VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

John the Ripper

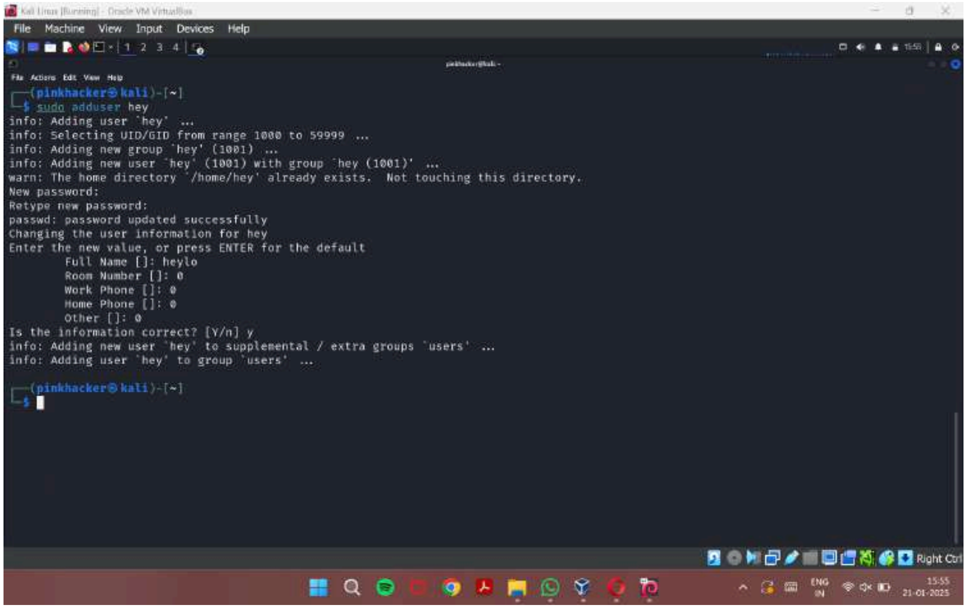
NAME: DHEVATHA S P
REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

John the ripper

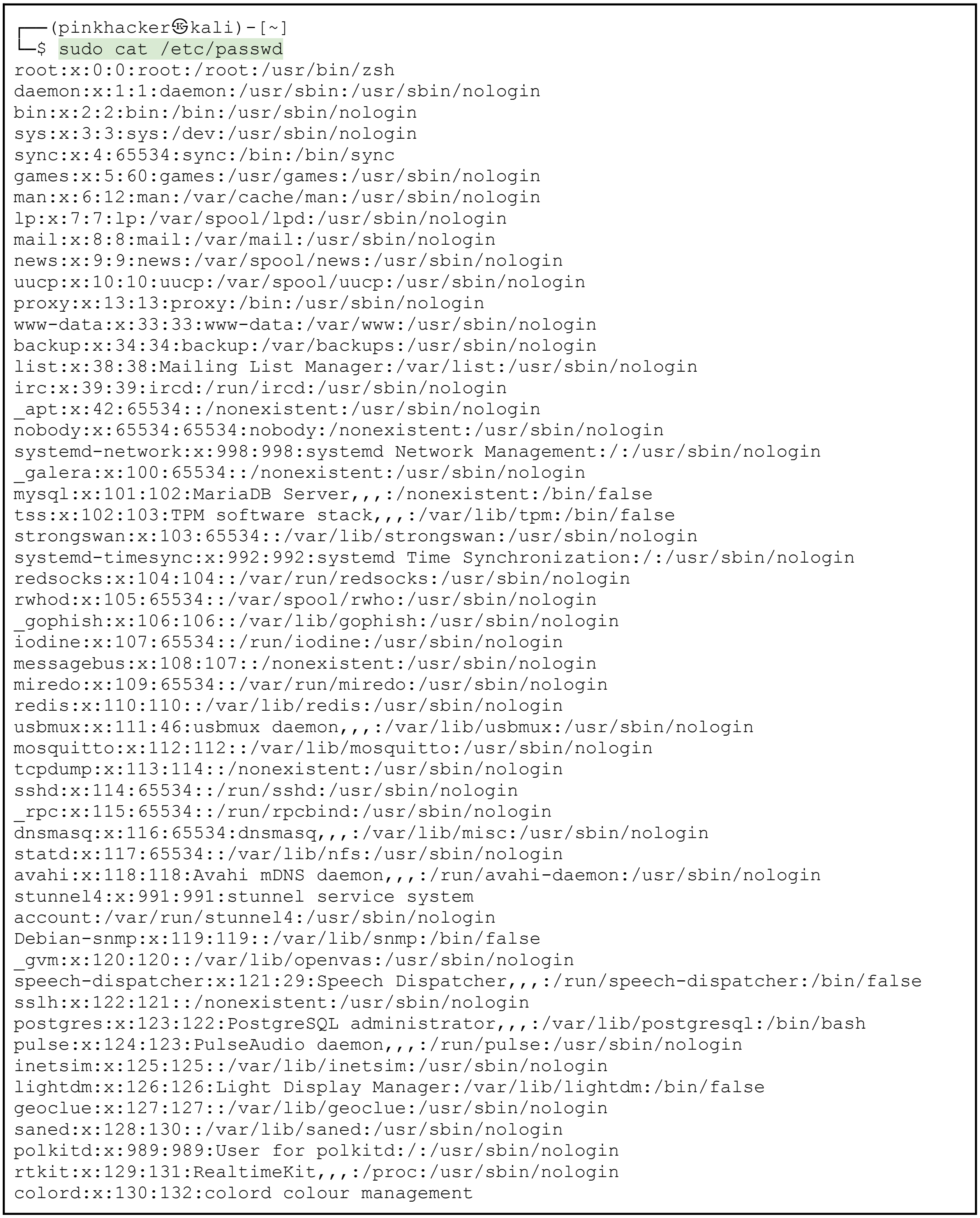
1. Creating new user to Kali Linux (User name : hey, Password : hello)

```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo adduser hey
[sudo] password for pinkhacker:
info: Adding user `hey' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `hey' (1001) ...
info: Adding new user `hey' (1001) with group `hey (1001)' ...
info: Creating home directory `/home/hey' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hey
Enter the new value, or press ENTER for the default
        Full Name []: heylo
        Room Number []: 1
        Work Phone []: 1
        Home Phone []: 1
        Other []: 1
Is the information correct? [Y/n] y
info: Adding new user `hey' to supplemental / extra groups `users' ...
info: Adding user `hey' to group `users' ...
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl

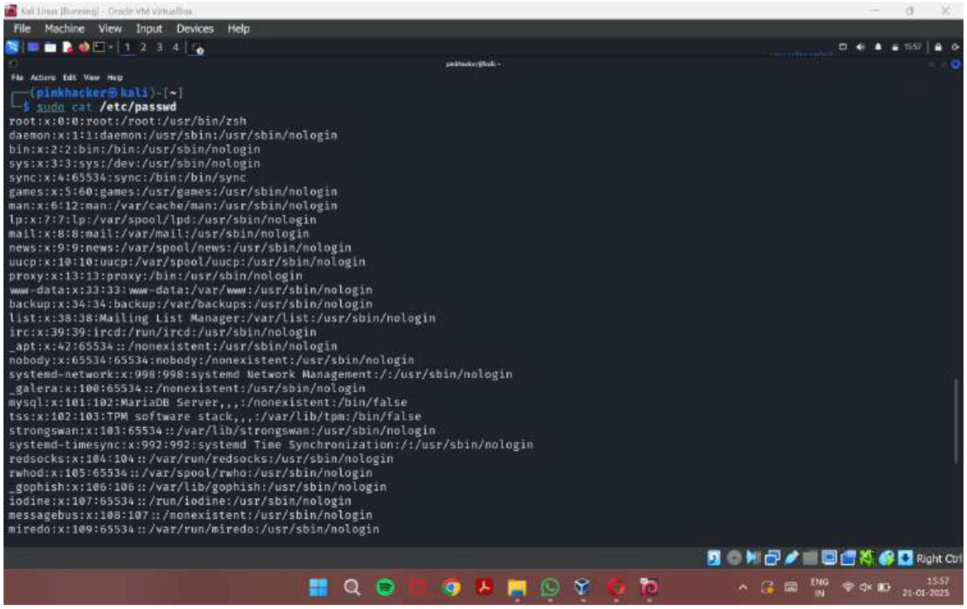
```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo adduser hey
info: Adding user `hey' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `hey' (1001) ...
info: Adding new user `hey' (1001) with group `hey (1001)' ...
warn: The home directory `/home/hey' already exists.  Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hey
Enter the new value, or press ENTER for the default
        Full Name []: heylo
        Room Number []: 0
        Work Phone []: 0
        Home Phone []: 0
        Other []: 0
Is the information correct? [Y/n] y
info: Adding new user `hey' to supplemental / extra groups `users' ...
info: Adding user `hey' to group `users' ...

┌──(pinkhacker㉿kali)-[~]
└─$
```

2. Checking new username in Kali Linux

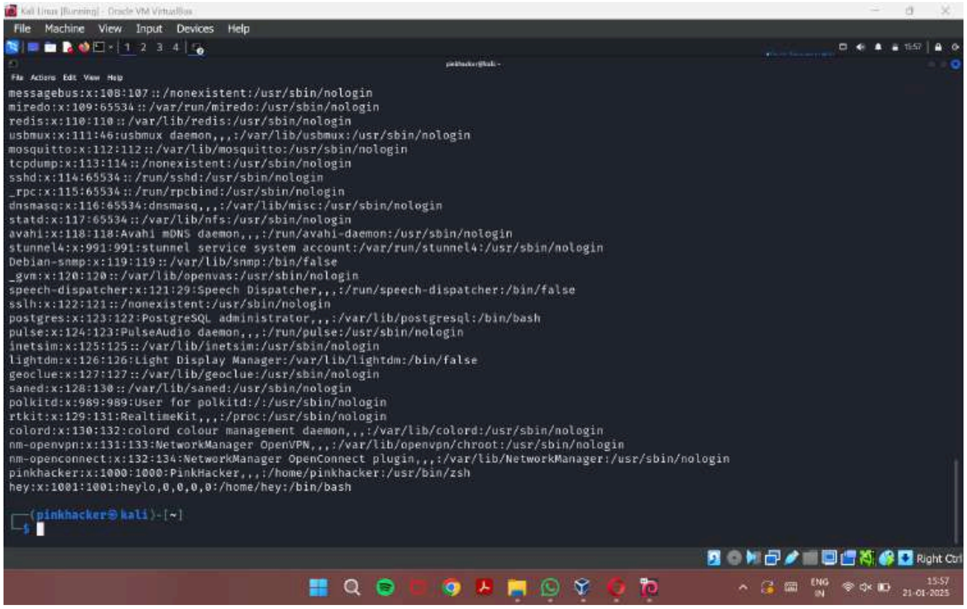


```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
_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/nologin
redsocks:x:104:104::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:105:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:106:106::/var/lib/gophish:/usr/sbin/nologin
iodine:x:107:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:108:107::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:110:110::/var/lib/redis:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:112:112::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:x:113:114::/nonexistent:/usr/sbin/nologin
sshd:x:114:65534::/run/sshd:/usr/sbin/nologin
_rpc:x:115:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:116:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:x:118:118:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system
account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:119:119::/var/lib/snmp:/bin/false
_gvm:x:120:120::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:121:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:x:122:121::/nonexistent:/usr/sbin/nologin
postgres:x:123:122:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:x:124:123:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
inetsim:x:125:125::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:126:126:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:x:127:127::/var/lib/geoclue:/usr/sbin/nologin
saned:x:128:130::/var/lib/saned:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
rtkit:x:129:131:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:130:132:colord colour management
```

```
daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:131:133:NetworkManager
OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:132:134:NetworkManager OpenConnect
plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
pinkhacker:x:1000:1000:PinkHacker,,,:/home/pinkhacker:/usr/bin/zsh
hey:x:1001:1001:heylo,1,1,1,1:/home/hey:/bin/bash
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
ENG IN
15:57
21-01-2025

```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo 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
_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/nologin
redsocks:x:104:104::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:105:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:106:106::/var/lib/gophish:/usr/sbin/nologin
iodine:x:107:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:108:107::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
```

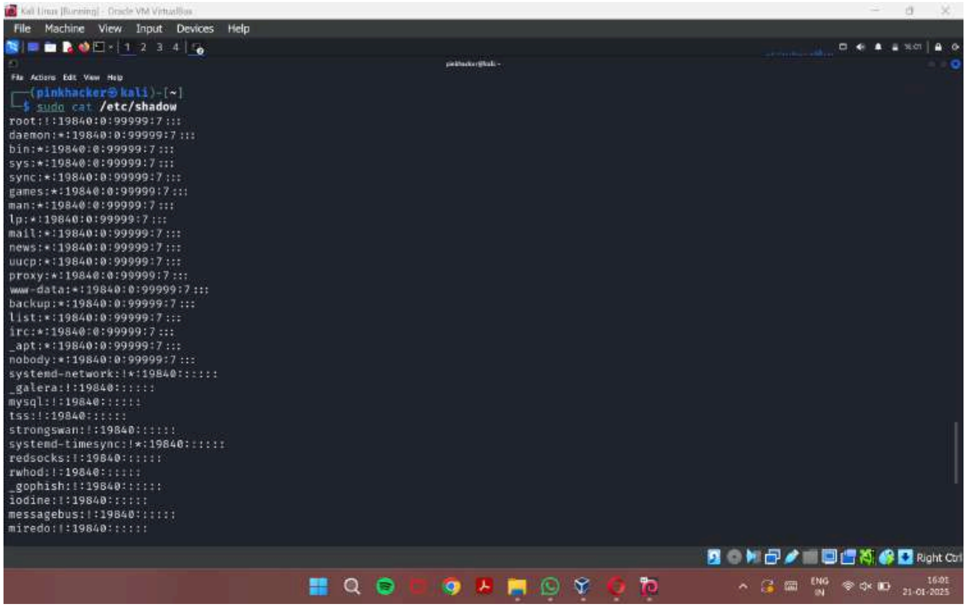

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
ENG IN
15:57
21-01-2025

```
messagebus:x:108:107::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:110:110::/var/lib/redis:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:112:112::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:x:113:114::/nonexistent:/usr/sbin/nologin
sshd:x:114:65534::/run/sshd:/usr/sbin/nologin
_rpc:x:115:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:116:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:x:118:118:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:119:119::/var/lib/snmp:/bin/false
_gvm:x:120:120::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:121:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:x:122:121::/nonexistent:/usr/sbin/nologin
postgres:x:123:122:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:x:124:123:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
inetsim:x:125:125::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:126:126:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:x:127:127::/var/lib/geoclue:/usr/sbin/nologin
saned:x:128:130::/var/lib/saned:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
rtkit:x:129:131:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:130:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:131:133:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:132:134:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
pinkhacker:x:1000:1000:PinkHacker,,,:/home/pinkhacker:/usr/bin/zsh
hey:x:1001:1001:heylo,0,0,0,0:/home/hey:/bin/bash

┌──(pinkhacker㉿kali)-[~]
└─$ 
```

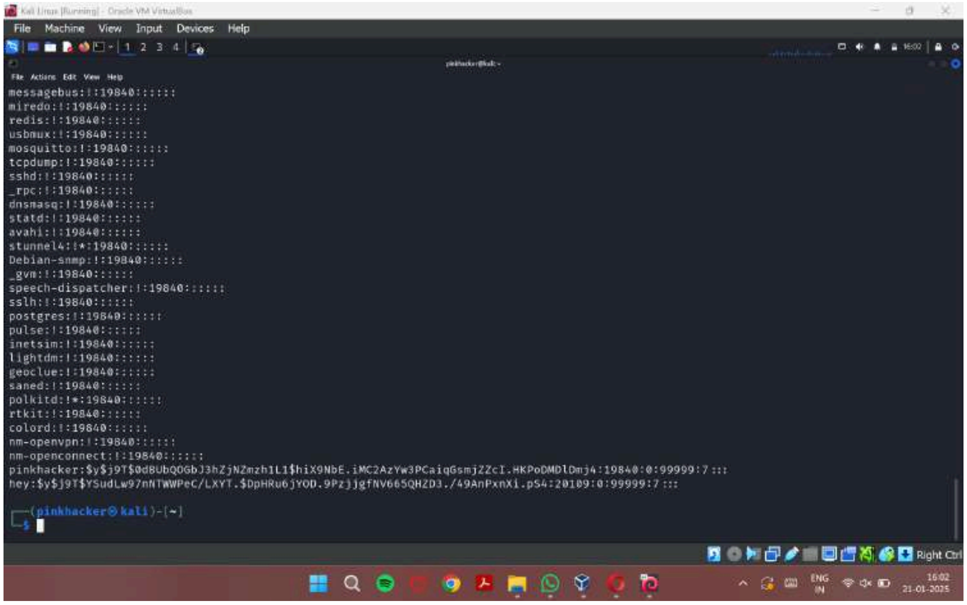
3. Checking new user’s password (encrypted) in Kali Linux

```
┌──(pinkhacker㉿kali)-[~]
```

```
└─$ sudo cat /etc/shadow
root:!:19840:0:99999:7:::
daemon:*:19840:0:99999:7:::
bin:*:19840:0:99999:7:::
sys:*:19840:0:99999:7:::
sync:*:19840:0:99999:7:::
games:*:19840:0:99999:7:::
man:*:19840:0:99999:7:::
lp:*:19840:0:99999:7:::
mail:*:19840:0:99999:7:::
news:*:19840:0:99999:7:::
uucp:*:19840:0:99999:7:::
proxy:*:19840:0:99999:7:::
www-data:*:19840:0:99999:7:::
backup:*:19840:0:99999:7:::
list:*:19840:0:99999:7:::
irc:*:19840:0:99999:7:::
_apt:*:19840:0:99999:7:::
nobody:*:19840:0:99999:7:::
systemd-network:!*:19840::::::
_galera:!:19840::::::
mysql:!:19840::::::
tss:!:19840::::::
strongswan:!:19840::::::
systemd-timesync:!*:19840::::::
redsocks:!:19840::::::
rwhod:!:19840::::::
_gophish:!:19840::::::
iodine:!:19840::::::
messagebus:!:19840::::::
miredo:!:19840::::::
redis:!:19840::::::
usbmux:!:19840::::::
mosquitto:!:19840::::::
tcpdump:!:19840::::::
sshd:!:19840::::::
_rpc:!:19840::::::
dnsmasq:!:19840::::::
statd:!:19840::::::
avahi:!:19840::::::
stunnel4:!*:19840::::::
Debian-snmp:!:19840::::::
_gvm:!:19840::::::
speech-dispatcher:!:19840::::::
sslh:!:19840::::::
postgres:!:19840::::::
pulse:!:19840::::::
inetsim:!:19840::::::
lightdm:!:19840::::::
geoclue:!:19840::::::
saned:!:19840::::::
polkitd:!*:19840::::::
rtkit:!:19840::::::
colord:!:19840::::::
nm-openvpn:!:19840::::::
nm-openconnect:!:19840::::::
pinkhacker:$y$j9T$0dBUbQOGbJ3hZjNZmzh1L1$hiX9NbE.iMC2AzYw3PCaiqGsmjZZcI.HKPoDMDlDmj4
:19840:0:99999:7:::
hey:$y$j9T$c3sSjjPYkFmEL.oOHqiGU/$uZqLfOoSozixCWPFLagLM5BhcqngSon5YxzP7e/cQX9:20108:
0:99999:7:::
```



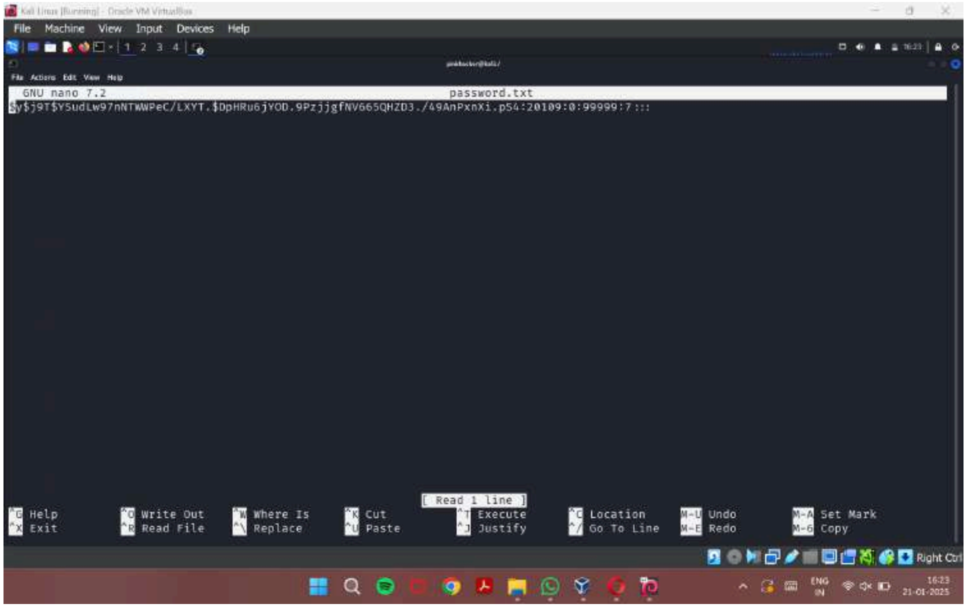
```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo cat /etc/shadow
root:!:19840:0:99999:7:::
daemon:*:19840:0:99999:7:::
bin:*:19840:0:99999:7:::
sys:*:19840:0:99999:7:::
sync:*:19840:0:99999:7:::
games:*:19840:0:99999:7:::
man:*:19840:0:99999:7:::
lp:*:19840:0:99999:7:::
mail:*:19840:0:99999:7:::
news:*:19840:0:99999:7:::
uucp:*:19840:0:99999:7:::
proxy:*:19840:0:99999:7:::
www-data:*:19840:0:99999:7:::
backup:*:19840:0:99999:7:::
list:*:19840:0:99999:7:::
irc:*:19840:0:99999:7:::
_apt:*:19840:0:99999:7:::
nobody:*:19840:0:99999:7:::
systemd-network:!*:19840::::::
_galera:!:19840::::::
mysql:!:19840::::::
tss:!:19840::::::
strongswan:!:19840::::::
systemd-timesync:!*:19840::::::
redsocks:!:19840::::::
rwhod:!:19840::::::
_gophish:!:19840::::::
iodine:!:19840::::::
messagebus:!:19840::::::
miredo:!:19840::::::
```



```
messagebus:!:19840::::::
miredo:!:19840::::::
redis:!:19840::::::
usbmux:!:19840::::::
mosquitto:!:19840::::::
tcpdump:!:19840::::::
sshd:!:19840::::::
_rpc:!:19840::::::
dnsmasq:!:19840::::::
statd:!:19840::::::
avahi:!:19840::::::
stunnel4:!*:19840::::::
Debian-snmp:!:19840::::::
_gvm:!:19840::::::
speech-dispatcher:!:19840::::::
sslh:!:19840::::::
postgres:!:19840::::::
pulse:!:19840::::::
inetsim:!:19840::::::
lightdm:!:19840::::::
geoclue:!:19840::::::
saned:!:19840::::::
polkitd:!*:19840::::::
rtkit:!:19840::::::
colord:!:19840::::::
nm-openvpn:!:19840::::::
nm-openconnect:!:19840::::::
pinkhacker:$y$j9T$0dBUbQOGbJ3hZjNZmzh1L1$hiX9NbE.iMC2AzYw3PCaiqGsmjZZcI.HKPoDMDlDmj4:19840:0:99999:7:::
hey:$y$j9T$YSudLw97nNTWWPeC/LXYT.$DpHRu6jYOD.9PzjjgfNV665QHZD3./49AnPxnXi.pS4:20109:0:99999:7:::

┌──(pinkhacker㉿kali)-[~]
└─$ 
```

4. Creating the password.txt file

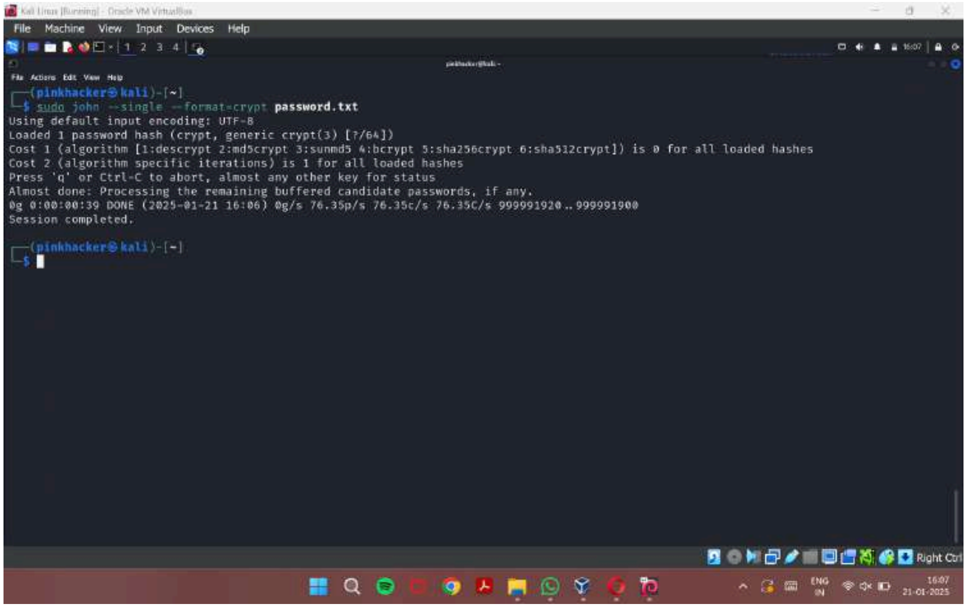
```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo nano password.txt
```



```
  GNU nano 7.2                                                password.txt
$y$j9T$Y5udLw97nNTWWPeC/LXYT.$DpHRu6jYOD.9PzjjgfNV665QHZD3./49AnPxnXi.p54:20109:0:99999:7:::
```

5. Passing the password.txt through John toolkit

```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo john --single --format=crypt password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (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
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
0g 0:00:00:35 DONE (2025-01-20 22:39) 0g/s 84.61p/s 84.61c/s 84.61C/s
999991920..999991900
Session completed.
```



```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo john --single --format=crypt password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (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
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
0g 0:00:00:39 DONE (2025-01-21 16:06) 0g/s 76.35p/s 76.35c/s 76.35C/s 999991920..999991900
Session completed.

┌──(pinkhacker㉿kali)-[~]
└─$ 
```

This outcome could be due to several reasons:

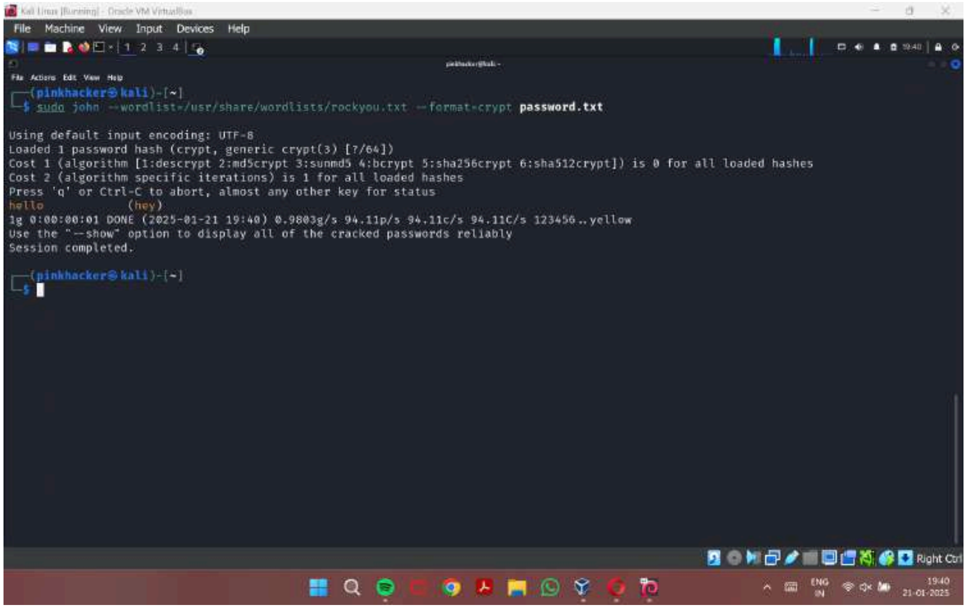
- The hash format might not be supported by the configuration you're using.
- The hash might be too complex, and john in "single" mode might not be able to handle it.
- You may need to specify the correct hash format explicitly or use a different attack mode.

If you'd like, you could try specifying a different attack mode (e.g., --wordlist or --incremental) or check that the hash format is correct.

6. Wordlists

```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt
password.txt

Using default input encoding: UTF-8
Loaded 1 password hash (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
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (hey)
1g 0:00:00:01 DONE (2025-01-21 19:40) 0.9803g/s 94.11p/s 94.11c/s 94.11C/s
123456..yellow
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

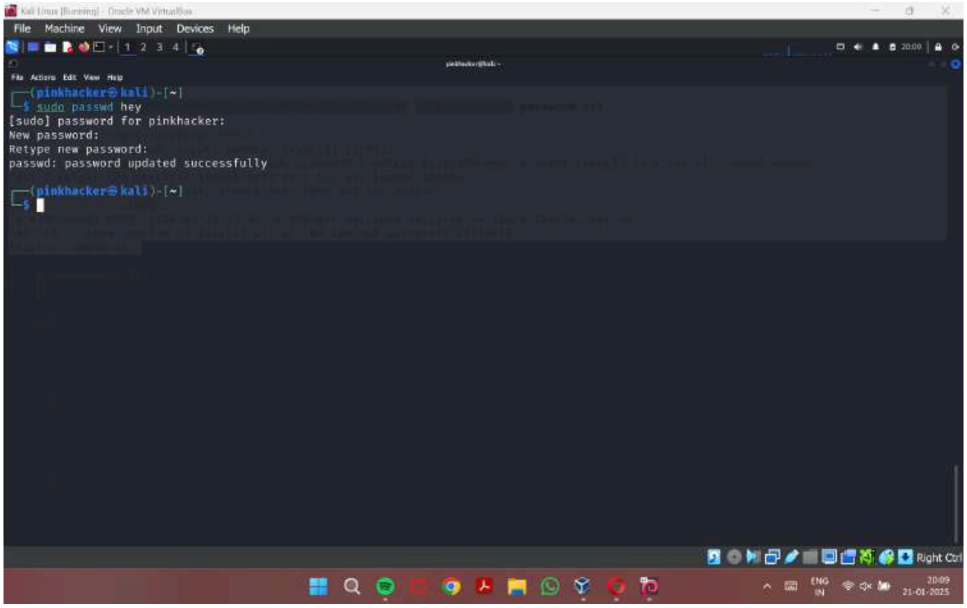


```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt password.txt

Using default input encoding: UTF-8
Loaded 1 password hash (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
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (hey)
1g 0:00:00:01 DONE (2025-01-21 19:40) 0.9803g/s 94.11p/s 94.11c/s 94.11C/s 123456..yellow
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(pinkhacker㉿kali)-[~]
└─$ 
```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
19:40
21-01-2025

7. Changing the password

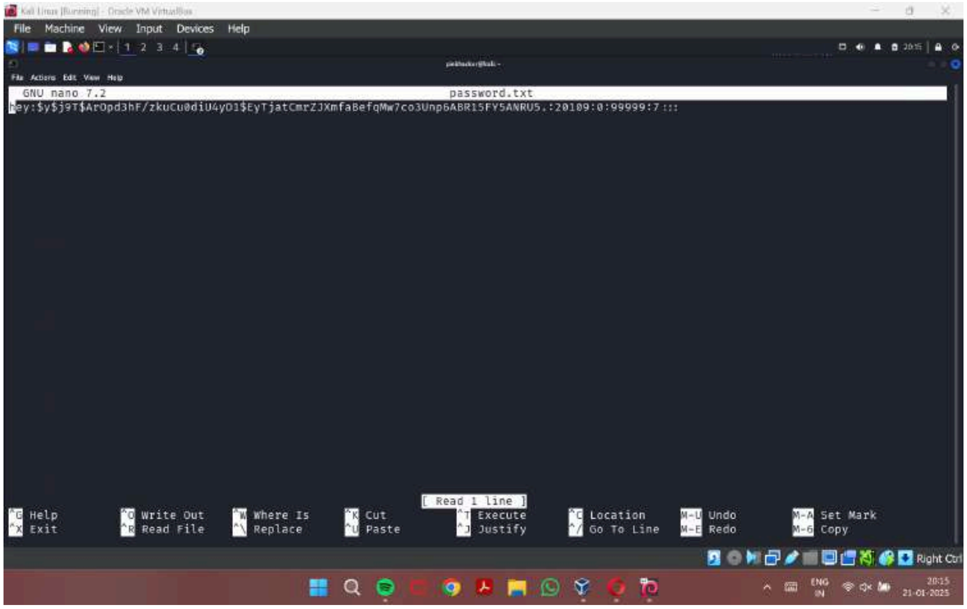
```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo passwd hey
[sudo] password for pinkhacker:
New password:
Retype new password:
passwd: password updated successfully
```



```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo passwd hey
[sudo] password for pinkhacker:
New password:
Retype new password:
passwd: password updated successfully

┌──(pinkhacker㉿kali)-[~]
└─$ 
```

8. Updating the password.txt

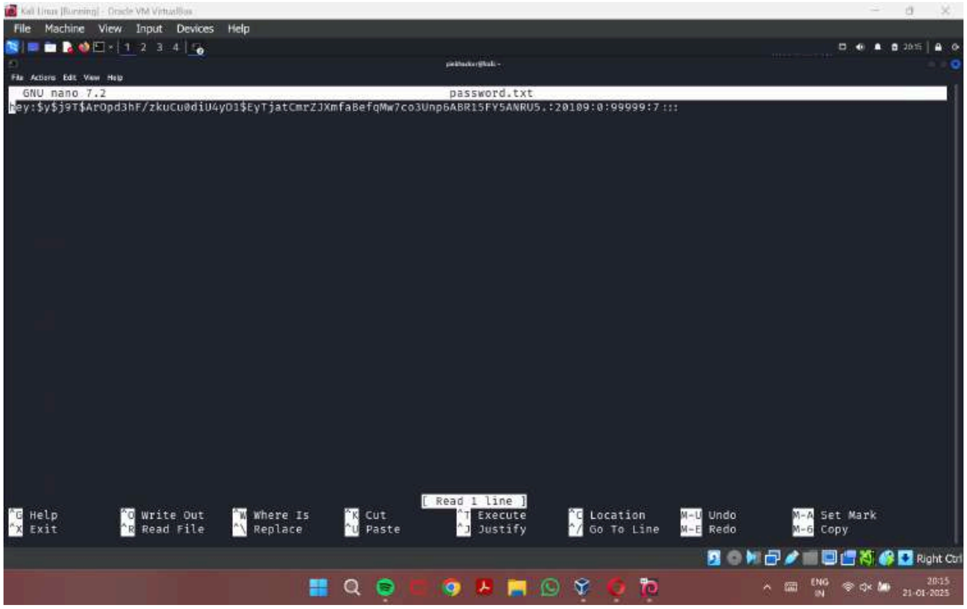
```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo nano password.txt
```



```
  GNU nano 7.2                                   password.txt
hey:$y$j9T$ArOpd3hF/zkuCu0diU4yD1$EyTjatCmrZJXmfaBefqMw7co3Unp6ABR15FY5ANRU5.:20109:0:99999:7:::

                                 [ Read 1 line ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo     M-6 Copy
```

9. Updating the password.txt

```
┌──(pinkhacker㉿kali)-[~]
└─$ sudo nano password.txt
```



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Right Ctrl
ENG IN
20:15
21-01-2025

```
  GNU nano 7.2                                          password.txt
hey:$y$j9T$ArOpd3hF/zkuCu0diU4yO1$EyTjatCmrZJXmfaBefqMw7co3Unp6ABR15FY5ANRU5.:20109:0:99999:7:::

                                          [ Read 1 line ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```