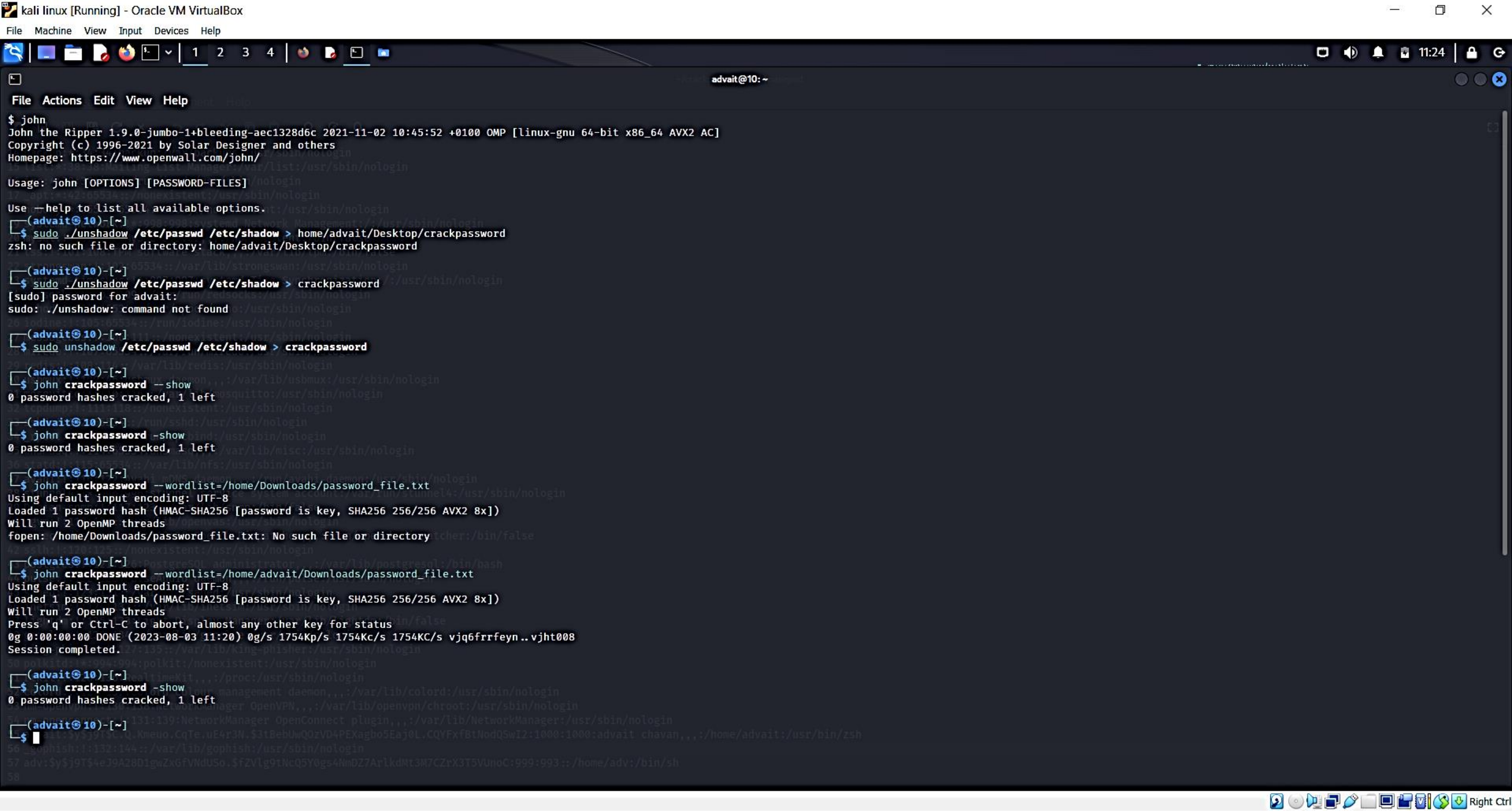
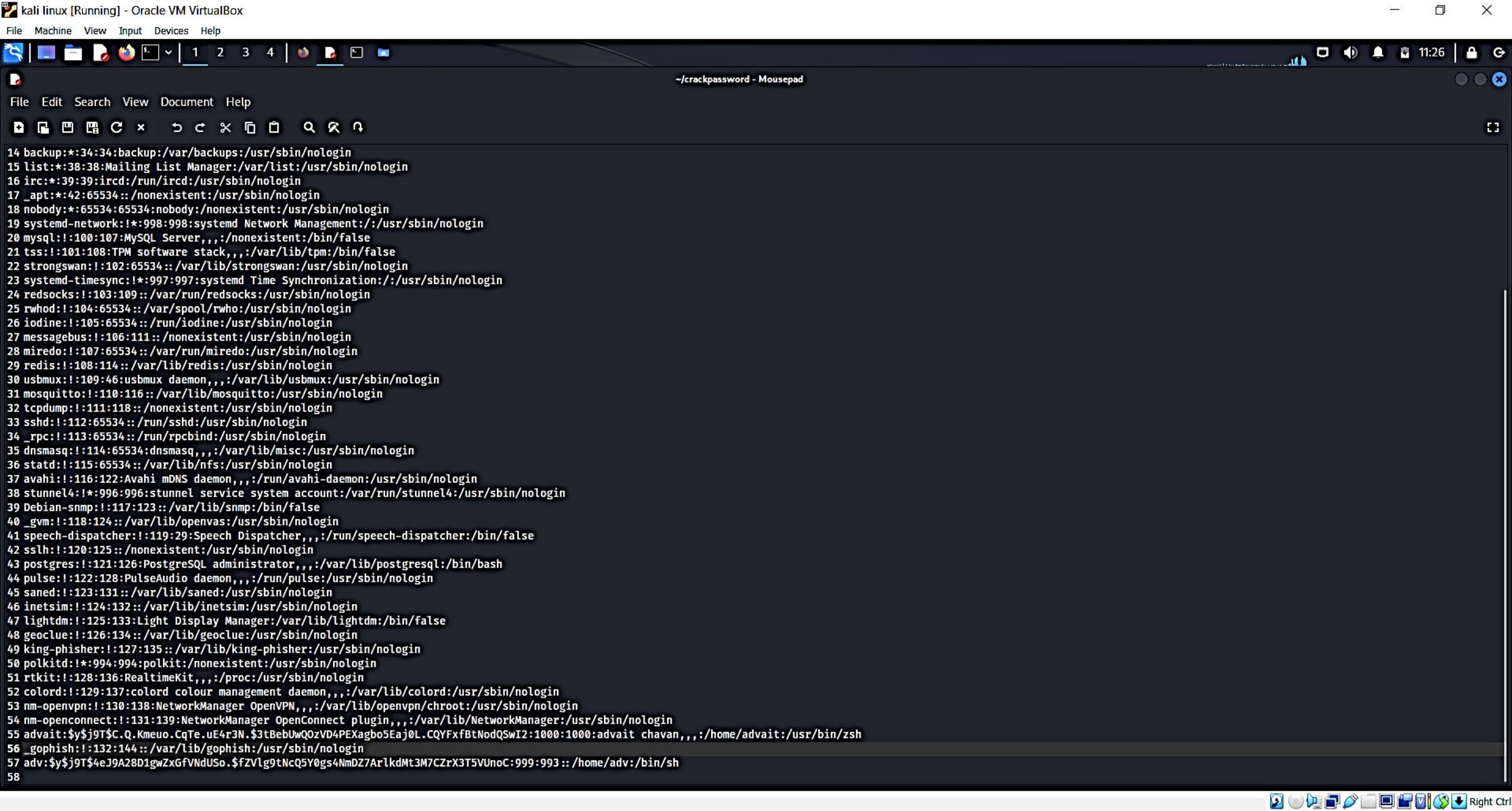
Steps for cracking password of the system(kail root user) :-

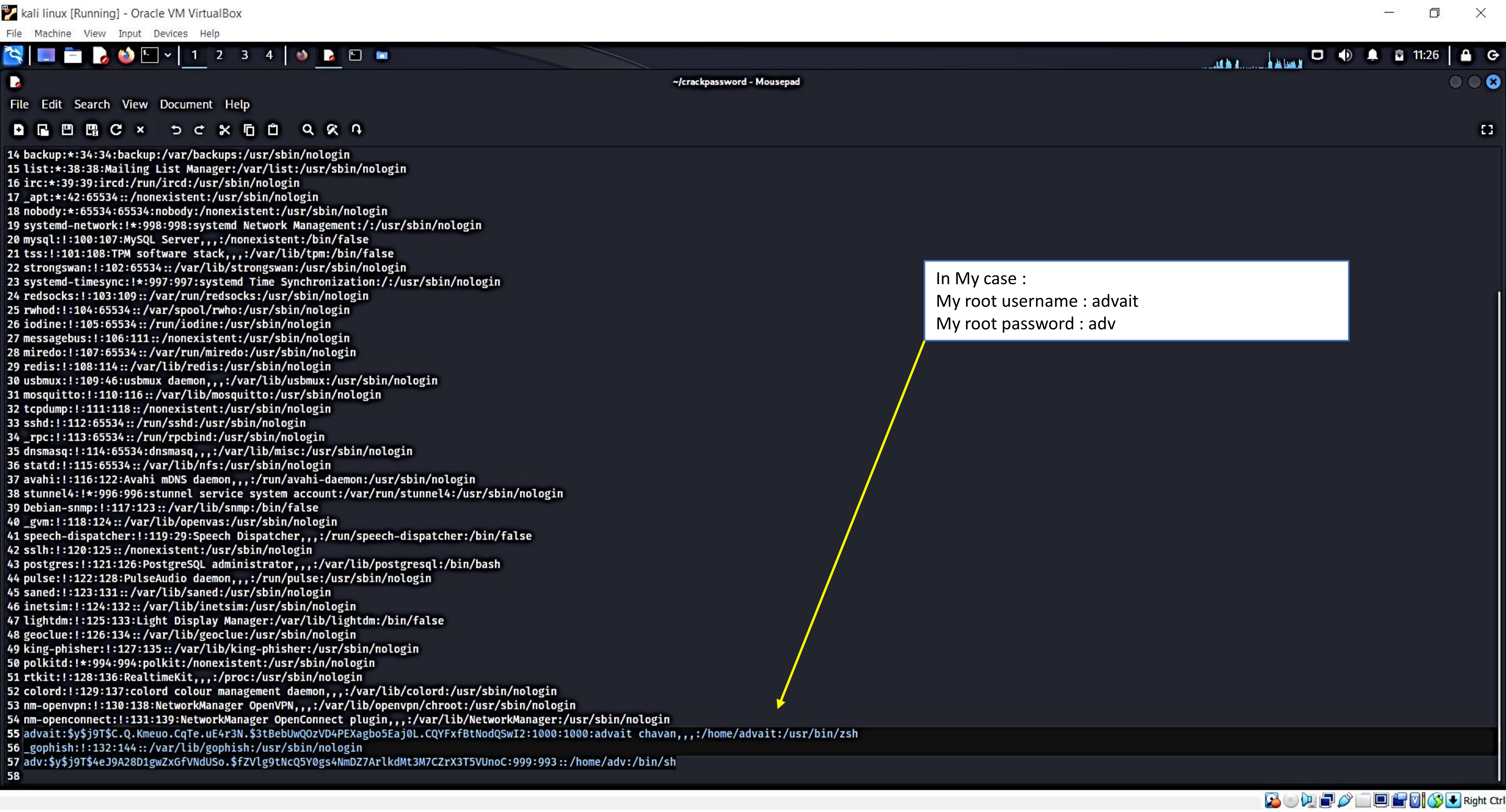
1. Create a new file named ‘crackpassword’ to save all the details using the command
   sudo unshadow /etc/passwd /etc/password > crackpassword . This will save the fetch and store the root user’s username and password in hash(SAH256) format.
2. Then using the john ripper using the following command crack the user’s username and password with the help of a password_file.txt using the command
   john crackpassword –wordlist=/home/advait/Downloads/password_file.txt
3. On hitting the above command the linux shell will display a message ‘**Session Completed**’.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:24
advait@10: ~
File Actions Edit View Help
Right Ctrl

```
$ 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.
┌──(advait㉿10)-[~]
└─$ sudo ./unshadow /etc/passwd /etc/shadow > home/advait/Desktop/crackpassword
zsh: no such file or directory: home/advait/Desktop/crackpassword

┌──(advait㉿10)-[~]
└─$ sudo ./unshadow /etc/passwd /etc/shadow > crackpassword
[sudo] password for advait:
sudo: ./unshadow: command not found

┌──(advait㉿10)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > crackpassword

┌──(advait㉿10)-[~]
└─$ john crackpassword --show
0 password hashes cracked, 1 left

┌──(advait㉿10)-[~]
└─$ john crackpassword -show
0 password hashes cracked, 1 left

┌──(advait㉿10)-[~]
└─$ john crackpassword --wordlist=/home/Downloads/password_file.txt
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 2 OpenMP threads
fopen: /home/Downloads/password_file.txt: No such file or directory

┌──(advait㉿10)-[~]
└─$ john crackpassword --wordlist=/home/advait/Downloads/password_file.txt
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2023-08-03 11:20) 0g/s 1754Kp/s 1754Kc/s 1754KC/s vjq6frrfeyn..vjht008
Session completed.

┌──(advait㉿10)-[~]
└─$ john crackpassword -show
0 password hashes cracked, 1 left

┌──(advait㉿10)-[~]
└─$ 
```


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:26
~/crackpassword - Mousepad
File Edit Search View Document Help
Right Ctrl

```
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
mysql:!:100:107:MySQL Server,,,:/nonexistent:/bin/false
tss:!:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:!:102:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:!*:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
redsocks:!:103:109::/var/run/redsocks:/usr/sbin/nologin
rwhod:!:104:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:!:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:!:106:111::/nonexistent:/usr/sbin/nologin
miredo:!:107:65534::/var/run/miredo:/usr/sbin/nologin
redis:!:108:114::/var/lib/redis:/usr/sbin/nologin
usbmux:!:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:!:110:116::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:!:111:118::/nonexistent:/usr/sbin/nologin
sshd:!:112:65534::/run/sshd:/usr/sbin/nologin
_rpc:!:113:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:!:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:!:115:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:!:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:!*:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:!:117:123::/var/lib/snmp:/bin/false
_gvm:!:118:124::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:!:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:!:120:125::/nonexistent:/usr/sbin/nologin
postgres:!:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:!:122:128:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:!:123:131::/var/lib/saned:/usr/sbin/nologin
inetsim:!:124:132::/var/lib/inetsim:/usr/sbin/nologin
lightdm:!:125:133:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:!:126:134::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:!:127:135::/var/lib/king-phisher:/usr/sbin/nologin
polkitd:!*:994:994:polkit:/nonexistent:/usr/sbin/nologin
rtkit:!:128:136:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:!:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:!:130:138:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:!:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
advait:$y$j9T$C.Q.Kmeuo.CqTe.uE4r3N.$3tBebUwQOzVD4PEXagbo5Eaj0L.CQYFxfBtNodQSwI2:1000:1000:advait chavan,,,:/home/advait:/usr/bin/zsh
_gophish:!:132:144::/var/lib/gophish:/usr/sbin/nologin
adv:$y$j9T$4eJ9A28D1gwZxGfVNdUSo.$fZVlg9tNcQ5Y0gs4NmDZ7ArlkdMt3M7CZrX3T5VUnoC:999:993::/home/adv:/bin/sh

```


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~/crackpassword - Mousepad
File Edit Search View Document Help
11:26
Right Ctrl

```
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
mysql:!:100:107:MySQL Server,,,:/nonexistent:/bin/false
tss:!:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:!:102:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:!*:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
redsocks:!:103:109::/var/run/redsocks:/usr/sbin/nologin
rwhod:!:104:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:!:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:!:106:111::/nonexistent:/usr/sbin/nologin
miredo:!:107:65534::/var/run/miredo:/usr/sbin/nologin
redis:!:108:114::/var/lib/redis:/usr/sbin/nologin
usbmux:!:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:!:110:116::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:!:111:118::/nonexistent:/usr/sbin/nologin
sshd:!:112:65534::/run/sshd:/usr/sbin/nologin
_rpc:!:113:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:!:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:!:115:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:!:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:!*:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:!:117:123::/var/lib/snmp:/bin/false
_gvm:!:118:124::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:!:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sslh:!:120:125::/nonexistent:/usr/sbin/nologin
postgres:!:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:!:122:128:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:!:123:131::/var/lib/saned:/usr/sbin/nologin
inetsim:!:124:132::/var/lib/inetsim:/usr/sbin/nologin
lightdm:!:125:133:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:!:126:134::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:!:127:135::/var/lib/king-phisher:/usr/sbin/nologin
polkitd:!*:994:994:polkit:/nonexistent:/usr/sbin/nologin
rtkit:!:128:136:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:!:129:137:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:!:130:138:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:!:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
advait:$y$j9T$C.Q.Kmeuo.CqTe.uE4r3N.$3tBebUwQOzVD4PEXagbo5Eaj0L.CQYFxfBtNodQSwI2:1000:1000:advait chavan,,,:/home/advait:/usr/bin/zsh
_gophish:!:132:144::/var/lib/gophish:/usr/sbin/nologin
adv:$y$j9T$4eJ9A28D1gwZxGfVNdUSo.$fZVlg9tNcQ5Y0gs4NmDZ7ArlkdMt3M7CZrX3T5VUnoC:999:993::/home/adv:/bin/sh
```

In My case :
My root username : advait
My root password : adv