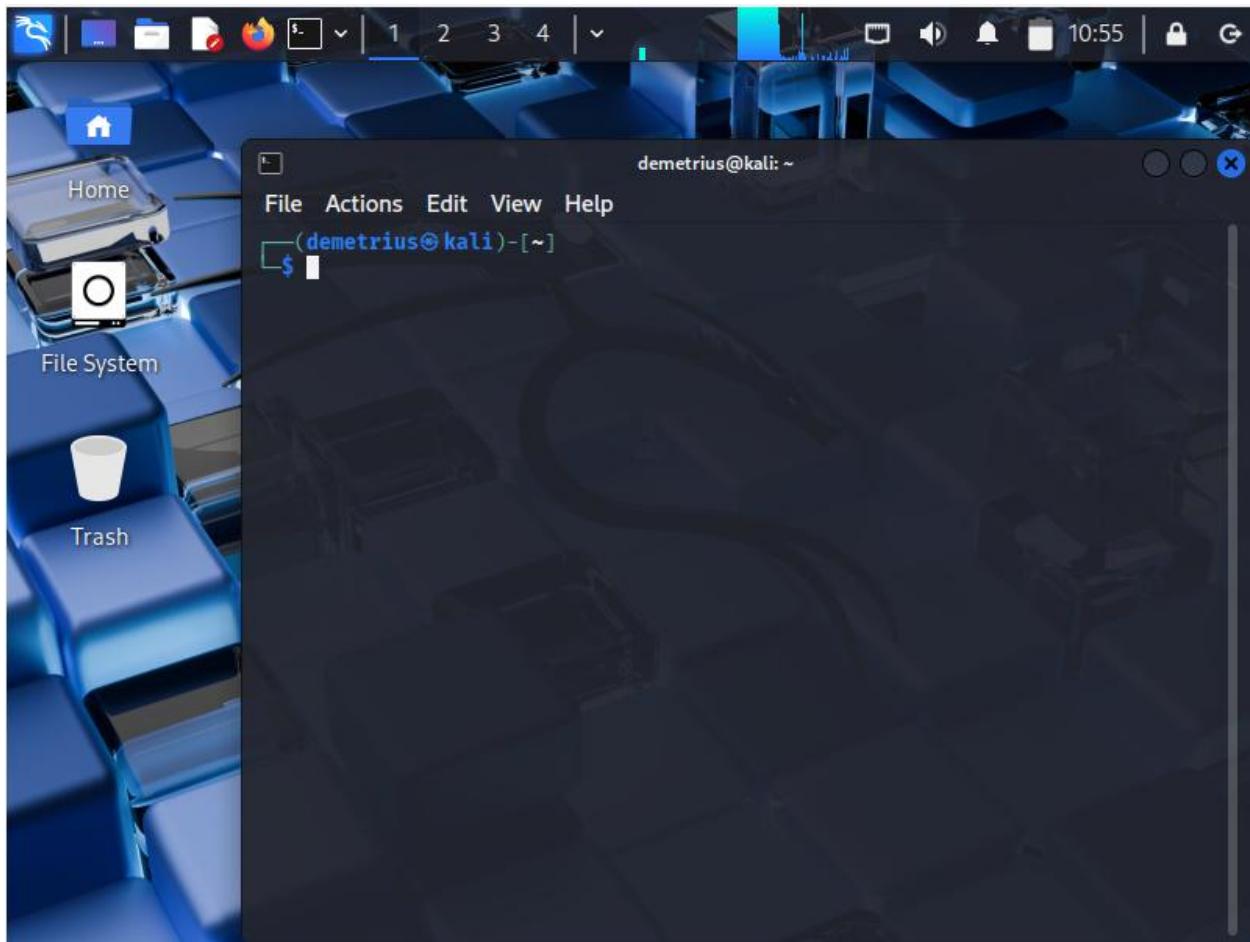


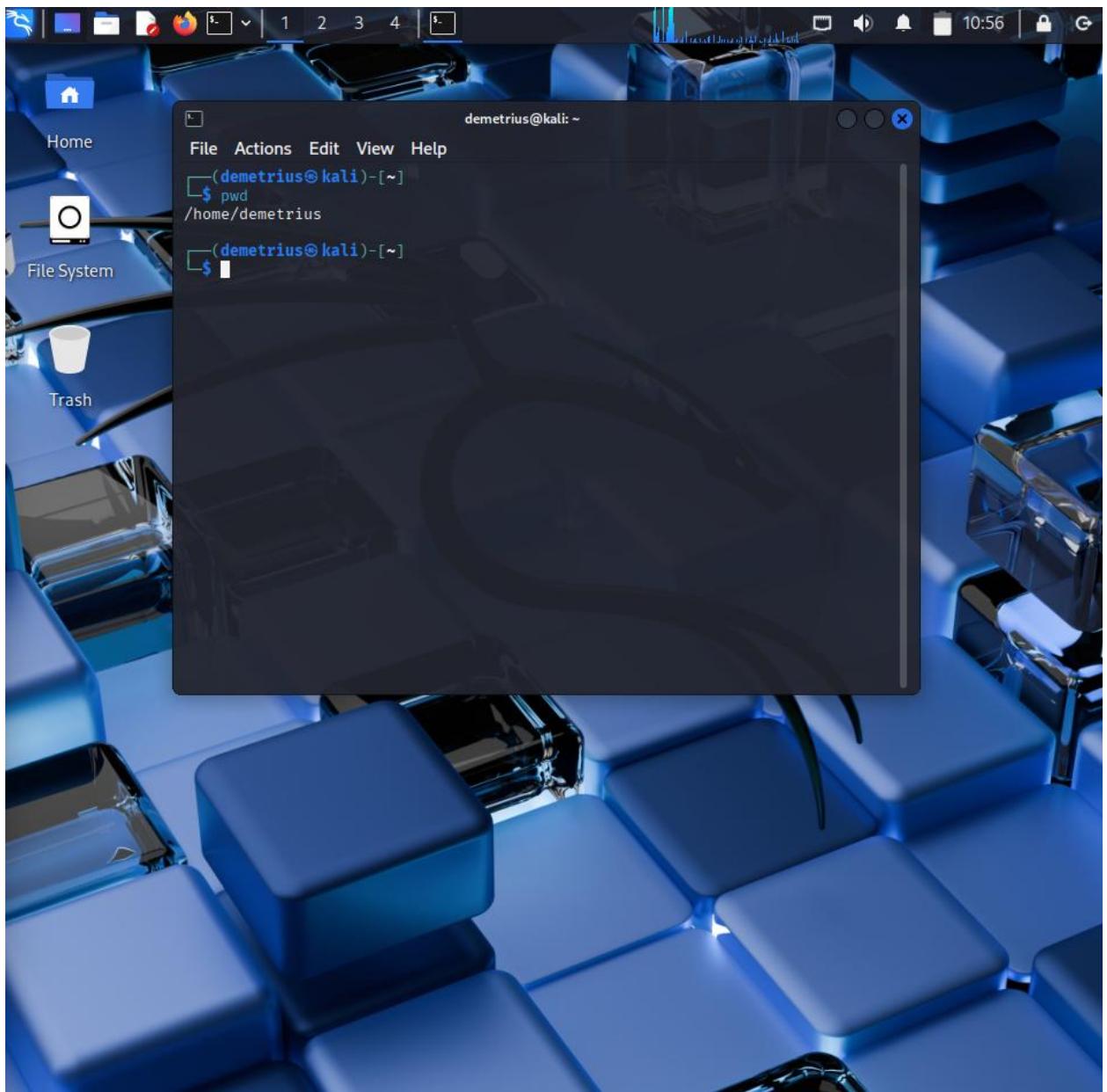
Lab Assignment 2

Steps:

1)



2)



3)

4)

demetrius@kali: /etc/skel

```
File Actions Edit View Help
(demetrius@kali)-[~]
$ pwd
/home/demetrius

(demetrius@kali)-[~]
$ cd /etc
(demetrius@kali)-[/etc] Help
$ cd skel
(demetrius@kali)-[/etc/skel]

$ ls
bin  binfmt.d  dev  etc  lib  lib32  lib64  libx32  libx64  mnt  proc  root  run  sbin  sys  tmp  var

(demetrius@kali)-[/etc/skel]
$ cd ..
(demetrius@kali)-[/home]
$ cd ..
(demetrius@kali)-[~]
$ cd bin
cd: no such file or directory: bin

$ cd documents
cd: no such file or directory: documents

(demetrius@kali)-[~]
$ cd Documents
(demetrius@kali)-[~/Documents]
```

5)

```
demetrius@kali: /etc
File Actions Edit View Help
(demetrius@kali)-[~]
$ pwd
/
(demetrius@kali)-[~]
$ pwd
/
(demetrius@kali)-[~]
$ cd /etc
(demetrius@kali)-[/etc]
$ cd skel
(demetrius@kali)-[/etc/skel]
$ cd ..
/home/demetrius
(demetrius@kali)-[/etc]
$ 

$ cd documents
cd: no such file or directory: documents

(demetrius@kali)-[~]
$ cd Documents
(demetrius@kali)-[~/Documents]
$ 
```

6)

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "demetrius@kali: /etc". The user has run the command "ls" to list the contents of the /etc directory. The output shows numerous configuration files and scripts, many of which are highlighted in red, likely due to being modified or being part of a exploit payload. Some of the files listed include ipsec.conf, radcli, rc0.d, rc1.d, rc2.d, rc3.d, rc4.d, rc5.d, rc6.d, rcs.d, reader.conf.d, rearj.cfg, redis, redsocks.conf, request-key.conf, request-key.d, resolv.conf, responder, rmt, rpc, runit, samba, sane.d, scalpel, screenrc, sddm.conf.d, searchsploit_rc, security, selinux, sensors3.conf, sensors.d, sgml, shadow, shadow-, shells, skel, smartd.conf, smartmontools, smi.conf, snmp, speech-dispatcher, sqlmap, ssh, ssl, and sslsplit.

```
(demetrius㉿kali)-[~/etc/skel]
$ cd ..

(demetrius㉿kali)-[~/etc]
$ ls
adduser.conf          ipsec.conf      python3.13
alternatives          ipsec.d        radcli
apache2               ipsec.secrets   rc0.d
apparmor              issue          rc1.d
apparmor.d            issue.net     rc2.d
apt                   java-21-openjdk rc3.d
arp-scan              john          rc4.d
avahi                 kali-menu     rc5.d
bash.bashrc           kernel         rc6.d
bash_completion       kernel-img.conf rcs.d
bash_completion.d    keyutils       reader.conf.d
bindresport.blacklist kismet        rearj.cfg
binfmt.d              ldap          redis
bluetooth             ld.so.cache   redsocks.conf
ca-certificates       ld.so.conf    request-key.conf
ca-certificates.conf  ld.so.conf.d  request-key.d
chatscripts           legion.conf   resolv.conf
chromium              libaudit.conf responder
chromium.d            libao.conf    rmt
cifs-utils            libblockdev   rpc
cloud                 libccid.plist runit
colord                libl10n-3    samba
console-setup         libpaper.d   sane.d
cracklib              lightdm       scalpel
credstore             lighttpd      screenrc
credstore.encrypted   locale.alias  sddm.conf.d
cron.d                locale.conf   searchsploit_rc
cron.daily             locale.gen    security
cron.hourly            localtime   selinux
cron.monthly           logcheck     sensors3.conf
cron.weekly            login.defs   sensors.d
cron.yearly            logrotate.conf services
cryptsetup-initramfs  macchanger   sgml
cryptsetup-nuke-password machine-id  shadow
crypttab              magic        shadow-
cupshelpers           magic.mime   shells
dbus-1                manpath.config skel
dconf                 matplotlibrc smartmontools
debconf.conf          mime.types   smi.conf
debian_version        minicom     snmp
default               miredo      speech-dispatcher
deluser.conf          miredo.conf  sqlmap
depmod.d              mke2fs.conf  ssh
dhcpc                ModemManager  ssl
dhcpcd.conf           modprobe.d  sslsplit
```

7)

The screenshot shows a terminal window titled "demetrius@kali: /etc". The window contains a file listing command output:

```
File Actions Edit View Help
eac ld.so.cache opensc shadow xfce4
emacs ld.so.conf openvas shadow-
environment ld.so.conf.d legion.conf opt shells xml
environment.d libao.conf os-release smartd.conf smartmontools xrdp
ethertypes libaudit.conf pam.conf smi.conf zsh
ettercap libblockdev pam.d zsh_command_not_found
firebird

(demetrius@kali)-[~/etc]
$ ls -l
total 1508
-rw-r--r-- 1 root root 3981 May 6 14:25 adduser.conf
drwxr-xr-x 2 root root 20480 Aug 28 12:04 alternatives
drwxr-xr-x 8 root root 4096 Aug 28 12:03 apache2
drwxr-xr-x 2 root root 4096 Aug 28 11:53 apparmor
drwxr-xr-x 9 root root 4096 Aug 28 12:03 apparmor.d
drwxr-xr-x 8 root root 4096 Aug 28 12:06 apt
drwxr-xr-x 2 root root 4096 Aug 28 12:00 arp-scan
drwxr-xr-x 3 root root 4096 Aug 28 12:02 avahi
-rw-r--r-- 1 root root 1997 May 19 14:11 bash.bashrc
```

8)

demetrius@kali: /etc

```

File Actions Edit View Help
drwxr-xr-x 2 root      root      4096 Aug 28 12:04 sudoers.d
-rw-r--r-- 1 root      root      9804 May  4 11:48 sudo_logsvrd.conf
drwxr-xr-x 2 root      root      4096 Aug 28 11:53 supercat
drwxr-xr-x 4 root      root      4096 Aug 28 11:55 sv
drwxr-xr-x 2 root      root      4096 Aug 28 11:53 sysctl.d
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 sysstat
drwxr-xr-x 5 root      root      4096 Aug 28 12:00 systemd
drwxr-xr-x 2 root      root      4096 Aug 28 11:53 terminfo
drwxr-xr-x 8 root      root      4096 Aug 28 12:00 texmf
drwxr-xr-x 3 root      root      4096 Aug 28 12:03 theHarvester
-rw-r--r-- 1 root      root      1493 Jul  5 2024 tightvncserver.conf
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 timidity
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 tmpfiles.d
-rw-r--r-- 1 root      root      938 Sep  9 2019 ts.conf
-rw-r--r-- 1 root      root      1259 Mar 31 05:25 ucf.conf
drwxr-xr-x 4 root      root      4096 Aug 28 11:53 udev
drwxr-xr-x 2 root      root      4096 Aug 28 12:04 udisks2
drwxr-xr-x 3 root      root      4096 Aug 28 11:55 ufw
drwxr-xr-x 2 root      root      4096 Aug 28 12:01 unicornscan
-rw-r--r-- 1 root      root      583 Nov 21 2022 updatedb.conf
drwxr-xr-x 2 root      root      4096 Aug 28 11:53 update-motd.d
drwxr-xr-x 2 root      root      4096 Aug 28 12:03 UPower
-rw-r--r-- 1 root      root      1523 Feb  1 2025 usb_modeswitch.conf
drwxr-xr-x 2 root      root      4096 May 24 2024 usb_modeswitch.d
lrwxrwxrwx 1 root      root      16 Aug 28 11:53 vconsole.conf → default/keyboard
-rw-r--r-- 1 root      root      51 Mar  7 2022 vdpaui_wrapper.cfg
drwxr-xr-x 2 root      root      4096 Aug 28 11:53 vim
drwx----- 2 root      root      4096 Aug 28 12:02 vpnc
drwxr-xr-x 5 root      root      4096 Aug 28 11:55 vulkan
-rw-r--r-- 1 root      root      4942 Mar  8 01:23 wgetrc
drwxr-xr-x 2 root      root      4096 Apr 17 16:48 wireshark
drwxr-xr-x 2 root      root      4096 Aug 28 12:02 wpa_supplicant
drwxr-xr-x 11 root     root      4096 Aug 28 12:03 X11
-rw-r--r-- 1 root      root      681 Feb 21 2025 xattr.conf
drwxr-xr-x 17 root     root      4096 Aug 28 12:03 xdg
drwxr-xr-x 2 root      root      4096 Aug 28 12:03 xfce4
drwxr-xr-x 2 root      root      4096 Aug 28 12:04 xml
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 xrdp
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 zsh
-rw-r--r-- 1 root      root      460 Jan 20 2023 zsh_command_not_found

└─(demetrius㉿kali)-[~/etc]
$ ls -d s*
samba      security      shadow      smi.conf      sslsplit      subuid      sudo_logsvrd.conf
sane.d      selinux       shadow-     snmp        strongswan.conf subuid-
scalpel    sensors3.conf shells      speech-dispatcher strongswan.d  subversion  supercat
screenrc   sensors.d      skel       sqlmap      stunnel       sudo.conf   sv
sddm.conf.d services      smartd.conf ssh        subgid       sudoers    sysctl.d
searchsploit_rc sgml       smartmontools ssl        subgid-     sudoers.d  sysstat
                                         smartmontools

└─(demetrius㉿kali)-[~/etc]
$ 
```

9)

```
demetrius@kali: /etc
File Actions Edit View Help
drwxr-xr-x 2 root      root      4096 Aug 28 12:04 xml
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 xrdp
drwxr-xr-x 2 root      root      4096 Aug 28 12:00 zsh
-rw-r--r-- 1 root      root      460 Jan 20 2023 zsh_command_not_found

└──(demetrius㉿kali)-[~/etc]
$ ls -d s*
samba      security      shadow      smi.conf      sslsplit      subuid      sudo_logsrvd.conf
sane.d     selinux       shadow-     snmp        strongswan.conf  subuid-    supercat
scalpel    sensors3.conf shells      speech-dispatcher  strongswan.d   subversion  sv
screenrc   sensors.d    skel       sqlmap       stunnel       sudo.conf   sysctl.d
sddm.conf.d services     smartd.conf ssh        subgid       sudoers    sysstat
searchsploit_rc sgml      smartmontools ssl        subgid-    sudoers.d  systemd

└──(demetrius㉿kali)-[~/etc]
$ file /etc/group
/etc/group: ASCII text

└──(demetrius㉿kali)-[~/etc]
$
```

10)

```
demetrius@kali: /etc
File Actions Edit View Help
sane.d     selinux      shadow-     snmp        strongswan.conf  subuid      supercat
scalpel    sensors3.conf shells      speech-dispatcher  strongswan.d   subversion  sv
screenrc   sensors.d    skel       sqlmap       stunnel       sudo.conf   sysctl.d
sddm.conf.d services     smartd.conf ssh        subgid       sudoers    sysstat
searchsploit_rc sgml      smartmontools ssl        subgid-    sudoers.d  systemd

└──(demetrius㉿kali)-[~/etc]
$ file /etc/group
/etc/group: ASCII text

└──(demetrius㉿kali)-[~/etc]
$ tail -n5 /etc/group
colord:x:131:
kali-trusted:x:132:
demetrius:x:1000:
vboxsf:x:133:demetrius
kaboxer:x:134:demetrius

└──(demetrius㉿kali)-[~/etc]
$
```

11)



demetrious@kali: ~

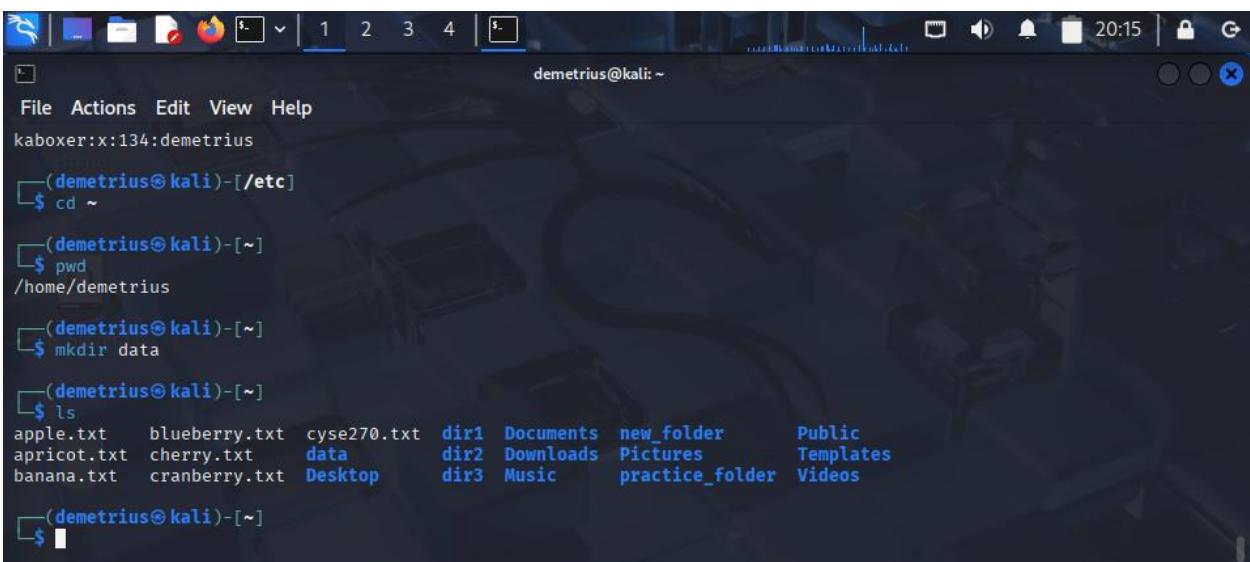
```
File Actions Edit View Help
sddm.conf.d services smartd.conf ssh subgid sudoers sysstat
searchsploit_rc sgml smartmontools ssl subgid-
(demetrius@kali)-[/etc]
$ file /etc/group
/etc/group: ASCII text

(demetrius@kali)-[/etc]
$ tail -n5 /etc/group
colord:x:131:
kali-trusted:x:132:
demetrius:x:1000:
vboxsf:x:133:demetrius
kabober:x:134:demetrius

(demetrius@kali)-[/etc]
$ cd ~

(demetrius@kali)-[~]
$
```

12)



demetrious@kali: ~

```
File Actions Edit View Help
kabober:x:134:demetrius

(demetrius@kali)-[/etc]
$ cd ~

(demetrius@kali)-[~]
$ pwd
/home/demetrius

(demetrius@kali)-[~]
$ mkdir data

(demetrius@kali)-[~]
$ ls
apple.txt blueberry.txt cyse270.txt dir1 Documents new_folder Public
apricot.txt cherry.txt data dir2 Downloads Pictures Templates
banana.txt cranberry.txt Desktop dir3 Music practice_folder Videos

(demetrius@kali)-[~]
$
```

13)

```
demetrius@kali: ~
File Actions Edit View Help
/home/demetrius
└──(demetrius@kali)-[~]
    $ mkdir data
    └──(demetrius@kali)-[~]
        $ ls
apple.txt  blueberry.txt  cyse270.txt  dir1  Documents  new_folder  Public
apricot.txt cherry.txt   data          dir2  Downloads  Pictures   Templates
banana.txt  cranberry.txt Desktop      dir3  Music     practice_folder  Videos
    └──(demetrius@kali)-[~]
        $ cp /etc/passwd data
    └──(demetrius@kali)-[~]
        $ ls data
passwd
    └──(demetrius@kali)-[~]
        $
```

14)

```
demetrius@kali: ~
File Actions Edit View Help
apricot.txt  cherry.txt   data          dir2  Downloads  Pictures   Templates
banana.txt  cranberry.txt Desktop      dir3  Music     practice_folder  Videos
    └──(demetrius@kali)-[~]
        $ ls -d p*
practice_folder
    └──(demetrius@kali)-[~]
        $ cp -r /etc/ppp .
cp: cannot open '/etc/ppp/pap-secrets' for reading: Permission denied
cp: cannot open '/etc/ppp/chap-secrets' for reading: Permission denied
    └──(demetrius@kali)-[~]
        $ ls
apple.txt  blueberry.txt  cyse270.txt  dir1  Documents  new_folder  practice_folder  Videos
apricot.txt cherry.txt   data          dir2  Downloads  Pictures   Public
banana.txt  cranberry.txt Desktop      dir3  Music     ppp       Templates
    └──(demetrius@kali)-[~]
        $
```

15) and 16)

demetrius@kali: ~

```
File Actions Edit View Help
cp: cannot open '/etc/ppp/pap-secrets' for reading: Permission denied
cp: cannot open '/etc/ppp/chap-secrets' for reading: Permission denied

(demetrius@kali)-[~]
$ ls
apple.txt blueberry.txt cyse270.txt dir1 Documents new_folder practice_folder Videos
apricot.txt cherry.txt data dir2 Downloads Pictures Public
banana.txt cranberry.txt Desktop dir3 Music ppp Templates

(demetrius@kali)-[~]
$ mv /home/demetrius/PPP peers

(demetrius@kali)-[~]
$ ls
apple.txt blueberry.txt cyse270.txt dir1 Documents new_folder practice_folder Videos
apricot.txt cherry.txt data dir2 Downloads peers Public
banana.txt cranberry.txt Desktop dir3 Music Pictures Templates

(demetrius@kali)-[~]
$ 
```

17)

demetrius@kali: ~/data

```
File Actions Edit View Help
banana.txt cranberry.txt Desktop dir3 Music ppp Templates

(demetrius@kali)-[~]
$ mv /home/demetrius/PPP peers

(demetrius@kali)-[~]
$ ls
apple.txt blueberry.txt cyse270.txt dir1 Documents new_folder practice_folder Videos
apricot.txt cherry.txt data dir2 Downloads peers Public
banana.txt cranberry.txt Desktop dir3 Music Pictures Templates

(demetrius@kali)-[~]
$ cd data ; touch test

(demetrius@kali)-[~/data]
$ ls
passwd test

(demetrius@kali)-[~/data]
$ 
```

18)

The screenshot shows a terminal window with a dark blue background. At the top, there is a menu bar with "File", "Actions", "Edit", "View", and "Help". The title bar indicates the user is "demetrius@kali: ~/data". The terminal window contains the following session:

```
(demetrius@kali)-[~]
$ cd data
(demetrius@kali)-[~/data]
$ touch passwd
(demetrius@kali)-[~/data]
$ ls
passwd test
(demetrius@kali)-[~/data]
$ rm passwd
(demetrius@kali)-[~/data]
$ ls
test
(demetrius@kali)-[~/data]
$
```

19) & 20)

This screenshot continues the terminal session from the previous one. The user has navigated to the root directory (~) and deleted the "passwd" file. They then listed the contents of the current directory, which includes a folder named "peers". Finally, they listed the contents of the root directory (~), showing various files and folders like "apple.txt", "blueberry.txt", "cyse270.txt", etc.

```
Applications File Actions Edit View Help
$ rm passwd
(demetrius@kali)-[~/data]
$ ls
test
(demetrius@kali)-[~/data]
$ cd ..
(demetrius@kali)-[~]
$ rm -r peers/
(demetrius@kali)-[~]
$ ls
apple.txt blueberry.txt cyse270.txt dir1 Documents new_folder Public
apricot.txt cherry.txt data dir2 Downloads Pictures Templates
banana.txt cranberry.txt Desktop dir3 Music practice_folder Videos
(demetrius@kali)-[~]
$
```