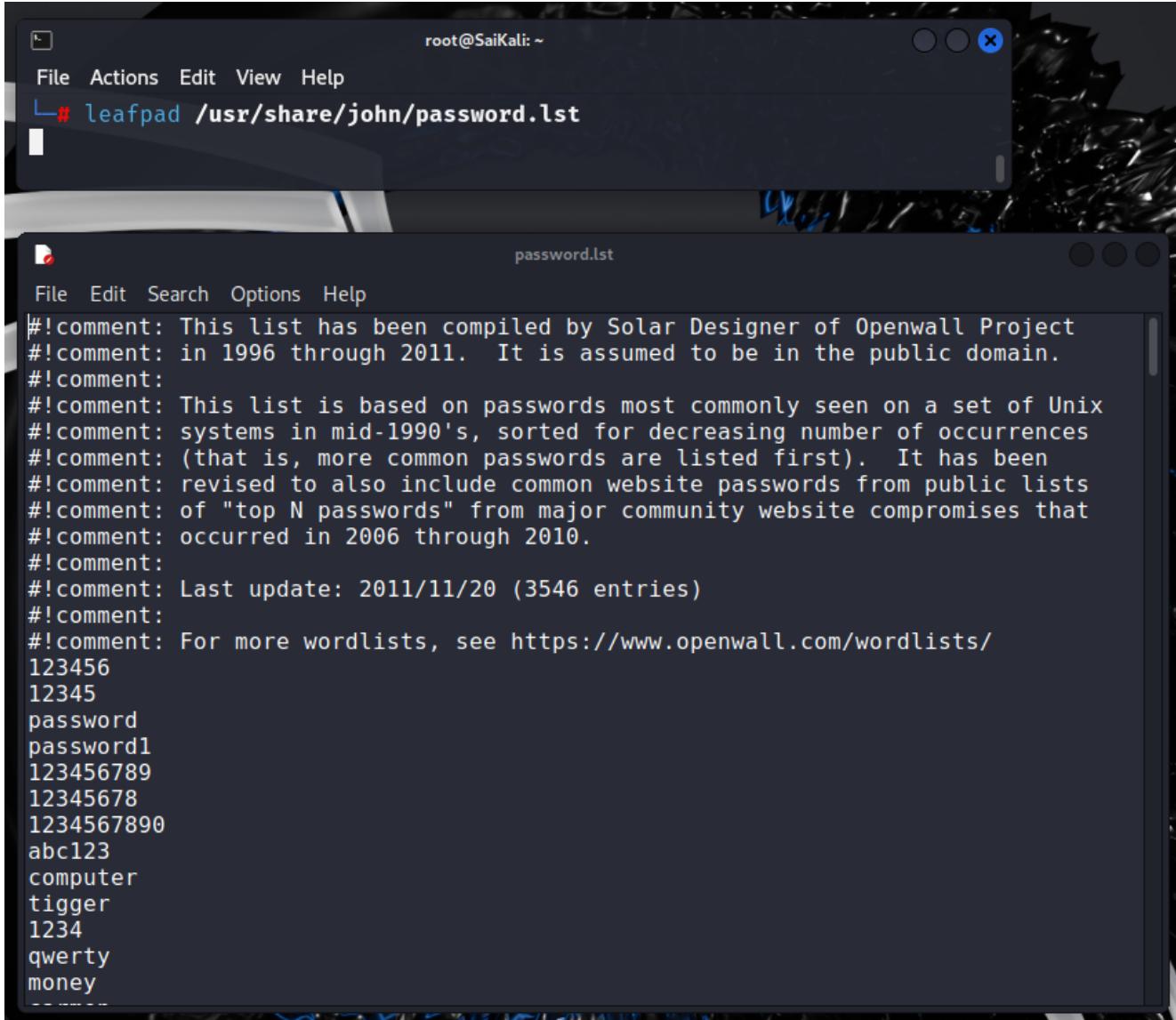
  Name      Compressed    Uncompressed   Date       Notes
canada         myspace.txt.bz2  n/a        2006-10  Captured via
maggie        myspace.txt.bz2  n/a        2006-10  eddieknee
mike          myspace.txt.bz2  n/a        2006-10
mustang        myspace.txt.bz2  n/a        2006-10
snoopy         myspace.txt.bz2  n/a        2006-10
buster         myspace.txt.bz2  n/a        2006-10
dragon         myspace.txt.bz2  n/a        2006-10
jordan         myspace.txt.bz2  n/a        2006-10
michael        myspace.txt.bz2  n/a        2006-10
michelle       myspace.txt.bz2  n/a        2006-10
mindy          myspace.txt.bz2  n/a        2006-10
patrick        myspace.txt.bz2  n/a        2006-10
```

```
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
michele
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

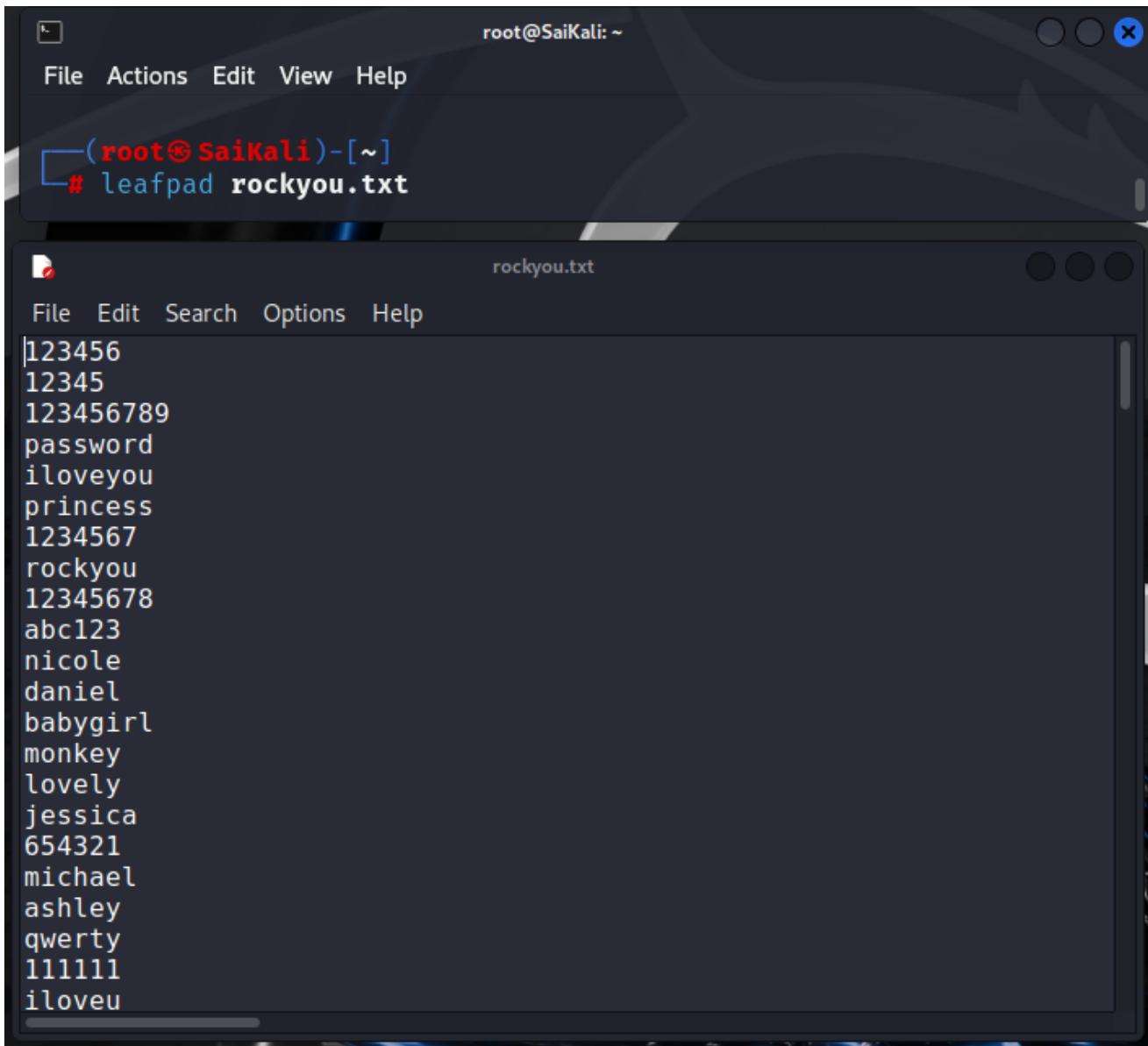


The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@SaiKali: ~". Inside the terminal, the command "leafpad /usr/share/john/password.lst" is run, and the output shows the contents of the password.lst file. The file contains various common passwords, starting with "123456" and "password".

```
root@SaiKali: ~
└# leafpad /usr/share/john/password.lst

File Edit Search Options Help
password.lst

File Edit Search Options Help
#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011. It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first). It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see https://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
```



root@SaiKali: ~

```
[root@SaiKali]# leafpad rockyou.txt
```

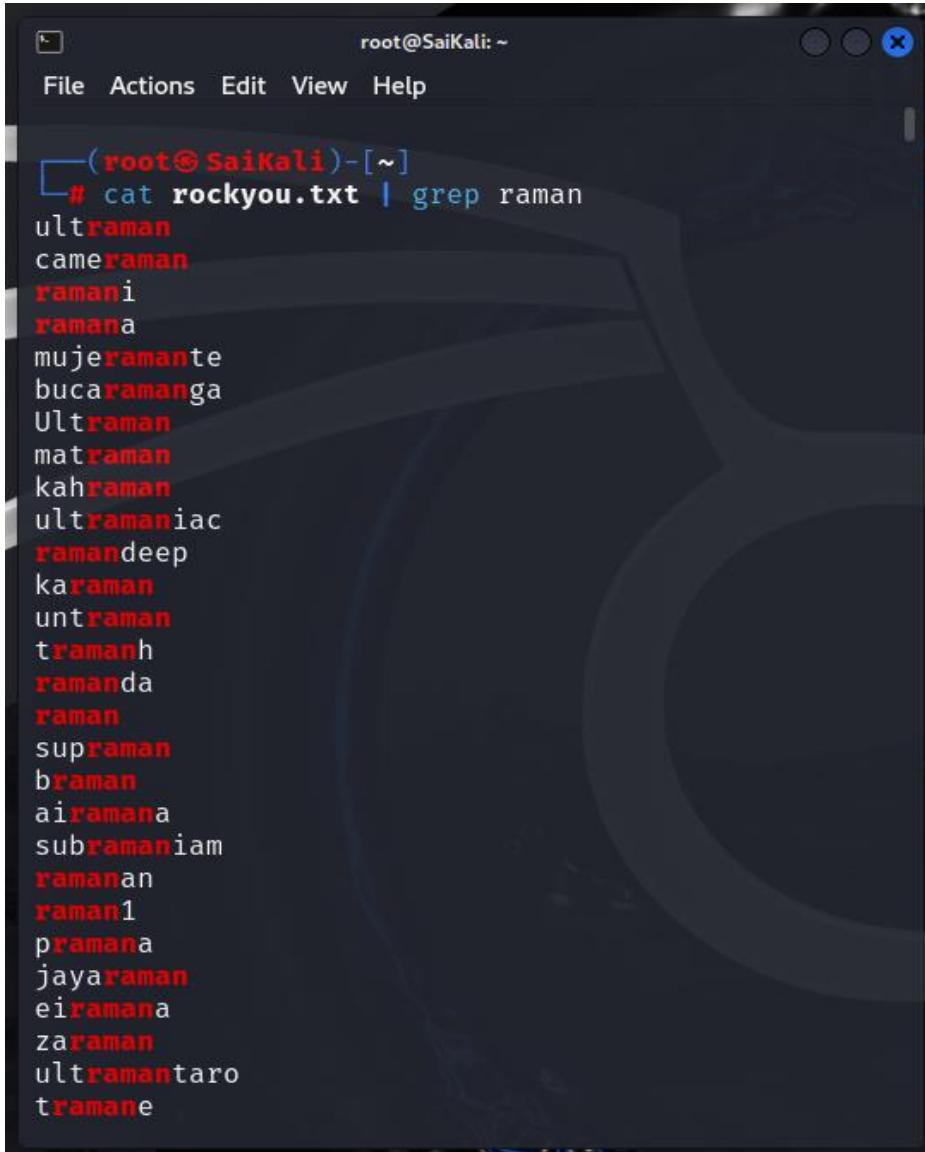
rockyou.txt

```
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
```



The terminal window shows the command `# cat rockyou.txt | grep raman` being run. The output lists numerous variations of the name "raman" in red text, indicating they were found in the file. Some words like "ultraman" and "raman" appear multiple times with different suffixes or prefixes.

```
[root@SaiKali ~]# cat rockyou.txt | grep raman
ultraman
cameraman
ramani
ramana
mujeramanante
bucaramanga
Ultraman
matraman
kahraman
ultramaniac
ramandeep
kazaman
untraman
tramanh
ramanda
raman
supraman
braman
airamana
subramaniam
ramanan
raman1
pramana
jayaraman
eiramana
zaraman
ultramantaro
tramane
```

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

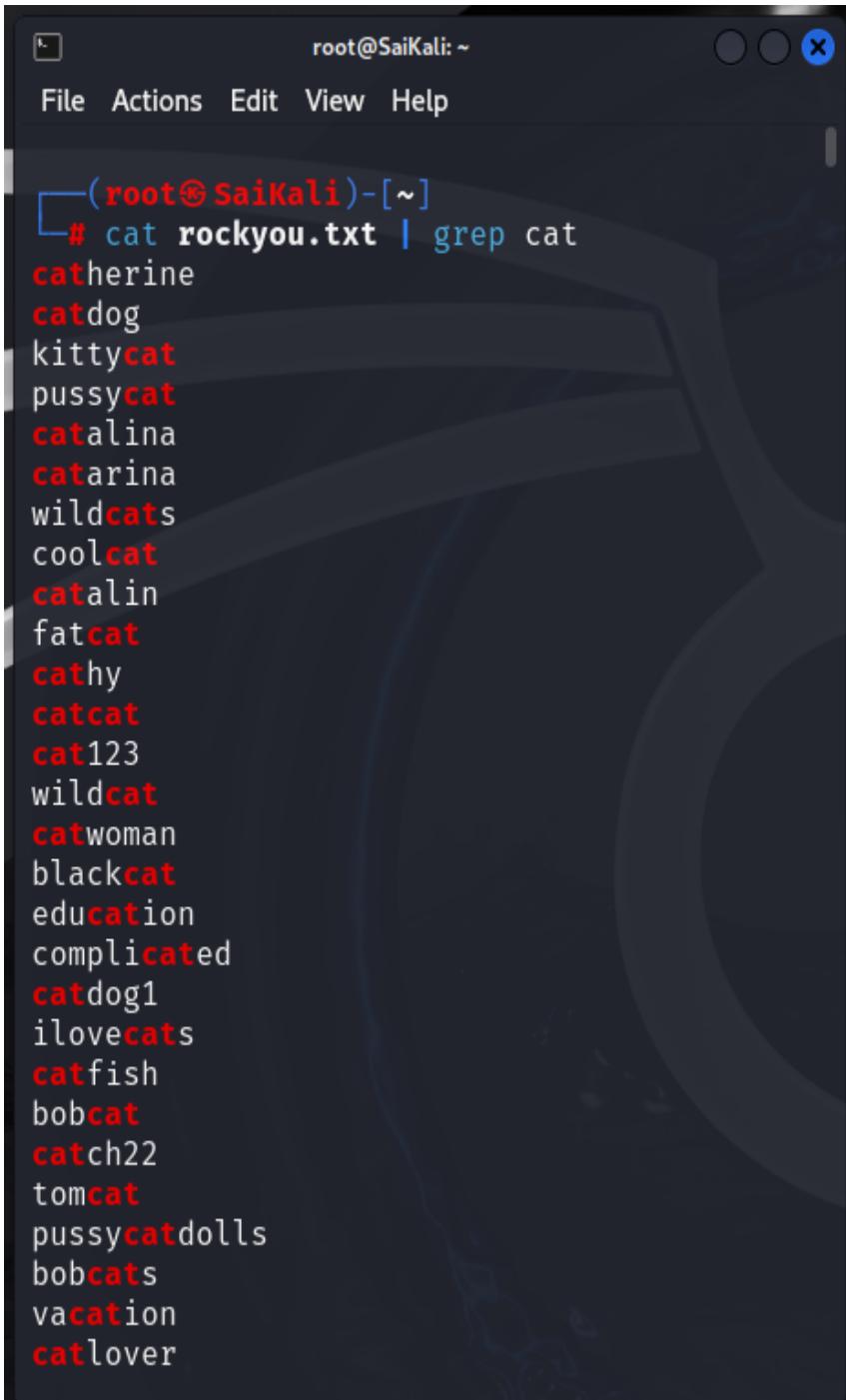
```
cat rockyou.txt | grep muhammad
```



The terminal window shows the command `cat rockyou.txt | grep sai` being run by root user on a Kali Linux system. The output lists numerous variations of the name 'sai' and other names containing 'sai'.

```
root@SaiKali: ~
└─# cat rockyou.txt | grep sai
isaiyah
sailormoon
saints
sailor
isaiyah1
isaias
bonsai
hussein
sailing
sai Baba
sairam
saint
saiful
lilsaint
saints1
saisai
omsairam
saiyuki
saiyan
sailboat
batusai
battousai
saint seiya
saikano
isaiyah2
saigon
allsaints
Isaiyah
```

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



The terminal window shows the command `cat rockyou.txt | grep cat` being run by a user with root privileges on a Kali Linux system. The output lists numerous password entries containing the string "cat".

```
root@SaiKali:~# cat rockyou.txt | grep cat
catherine
catdog
kittycat
pussycat
catalina
catarina
wildcats
coolcat
catalin
fatcat
cathy
catcat
cat123
wildcat
catwoman
blackcat
education
complicated
catdog1
ilovecats
catfish
bobcat
catch22
tomcat
pussycatdolls
bobcats
vacation
catlover
```



```
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
```

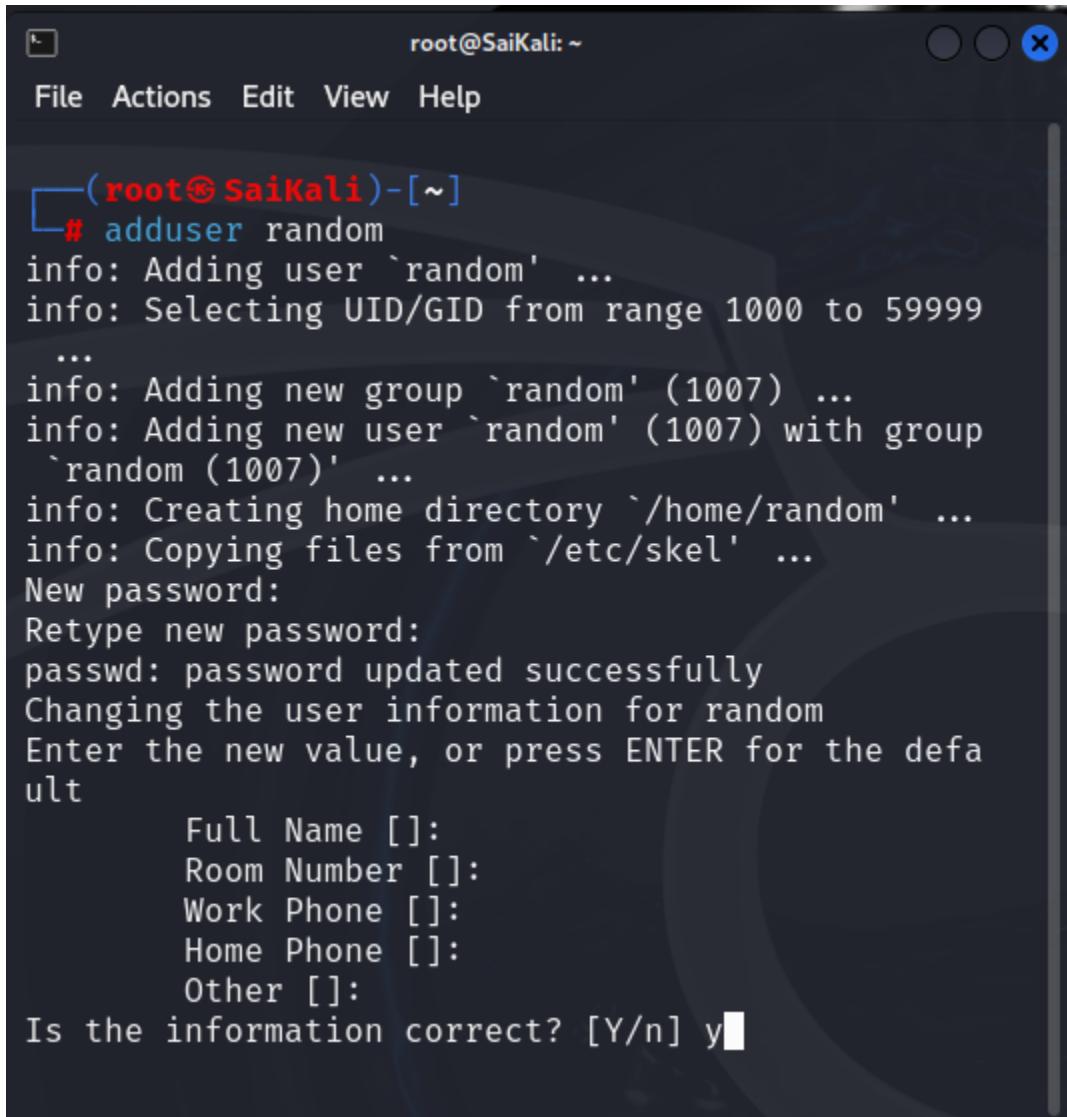


root@SaiKali: ~

```
root@SaiKali: ~
File Actions Edit View Help

└─(root@SaiKali)-[~]
  └─# cat rockyou.txt | grep lol
lolipop
lollypop
lolita
lolipop
lollol
lol123
lololo
lollies
lolly
lolipop1
lollie
lollypop1
lolliepop
lol123
lollipops
lolalola
lolol
lollypops
lolipop
lolito
lalola
lol
damilola
lolada
lol101
lolollol
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 random
info: Adding user `random' ...
info: Selecting UID/GID from range 1000 to 59999
...
info: Adding new group `random' (1007) ...
info: Adding new user `random' (1007) with group
`random (1007)' ...
info: Creating home directory `/home/random' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for random
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
```

```
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 group `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 default
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**

```
root@SaiKali:~  
File Actions Edit View Help  
└─(root@SaiKali)-[~]  
# john --wordlist=rockyou.txt --format=crypt rochester3.txt  
Using default input encoding: UTF-8  
Loaded 9 password hashes with 9 different salts (crypt, generic crypt(3) [?/64])  
Remaining 2 password hashes with 2 different salts  
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 f  
or all loaded hashes  
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
teacher      (aintrandom)  
Passw0rd     (random)  
2g 0:00:00:49 DONE (2024-09-16 00:17) 0.04074g/s 168.1p/s 197.5c/s 197.5C/s hhhhh..llcoolj  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```