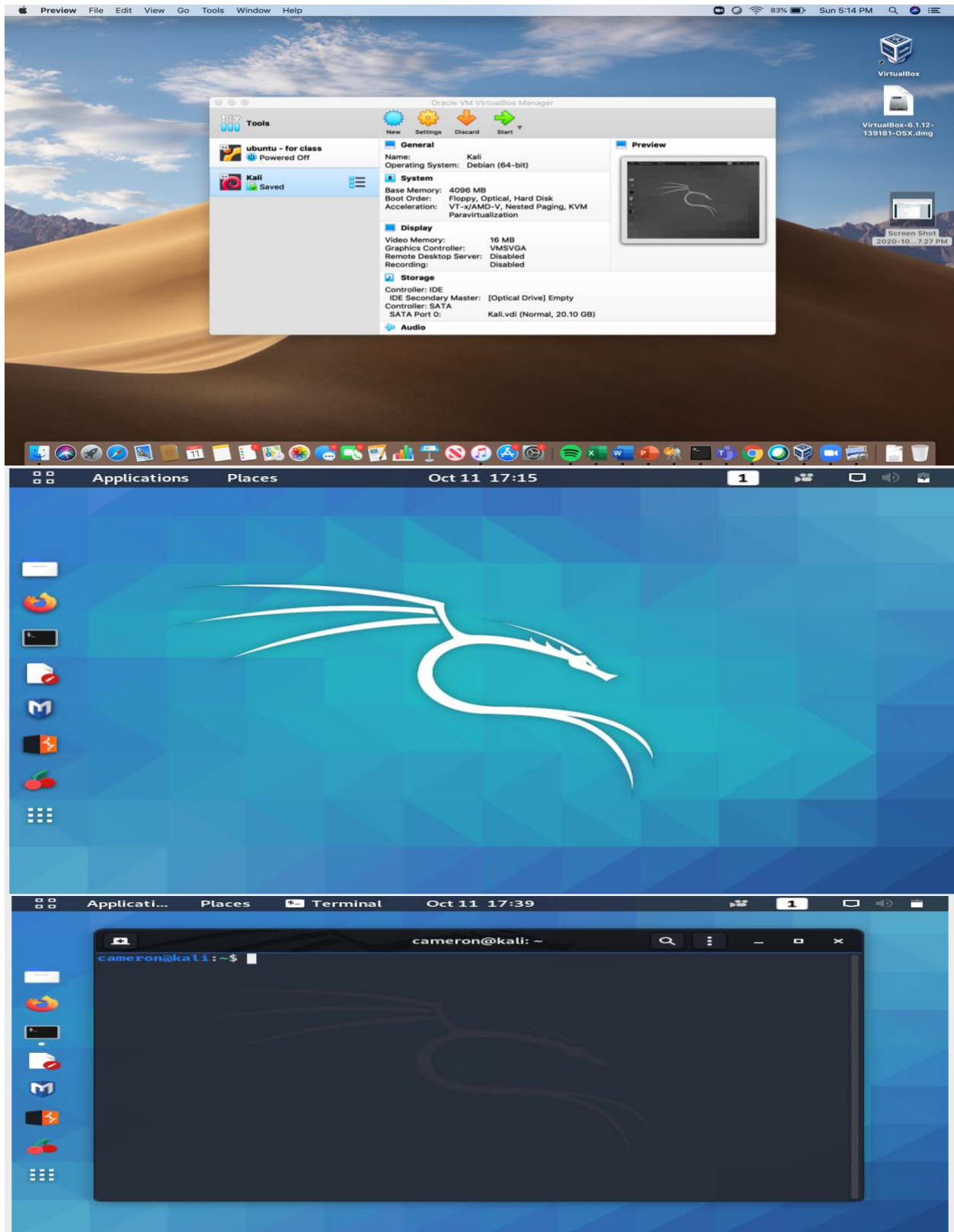
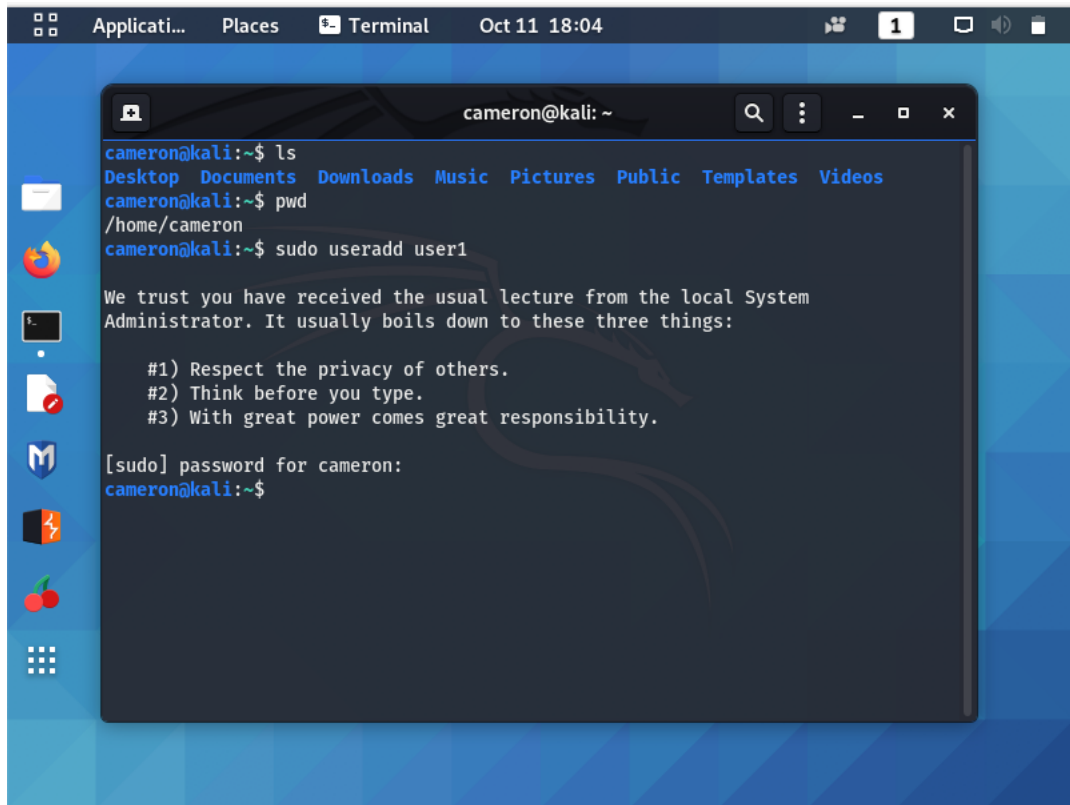


OLD DOMINION UNIVERSITY
CYSE 270 LINUX SYSTEM FOR CYBERSECURITY
Assignment #6
Task A – Password Cracking
Cameron Stegura
01160817

Step 1- I set up a kali linux vm and opened a terminal window.



Step 2- Adding users: user1, user2, user3, user4, user5, user6.



A terminal window titled 'cameron@kali: ~' is open on a Kali Linux desktop. The window shows the following commands and output:

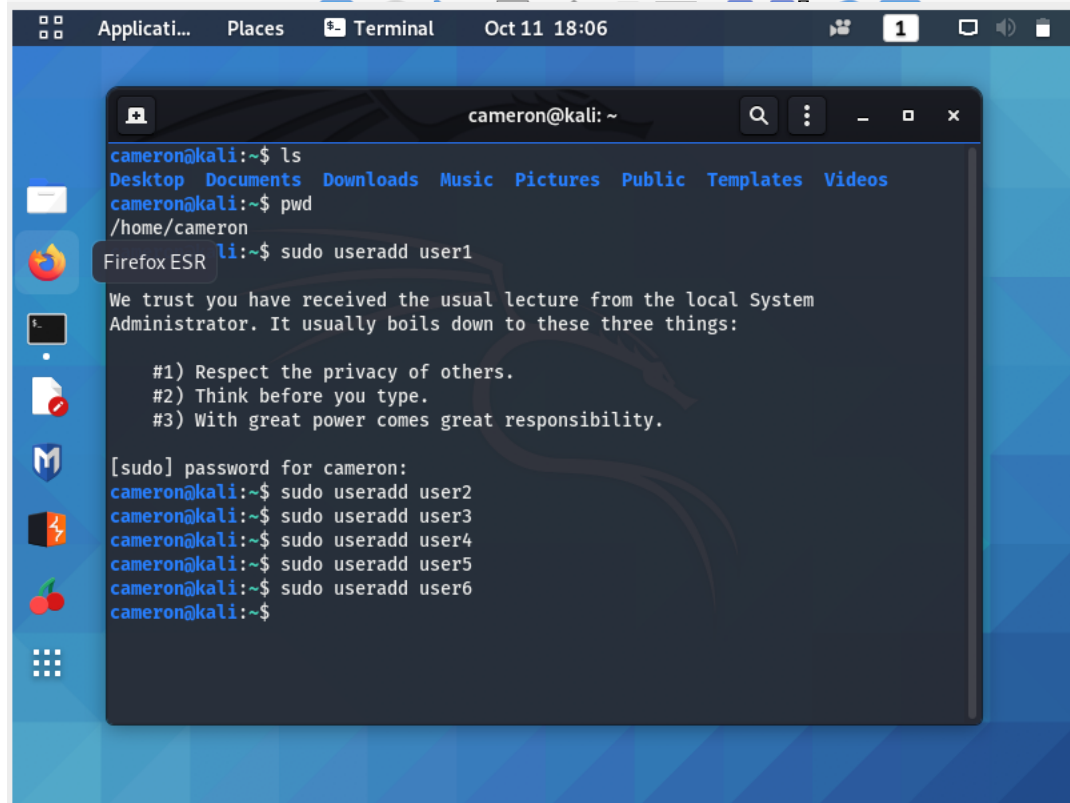
```
cameron@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
cameron@kali:~$ pwd
/home/cameron
cameron@kali:~$ sudo useradd user1
```

The output of the `sudo useradd user1` command is displayed:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for cameron:
cameron@kali:~$
```



A terminal window titled 'cameron@kali: ~' is open on a Kali Linux desktop. The window shows the following commands and output:

```
cameron@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
cameron@kali:~$ pwd
/home/cameron
li:~$ sudo useradd user1
```

The output of the `sudo useradd user1` command is displayed:

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for cameron:
cameron@kali:~$ sudo useradd user2
cameron@kali:~$ sudo useradd user3
cameron@kali:~$ sudo useradd user4
cameron@kali:~$ sudo useradd user5
cameron@kali:~$ sudo useradd user6
cameron@kali:~$
```

Step 3- I wrote down passwords for the users.

User1 – circle

User2 – circle123

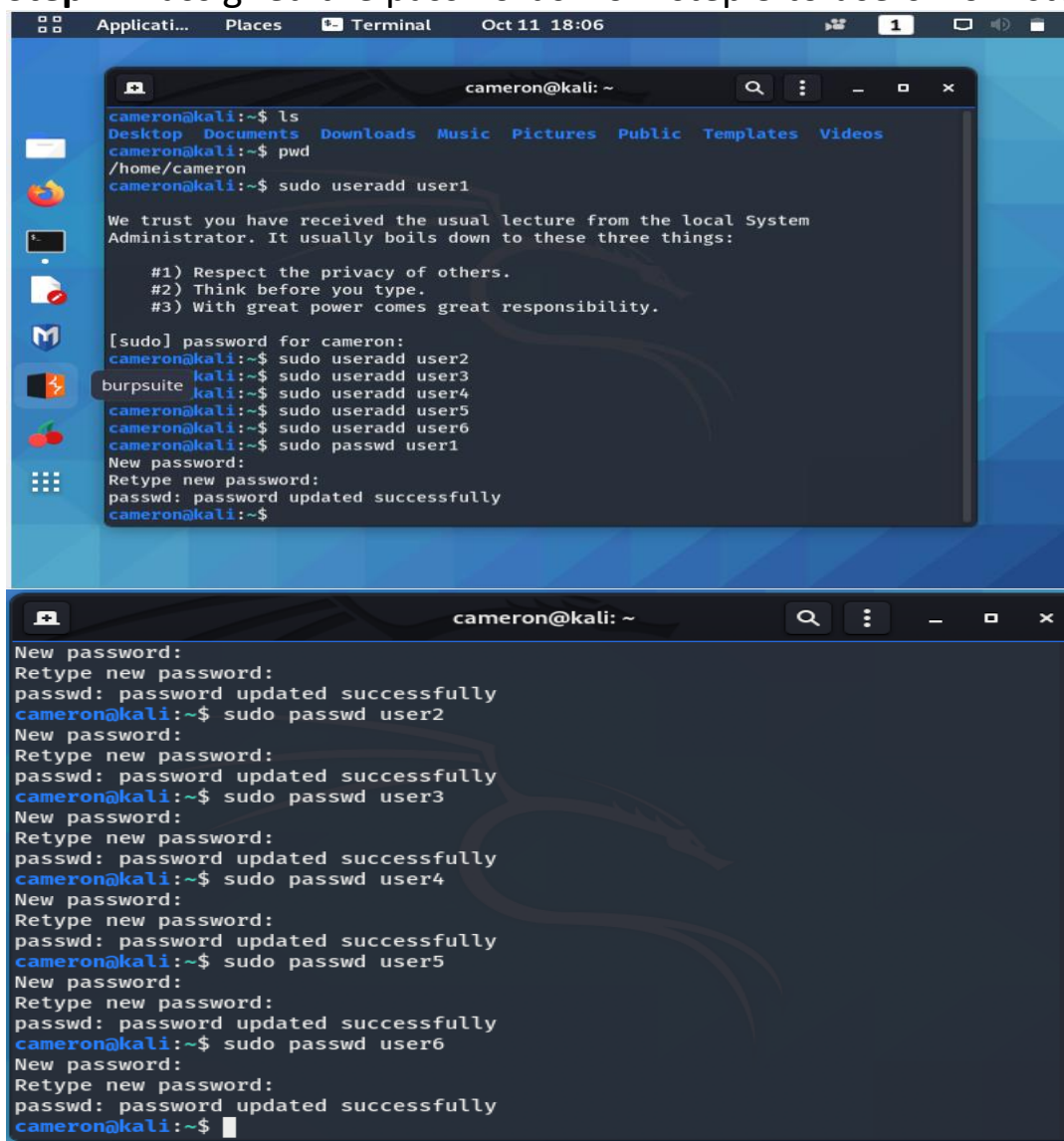
User3 - apple!

User4 – banana567

User5 – square\$

User6 – straw159!

Step 4- I assigned the passwords from step 3 to users from step 2.



The image shows two screenshots of a Kali Linux terminal window. The top screenshot shows the user 'cameron' running 'ls' to list files, then 'pwd' to show the current directory is '/home/cameron'. They then run 'sudo useradd user1', which prompts for a password for 'cameron'. After that, they run 'sudo useradd user2' through 'sudo useradd user6', and finally 'sudo passwd user1'. The bottom screenshot continues from the previous one, showing the password setting process for users 2 through 6. Each time 'sudo passwd' is run, it prompts for a new password and a retyped new password, followed by a confirmation message 'passwd: password updated successfully'.

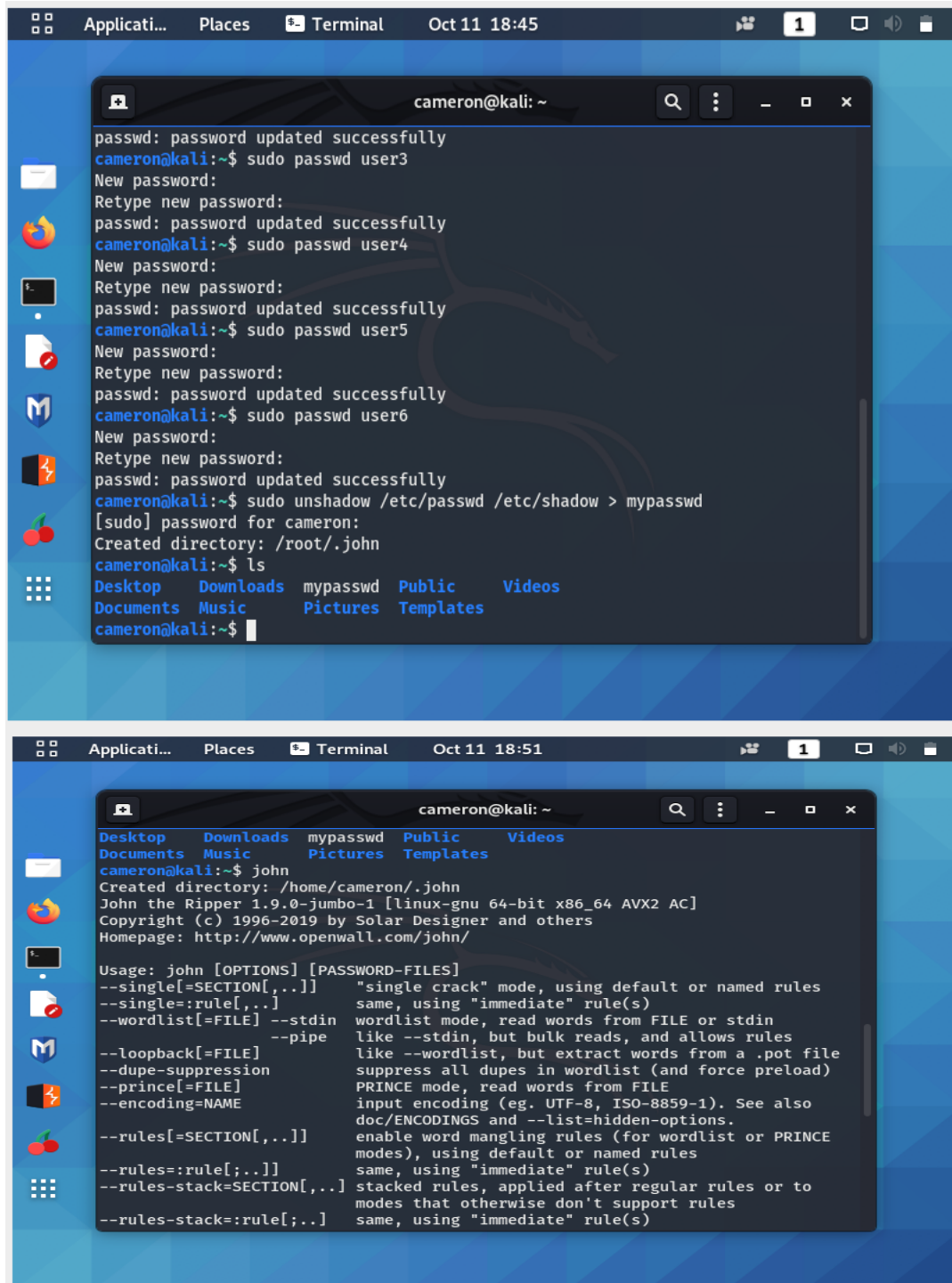
```
cameron@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
cameron@kali:~$ pwd
/home/cameron
cameron@kali:~$ sudo useradd user1

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for cameron:
cameron@kali:~$ sudo useradd user2
kali:~$ sudo useradd user3
kali:~$ sudo useradd user4
cameron@kali:~$ sudo useradd user5
cameron@kali:~$ sudo useradd user6
cameron@kali:~$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
cameron@kali:~$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
cameron@kali:~$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
cameron@kali:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
cameron@kali:~$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully
cameron@kali:~$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
cameron@kali:~$
```

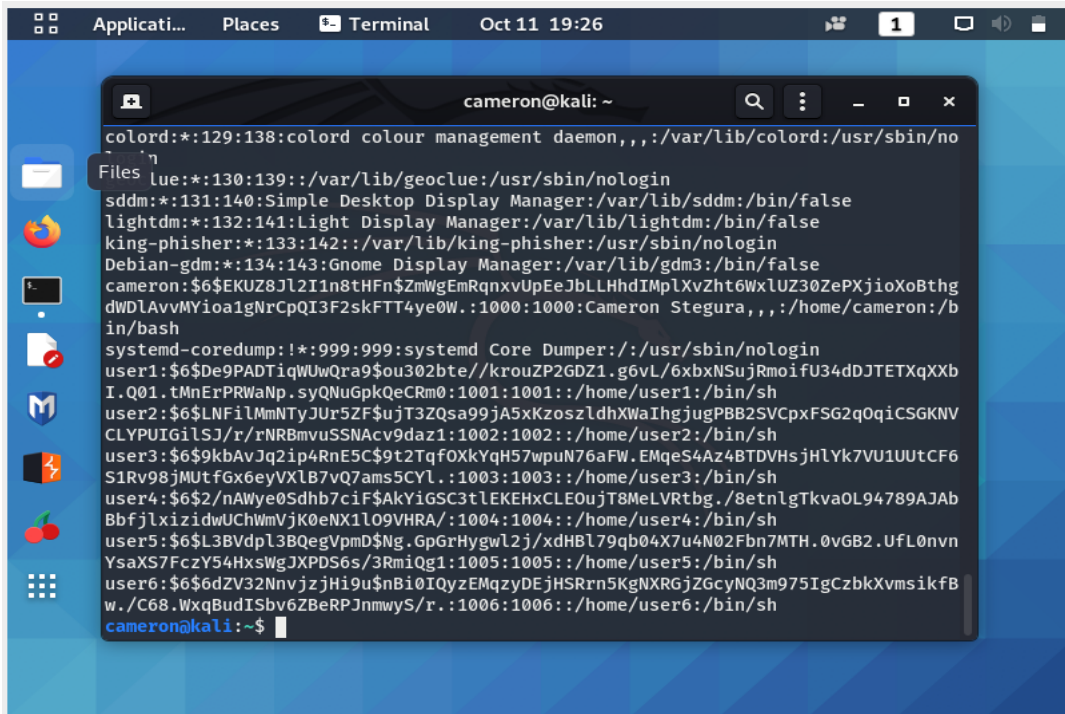
Step 5- I encrypted the passwords and then cracked them using John the Ripper.



The image consists of two screenshots of a Kali Linux desktop environment, specifically the terminal window. The top screenshot shows the user 'cameron' performing a series of password updates for users 3 through 6 using the 'passwd' command. After updating the passwords, the user runs 'sudo unshadow /etc/passwd /etc/shadow > mypasswd', which creates a directory '/root/.john'. The bottom screenshot shows the user running 'john' to start John the Ripper. The terminal displays the John the Ripper version (1.9.0-jumbo-1) and its usage instructions, including options for single crack, wordlist, loopback, dupe-suppression, prince, encoding, and rules.

```
cameron@kali: ~  
passwd: password updated successfully  
cameron@kali:~$ sudo passwd user3  
New password:  
Retype new password:  
passwd: password updated successfully  
cameron@kali:~$ sudo passwd user4  
New password:  
Retype new password:  
passwd: password updated successfully  
cameron@kali:~$ sudo passwd user5  
New password:  
Retype new password:  
passwd: password updated successfully  
cameron@kali:~$ sudo passwd user6  
New password:  
Retype new password:  
passwd: password updated successfully  
cameron@kali:~$ sudo unshadow /etc/passwd /etc/shadow > mypasswd  
[sudo] password for cameron:  
Created directory: /root/.john  
cameron@kali:~$ ls  
Desktop  Downloads  mypasswd  Public    Videos  
Documents Music      Pictures  Templates  
cameron@kali:~$  
  
cameron@kali: ~  
Desktop  Downloads  mypasswd  Public    Videos  
Documents Music      Pictures  Templates  
cameron@kali:~$ john  
Created directory: /home/cameron/.john  
John the Ripper 1.9.0-jumbo-1 [linux-gnu 64-bit x86_64 AVX2 AC]  
Copyright (c) 1996-2019 by Solar Designer and others  
Homepage: http://www.openwall.com/john/  
  
Usage: john [OPTIONS] [PASSWORD-FILES]  
--single[=SECTION[,...]] "single crack" mode, using default or named rules  
--single=:rule[,...] same, using "immediate" rule(s)  
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin  
--pipe like --stdin, but bulk reads, and allows rules  
--loopback[=FILE] like --wordlist, but extract words from a .pot file  
--dupe-suppression suppress all dupes in wordlist (and force preload)  
--prince[=FILE] PRINCE mode, read words from FILE  
--encoding=NAME input encoding (eg. UTF-8, ISO-8859-1). See also  
doc/ENCODINGS and --list-hidden-options.  
--rules[=SECTION[,...]] enable word mangling rules (for wordlist or PRINCE  
modes), using default or named rules  
--rules=:rule[;...]] same, using "immediate" rule(s)  
--rules-stack=SECTION[,...] stacked rules, applied after regular rules or to  
modes that otherwise don't support rules  
--rules-stack=:rule[;...]] same, using "immediate" rule(s)
```

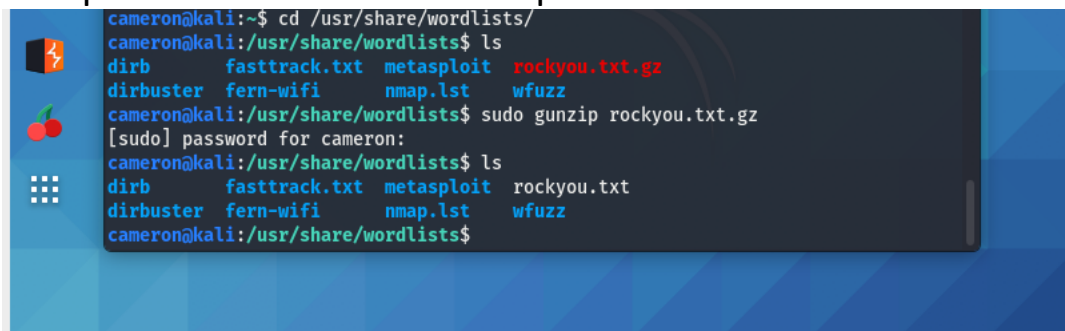
In this picture I saw what John could do.



A terminal window on a Kali Linux desktop. The window title is 'cameron@kali: ~'. The terminal output shows the contents of the /etc/passwd file, listing system users like colord, lue, sddm, lightdm, king-phisher, and regular users like cameron, systemd-coredump, and user1 through user6. The entry for cameron is: cameron:\$6\$EKU8JL2I1n8tHFn\$ZmWgEmRqnxvUpEeJbLLHhdIMpLXvZht6WxLUZ30ZePXjioXoBthgdWDLAvvMYioalgnrCpQI3F2skFTT4ye0W.:1000:1000:Cameron Stegura,,,:/home/cameron:/bin/bash.

```
colord::129:138:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
lue::130:139::/var/lib/geoclue:/usr/sbin/nologin
sddm::131:140:Simple Desktop Display Manager:/var/lib/sddm:/bin/false
lightdm::132:141:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher::133:142::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm::134:143:Gnome Display Manager:/var/lib/gdm3:/bin/false
cameron:$6$EKU8JL2I1n8tHFn$ZmWgEmRqnxvUpEeJbLLHhdIMpLXvZht6WxLUZ30ZePXjioXoBthgdWDLAvvMYioalgnrCpQI3F2skFTT4ye0W.:1000:1000:Cameron Stegura,,,:/home/cameron:/bin/bash
systemd-coredump:!:999:999:systemd Core Dumper:/usr/sbin/nologin
user1:$6$De9PADTiqWUwQra9$ou302bte//krouZP2GDZ1.g6vL/6xbxNSujRmoifU34dDJTETXqXXbI.Q01.tMnErPRWaNp.syQNuGpkQeCRm0:1001:1001::/home/user1:/bin/sh
user2:$6$LNfILmMnTyJUr5ZF$uJt3ZQsa99jA5xKzoszldhXWaIhgjugPBB2SVCpxFSG2q0qiCSGKNVCLYPUIGilSJ/r/rNRBmvuSSNAcv9daz1:1002:1002::/home/user2:/bin/sh
user3:$6$9kbAvJq2ip4RnE5C$9t2TqfOXkYqH57wpuN76aFW.EMqeS4Az4BTDVHsjHLYk7VU1UUTCF6S1Rv98jMutfGx6eyVXL7vQ7ams5CYL.:1003:1003::/home/user3:/bin/sh
user4:$6$2/nAWye0Sdnh7ciF$AkYiGSC3tLEKEHxCLE0ujT8MeLVrtbg./8etnlgTkva0L94789AJABBbfjLxizidwUChWmVjK0eNX1l09VHRA/:1004:1004::/home/user4:/bin/sh
user5:$6$L3BVdpl3BQegVpmD$Ng.GpGrHygwl2j/xdHBL79qb04X7u4N02Fbn7MTH.0vGB2.UfL0nvnYsaXS7FcZy54HxswGJXPDS6s/3RmiQg1:1005:1005::/home/user5:/bin/sh
user6:$6$dZV32NnvjzjHi9u$nBi0IQzyEMqzyDEjHSRrn5KgNXRGjZGcyNQ3m975IgCzbkXvmsikfBw./C68.WxqBudISbv6ZBeRPJnmwyS/r.:1006:1006::/home/user6:/bin/sh
cameron@kali:~$
```

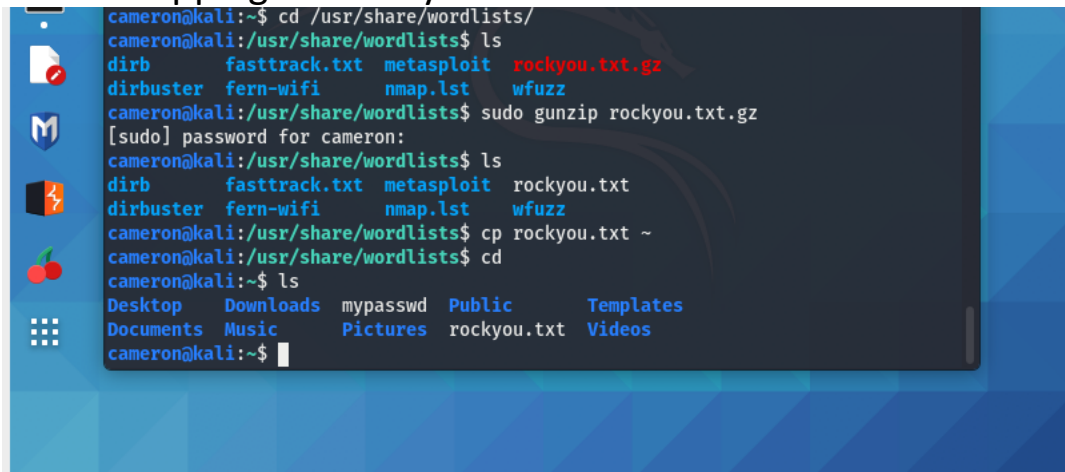
This picture shows the hashed passwords.



A terminal window showing the user navigating to /usr/share/wordlists/. The user lists files (dirb, fasttrack.txt, metasploit, rockyou.txt.gz, dirbuster, fern-wifi, nmap.lst, wfuzz) and then runs 'sudo gunzip rockyou.txt.gz'. After entering the password, the file is unzipped. The user then lists the files again, showing that rockyou.txt now exists alongside the other files.

```
cameron@kali:~$ cd /usr/share/wordlists/
cameron@kali:/usr/share/wordlists$ ls
dirb      fasttrack.txt  metasploit    rockyou.txt.gz
dirbuster fern-wifi      nmap.lst      wfuzz
cameron@kali:/usr/share/wordlists$ sudo gunzip rockyou.txt.gz
[sudo] password for cameron:
cameron@kali:/usr/share/wordlists$ ls
dirb      fasttrack.txt  metasploit    rockyou.txt
dirbuster fern-wifi      nmap.lst      wfuzz
cameron@kali:/usr/share/wordlists$
```

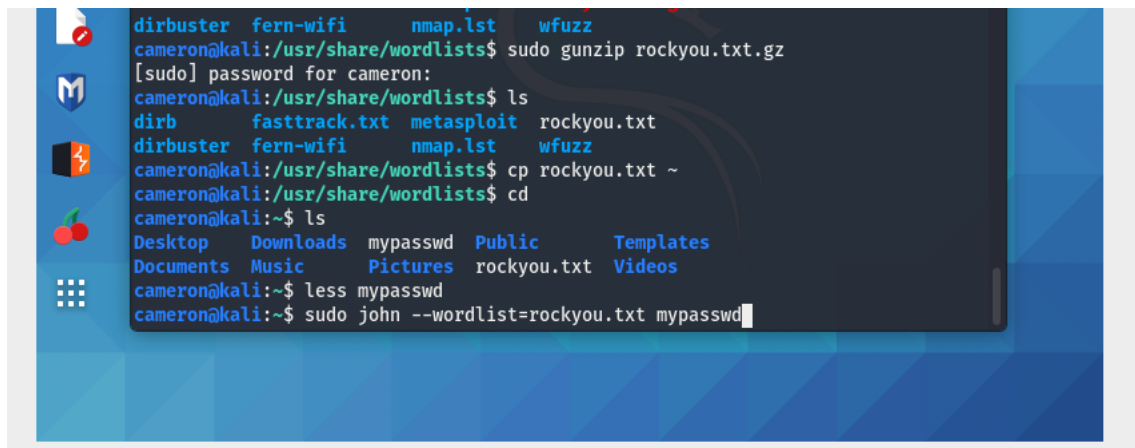
I was unzipping the rockyou.txt file.



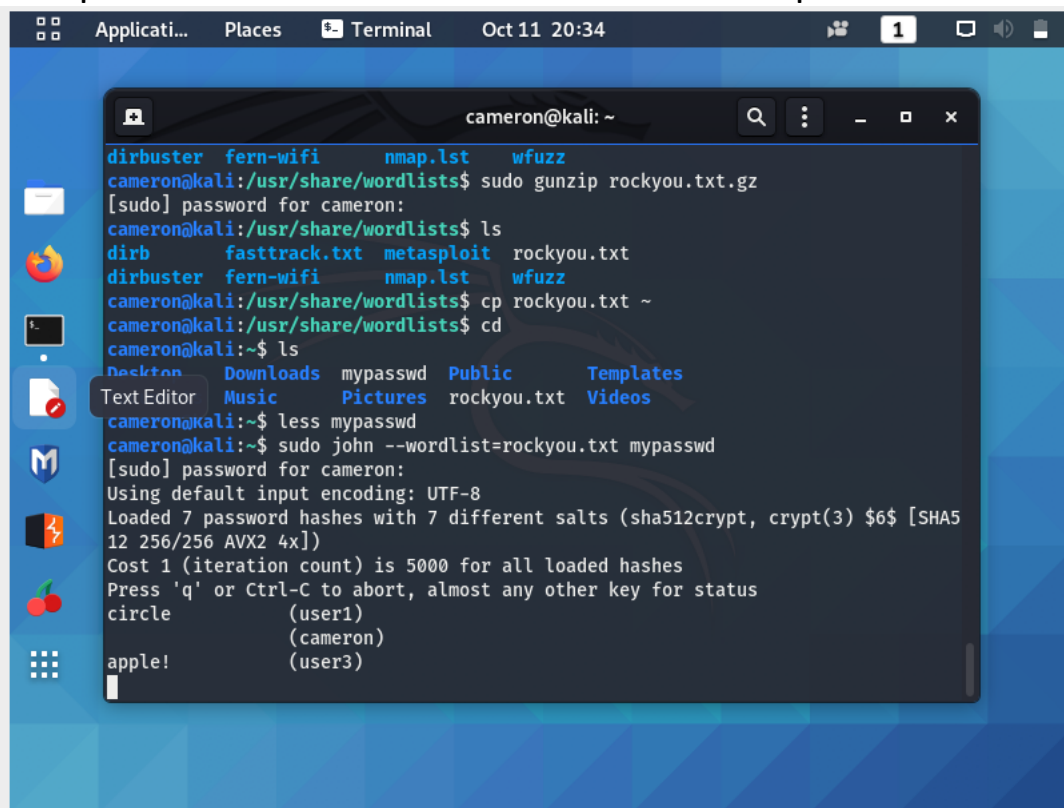
A terminal window showing the user copying the rockyou.txt file to their home directory. The user runs 'cp rockyou.txt ~' and then 'cd' to return to the home directory. A final 'ls' command shows the file is now in the home directory alongside other files like Desktop, Downloads, mypasswd, Public, Templates, Documents, Music, Pictures, and Videos.

```
cameron@kali:~$ cd /usr/share/wordlists/
cameron@kali:/usr/share/wordlists$ ls
dirb      fasttrack.txt  metasploit    rockyou.txt.gz
dirbuster fern-wifi      nmap.lst      wfuzz
cameron@kali:/usr/share/wordlists$ sudo gunzip rockyou.txt.gz
[sudo] password for cameron:
cameron@kali:/usr/share/wordlists$ ls
dirb      fasttrack.txt  metasploit    rockyou.txt
dirbuster fern-wifi      nmap.lst      wfuzz
cameron@kali:/usr/share/wordlists$ cp rockyou.txt ~
cameron@kali:/usr/share/wordlists$ cd
cameron@kali:~$ ls
Desktop  Downloads  mypasswd  Public    Templates
Documents Music      Pictures  rockyou.txt Videos
cameron@kali:~$
```

This picture I was copying the rockyou.txt file into the home directory.

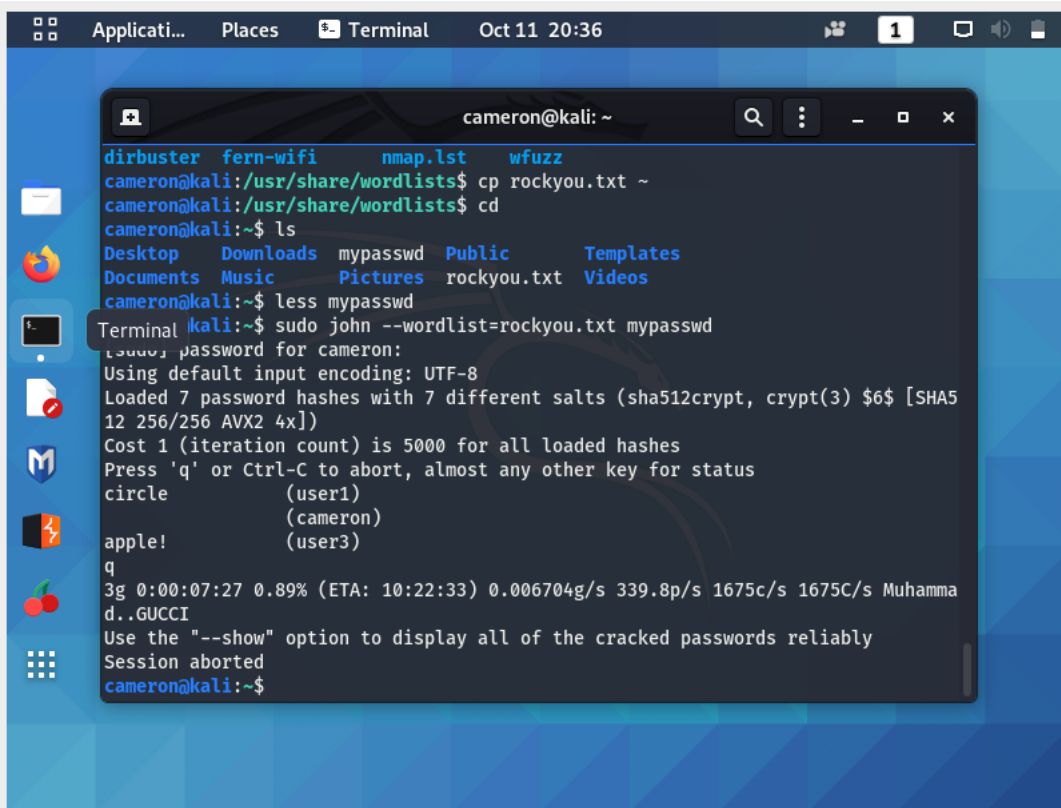


This picture shows the command to crack the passwords.



I am about to end the process in this picture.

Step 6- THE RESULTS – it was only able to crack the password for user1 (the password is circle) and user3 (the password is apple!).



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the following commands and output:

```
cameron@kali: ~  
dirbuster fern-wifi nmap.lst wfuzz  
cameron@kali:/usr/share/wordlists$ cp rockyou.txt ~  
cameron@kali:/usr/share/wordlists$ cd  
cameron@kali:~$ ls  
Desktop Downloads mypasswd Public Templates  
Documents Music Pictures rockyou.txt Videos  
cameron@kali:~$ less mypasswd  
Terminal kali:~$ sudo john --wordlist=rockyou.txt mypasswd  
[50000] password for cameron:  
Using default input encoding: UTF-8  
Loaded 7 password hashes with 7 different salts (sha512crypt, crypt(3) $6$ [SHA5  
12 256/256 AVX2 4x])  
Cost 1 (iteration count) is 5000 for all loaded hashes  
Press 'q' or Ctrl-C to abort, almost any other key for status  
circle (user1)  
 (cameron)  
apple! (user3)  
q  
3g 0:00:07:27 0.89% (ETA: 10:22:33) 0.006704g/s 339.8p/s 1675c/s 1675C/s Muhamma  
d..GUCCI  
Use the "--show" option to display all of the cracked passwords reliably  
Session aborted  
cameron@kali:~$
```