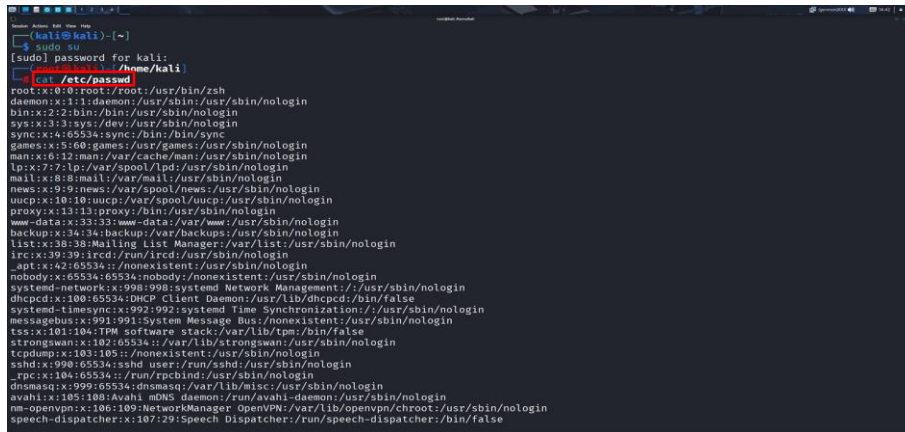
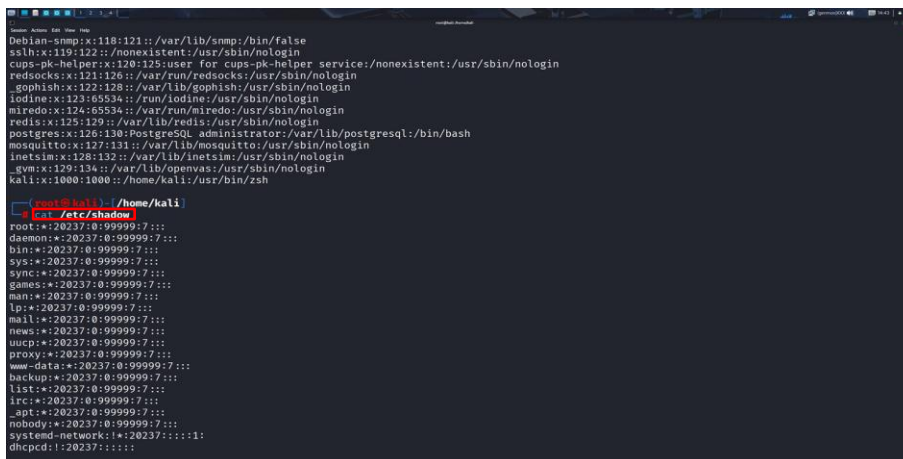


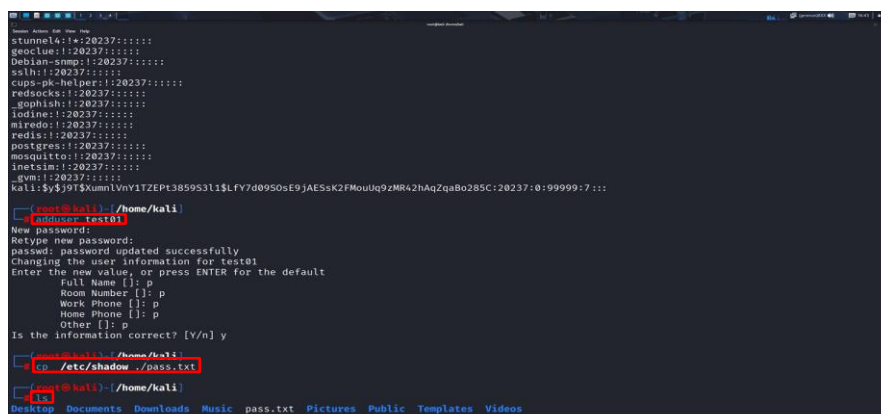
Password Cracking using John The Ripper:



- 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.



- 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.



- 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# cp /etc/shadow ./pass.txt
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:::
nobody:*:20237:0:99999:7:::
system-network:*:20237:0:99999:7:::
dhcpcd:*:20237:0:99999:7:::
system-timesync:*:20237:0:99999:7:::
messagebus:*:20237:0:99999:7:::
tss:*:20237:0:99999:7:::
strngswan:*:20237:0:99999:7:::
tcpdump:*:20237:0:99999:7:::
sshd:*:20237:0:99999:7:::
rpc:*:20237:0:99999:7:::
dnsmasq:*:20237:0:99999:7:::
avahi:*:20237:0:99999:7:::
nm-openvpn:*:20237:0:99999:7:::
speech-dispatcher:*:20237:0:99999:7:::
usbmuxd:*:20237:0:99999:7:::
nm-openconnect:*:20237:0:99999:7:::

```

- 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# cat pass.txt
root@kali:~/home/kali# nano pass.txt
root@kali:~/home/kali# nano pass.txt
root@kali:~/home/kali# john --format=crypt pass.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1]:descript 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
bunny
(test01)
ig 0:00:00:25 DONE 2/3 (2025-09-05 14:39) 0.03909g/s 151.6p/s 151.6c/s 151.6C/s bigdog..francesco
Session completed.

root@kali:~/home/kali# john --show pass.txt
--show: command not found

root@kali:~/home/kali# john --show pass.txt
test01:bunny:20237:0:99999:7:::
1 password hash cracked, 0 left

```

- 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.