

Password Cracking using John The Ripper:

- Open Kali linux and run it in the Root user.
 - Use cat /etc/passwd command to display the contents of the all user accounts registered on the system.

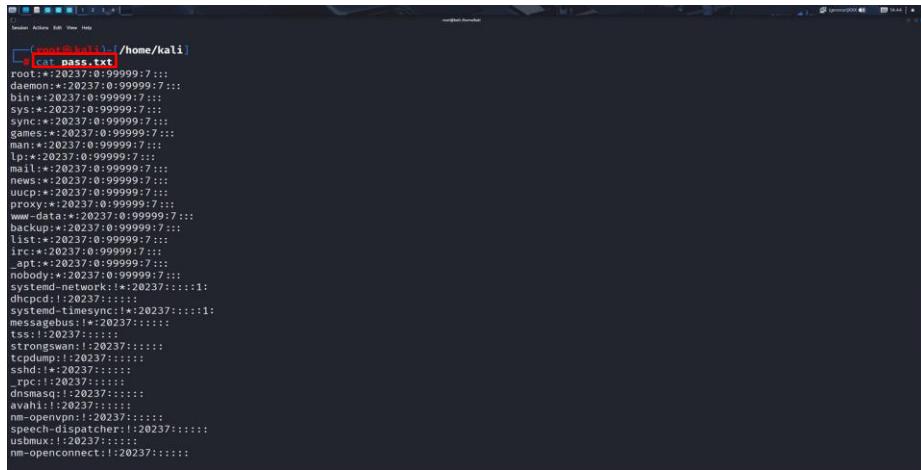
```
[root@kali ~]# /home/kali/usr/bin/zsh
[1]+ 118:121 ::/var/lib/snmp/bin/false
sslsh:x:119:122::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:120:125:user for cups-pk-helper service:/nonexistent:/usr/sbin/nologin
redsocks:x:121:126::/var/run/redsocks:/usr/sbin/nologin
libreoffice:x:122:127::/opt/libreoffice:/usr/sbin/nologin
indimed:x:123:65534::/run/indimed:/usr/sbin/nologin
miredo:x:124:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:125:129::/var/lib/redis:/usr/sbin/nologin
postgres:x:126:130::PostgreSQL administrator:/var/lib/postgresql:/bin/bash
memcached:x:127:131::/var/lib/memcached:/usr/sbin/nologin
inetutils:x:128:132::/var/lib/inetutils:/usr/sbin/nologin
gsmimx:x:129:134::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000::/home/kali:/usr/bin/zsh

[~root@kali ~]# cat /etc/shadow
[redacted]
root::20237:0:99999:7:::
daemon::20237:0:99999:7:::
bin::20237:0:99999:7:::
sys::20237:0:99999:7:::
sync::20237:0:99999:7:::
games::20237:0:99999:7:::
gdm::20237:0:99999:7:::
lp::20237:0:99999:7:::
mail::20237:0:99999:7:::
news::20237:0:99999:7:::
uucp::20237:0:99999:7:::
proxy::20237:0:99999:7:::
www-data::20237:0:99999:7:::
backups::20237:0:99999:7:::
ircd::20237:0:99999:7:::
lapt::20237:0:99999:7:::
nobody::20237:0:99999:7:::
systemd-network::1:20237::::1:
dhcpcd::1:20237::::1:
```

- Use `cat /etc/shadow` command in Linux to display the contents of the shadow password file, which stores encrypted user passwords and other sensitive account information.

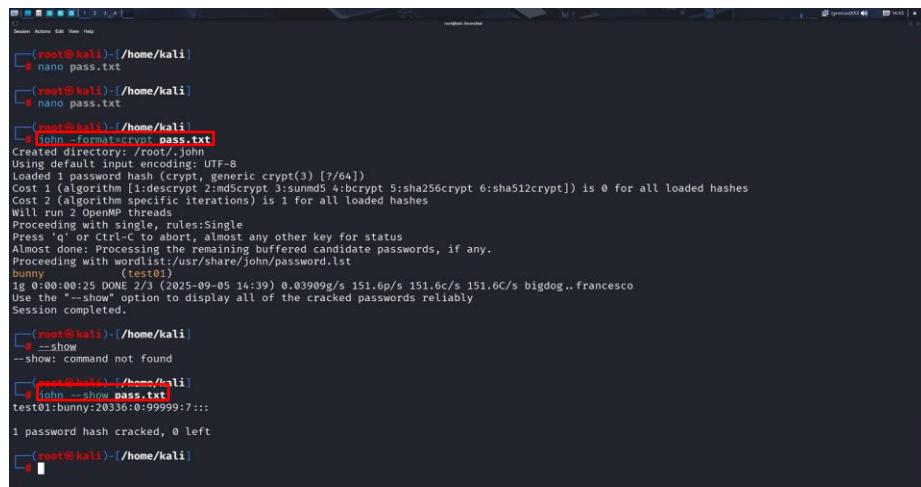
```
Kali:~# whoami
stunnel4[1]:20237::::
debcue[1]:20237::::
Debian-snmpproxy[1]:20237::::
cups-pk-helper[1]:20237::::
redsocks[1]:20237::::
_gophish[1]:20237::::
idle[1]:20237::::
niredo[1]:20237::::
redis[1]:20237::::
postgres[1]:20237::::
memcached[1]:20237::::
inetutils[1]:20237::::
_gvmm[1]:20237::::
kali:~$ id
uid=0(kali) gid=0(kali) groups=0(kali)
[+] /home/kali
[-] /bin/sh -c test01
New password:
Re-type new password:
Password: [REDACTED]
Password: [REDACTED] updated successfully
Changing the user information for test01
Enter the new value, or press ENTER for the default
    Full Name []: p
    Room Number []: p
    Work Phone []: p
    Home Phone []: p
    Other []: p
Is the information correct? [y/n] y
[+] /home/kali
[-] /etc/shadow ./pass.txt
[+] /home/kali
[-] /etc/passwd
[+] /home/kali
[-] /etc/shadow
[+] /home/kali
[-] /etc/passwd
[+] /home/kali
[-] /etc/shadow
[+] /home/kali
[-] /etc/passwd
```

- Give `adduser test01` command to Create a user and give a password to it.
- I have created the user with name of test01 and its password is bunny.
- And now give `cp /etc/shadow ./pass.txt` command , to copy the `/etc/shadow` file to a new file named `pass.txt` in the current directory.



```
(root@kali:~/home/kali] cat pass.txt
root:*:20237:0:99999:7:::
daemon:*:20237:0:99999:7:::
bin:*:20237:0:99999:7:::
sys:*:20237:0:99999:7:::
sync:*:20237:0:99999:7:::
games:*:20237:0:99999:7:::
man:*:20237:0:99999:7:::
lp:*:20237:0:99999:7:::
mail:*:20237:0:99999:7:::
news:*:20237:0:99999:7:::
uucp:*:20237:0:99999:7:::
proxy:*:20237:0:99999:7:::
www-data:*:20237:0:99999:7:::
backup:*:20237:0:99999:7:::
list:*:20237:0:99999:7:::
irc:*:20237:0:99999:7:::
apt:*:20237:0:99999:7:::
modem:*:20237:0:99999:7:::
systemd-network[*:20237:::1:
dhcpcd[*:20237:::1:
systemd-timesync[*:20237:::1:
messagebus[*:20237:::1:
tss[*:20237:::1:
strongswan[*:20237:::1:
tcpdump[*:20237:::1:
sshd[*:20237:::1:
 rpc[*:20237:::1:
dnsmasq[*:20237:::1:
avahi[*:20237:::1:
nm-openvpn[*:20237:::1:
speech-dispatcher[*:20237:::1:
usbmux[*:20237:::1:
nm-openconnect[*:20237:::1:
```

- Now give `cat pass.txt` command to view all the content in that file.
- Now delete all the content in the `pass.txt` file except test01 user credentials. by using `nano pass.txt` command you can edit the file.



```
(root@kali:~/home/kali] nano pass.txt
[root@kali:~/home/kali] nano pass.txt
[root@kali:~/home/kali] john --format=crypt pass.txt
john --format=crypt pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1]:descrypt 2:md5crypt 3:summd5 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 Ctrl-C or Ctrl-Break at any time for status
Almost done. Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
bunny          (test01)
1g 0:00:00:25 DONE 2/3 (2025-09-05 14:39) 0.03909g/s 151.6p/s 151.6c/s bigdog..francesco
Use the '--show' option to display all of the cracked passwords reliably
Session completed.

[root@kali:~/home/kali] --show
--show: command not found
[root@kali:~/home/kali] john --show pass.txt
test01:bunny:20336:0:99999:7:::
1 password hash cracked, 0 left
[root@kali:~/home/kali]
```

- Give `john -format=crypt pass.txt` command to crack the password of the created user.
- It cracks the password in seconds, Now the password cracking is completed.
- For verification Purpose, use `john --show pass.txt` command, to verify whether the password is cracked or not.