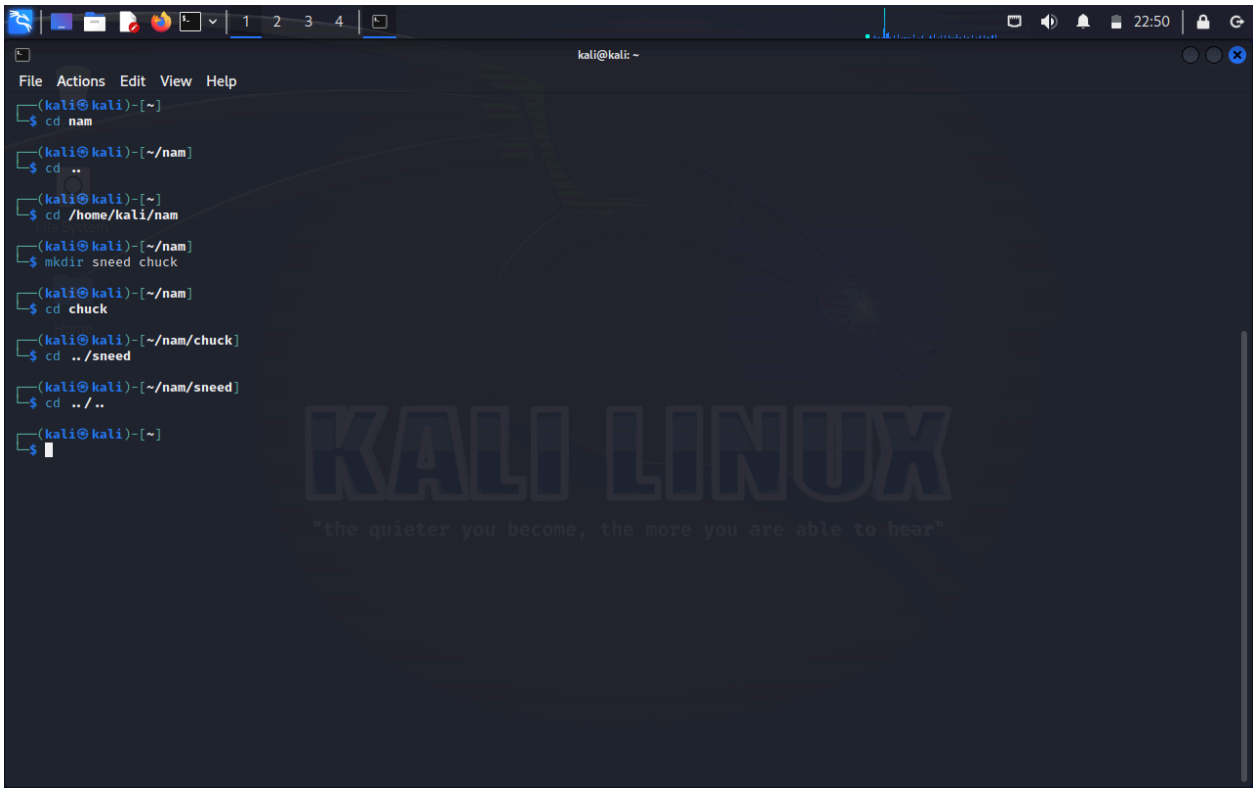
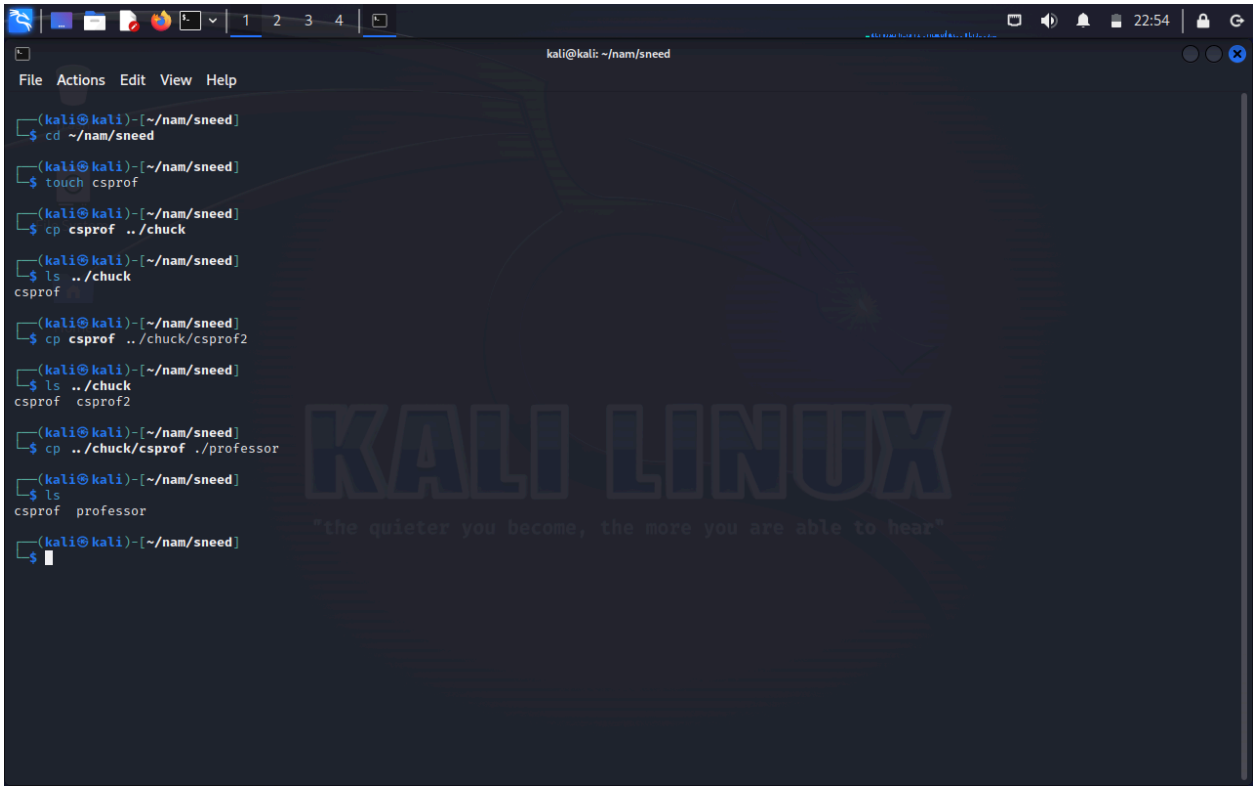
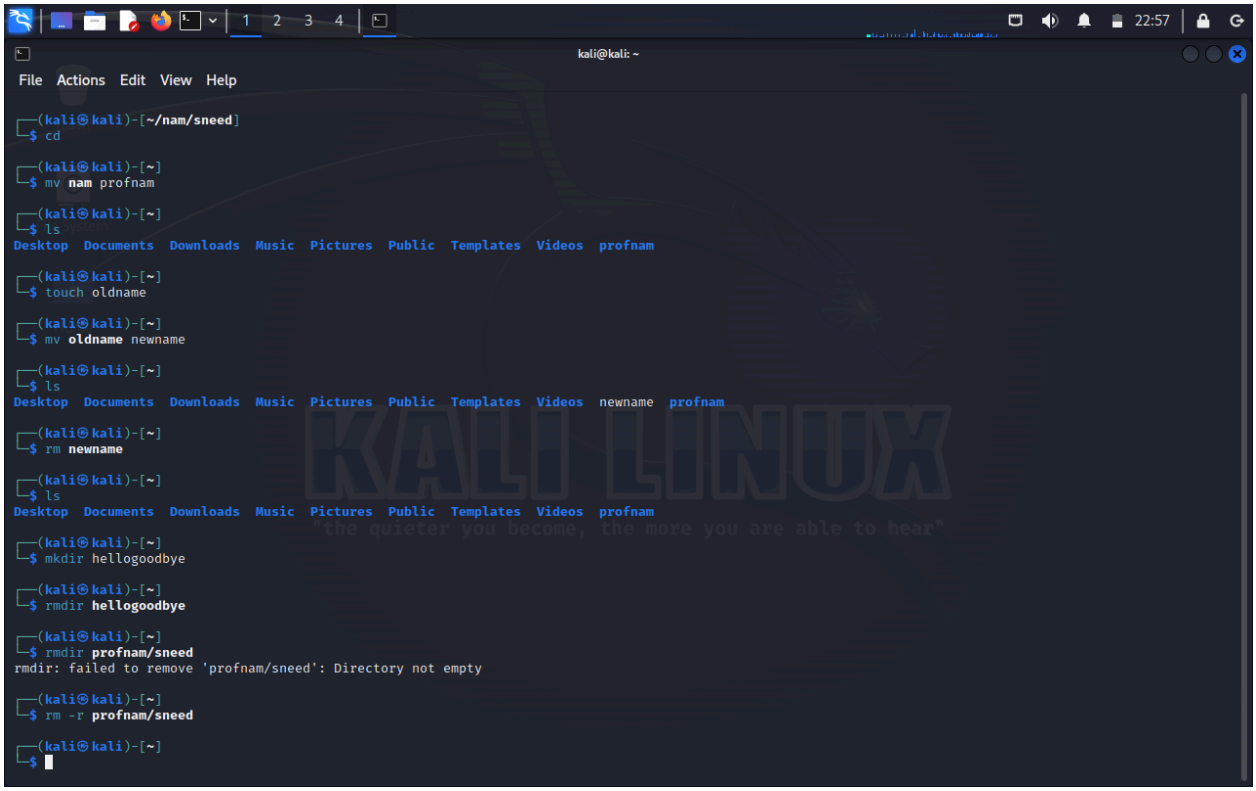
Lab 2.02
2,


1 2 3 4
22:50
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd nam
(kali㉿kali)-[~/nam]
$ cd ..
(kali㉿kali)-[~]
$ cd /home/kali/nam
(kali㉿kali)-[~/nam]
$ mkdir sneed chuck
(kali㉿kali)-[~/nam]
$ cd chuck
(kali㉿kali)-[~/nam/chuck]
$ cd ../sneed
(kali㉿kali)-[~/nam/sneed]
$ cd ../..
(kali㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

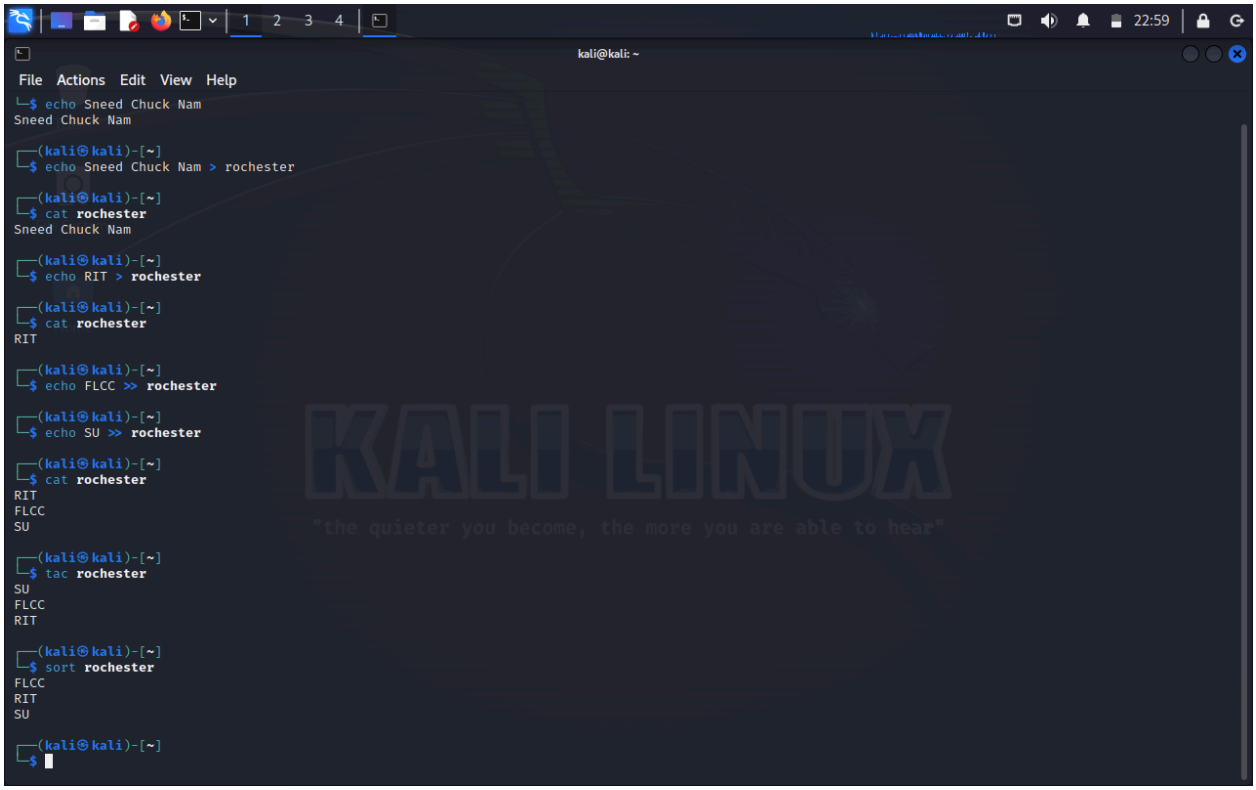
3,


22:54
kali@kali: ~/nam/sneed
File Actions Edit View Help
(kali㉿kali)-[~/nam/sneed]
$ cd ~/nam/sneed
(kali㉿kali)-[~/nam/sneed]
$ touch csprof
(kali㉿kali)-[~/nam/sneed]
$ cp csprof ../chuck
(kali㉿kali)-[~/nam/sneed]
$ ls ../chuck
csprof
(kali㉿kali)-[~/nam/sneed]
$ cp csprof ../chuck/csprof2
(kali㉿kali)-[~/nam/sneed]
$ ls ../chuck
csprof csprof2
(kali㉿kali)-[~/nam/sneed]
$ cp ../chuck/csprof ./professor
(kali㉿kali)-[~/nam/sneed]
$ ls
csprof professor
(kali㉿kali)-[~/nam/sneed]
$

4,

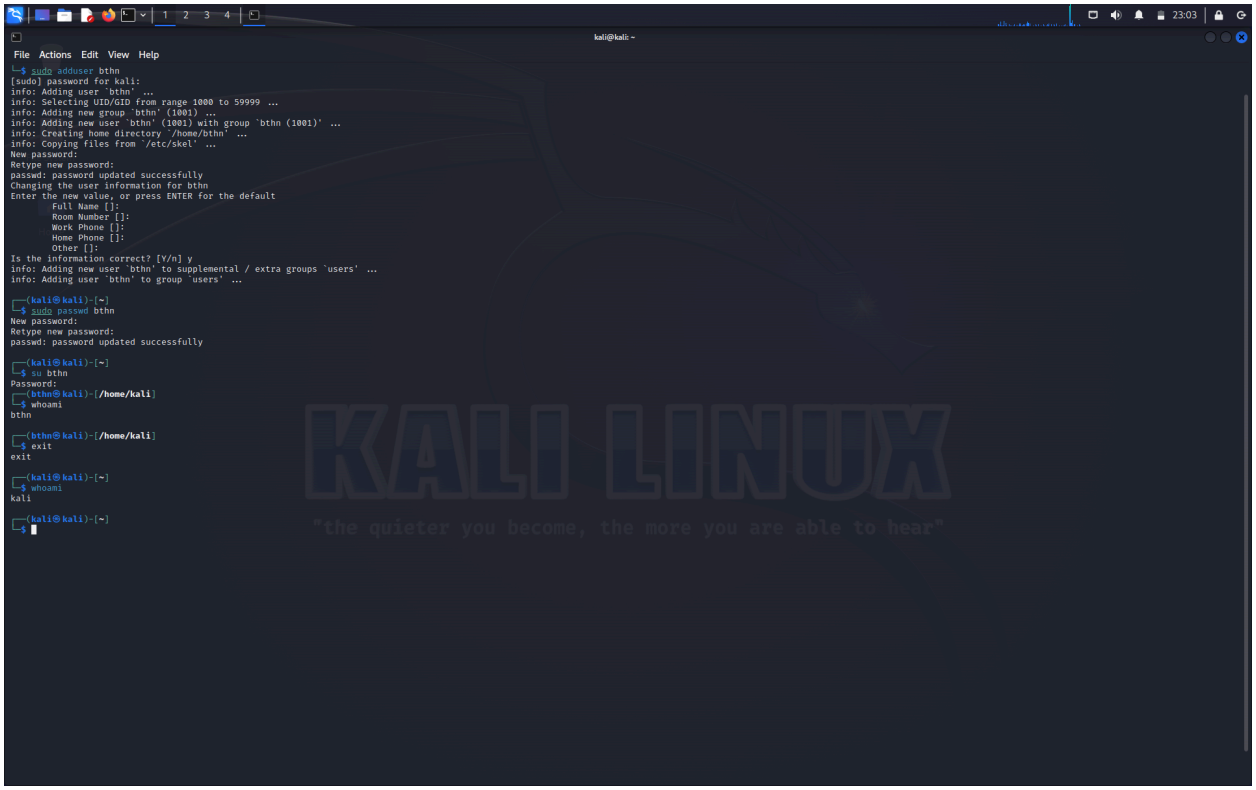

22:57
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~/nam/sneed]
$ cd
(kali㉿kali)-[~]
$ mv nam profnam
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos profnam
(kali㉿kali)-[~]
$ touch oldname
(kali㉿kali)-[~]
$ mv oldname newname
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos newname profnam
(kali㉿kali)-[~]
$ rm newname
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos profnam
(kali㉿kali)-[~]
$ mkdir hellogoodbye
(kali㉿kali)-[~]
$ rmdir hellogoodbye
(kali㉿kali)-[~]
$ rmdir profnam/sneed
rmdir: failed to remove 'profnam/sneed': Directory not empty
(kali㉿kali)-[~]
$ rm -r profnam/sneed
(kali㉿kali)-[~]
$

5,

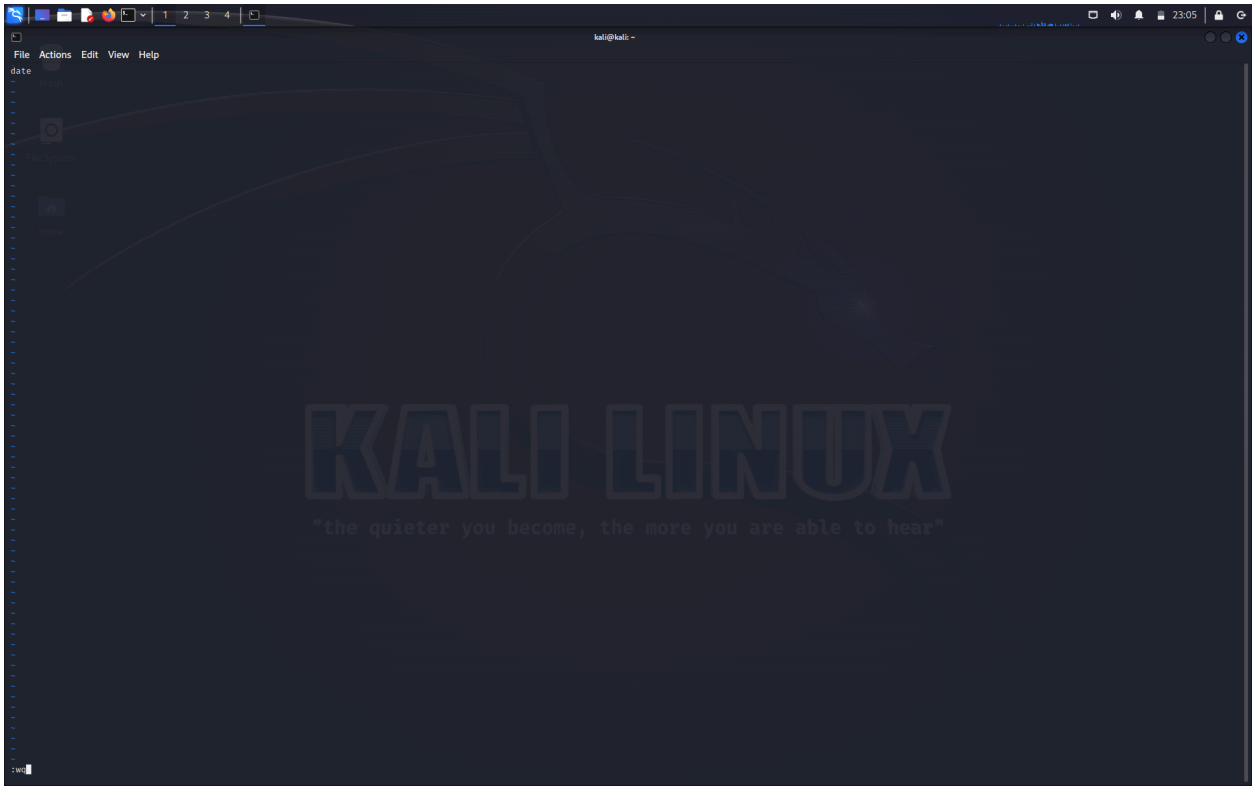

kali@kali: ~
File Actions Edit View Help
└─$ echo Sneed Chuck Nam
Sneed Chuck Nam
┌──(kali㉿kali)-[~]
└─$ echo Sneed Chuck Nam > rochester
┌──(kali㉿kali)-[~]
└─$ cat rochester
Sneed Chuck Nam
┌──(kali㉿kali)-[~]
└─$ echo RIT > rochester
┌──(kali㉿kali)-[~]
└─$ cat rochester
RIT
┌──(kali㉿kali)-[~]
└─$ echo FLCC >> rochester
┌──(kali㉿kali)-[~]
└─$ echo SU >> rochester
┌──(kali㉿kali)-[~]
└─$ cat rochester
RIT
FLCC
SU
┌──(kali㉿kali)-[~]
└─$ tac rochester
SU
FLCC
RIT
┌──(kali㉿kali)-[~]
└─$ sort rochester
FLCC
RIT
SU
┌──(kali㉿kali)-[~]
└─$
KALI LINUX
"the quieter you become, the more you are able to hear"

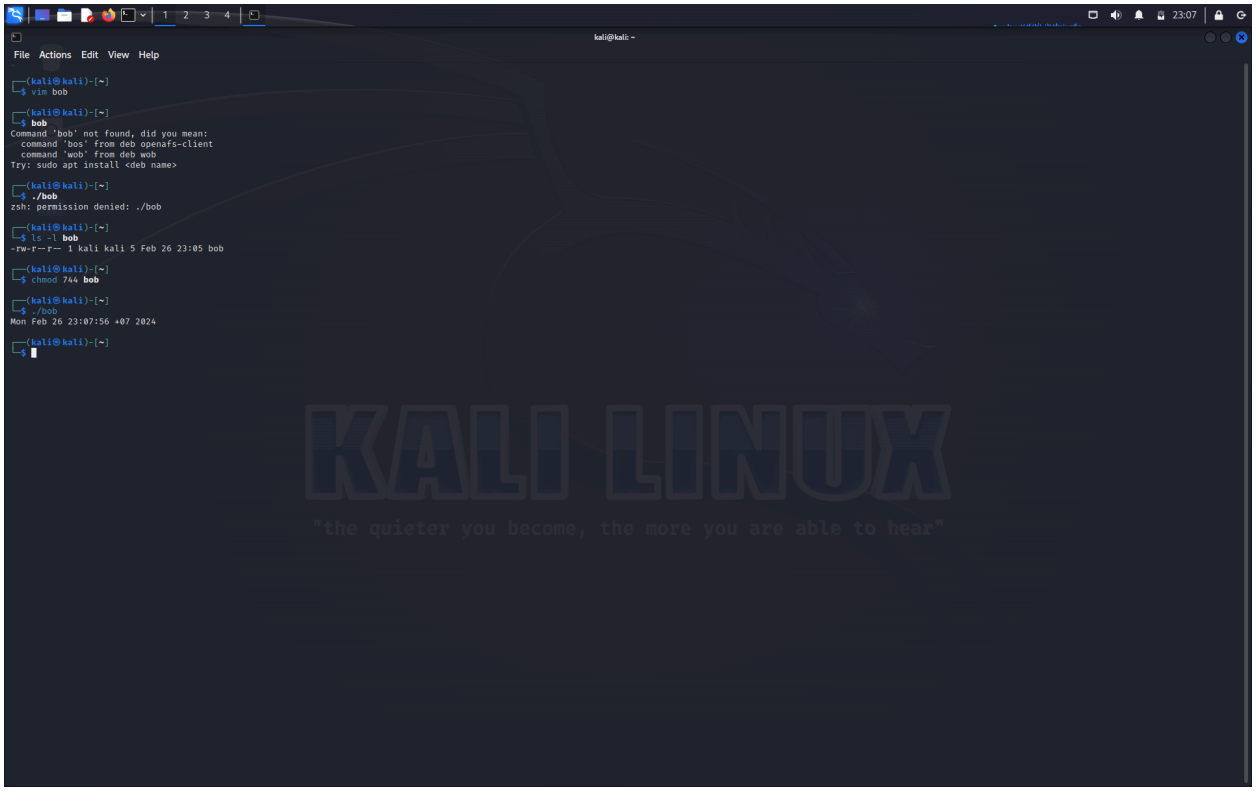
Lab 2.03

1,

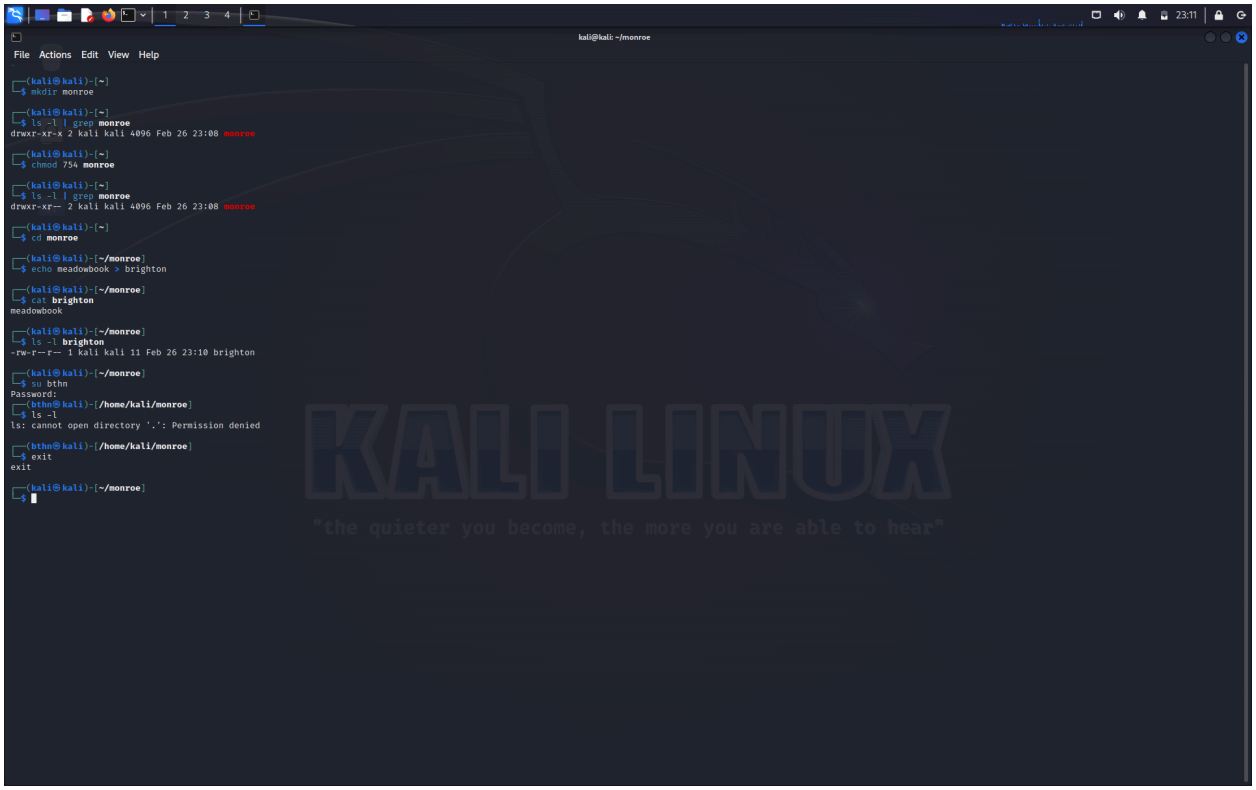


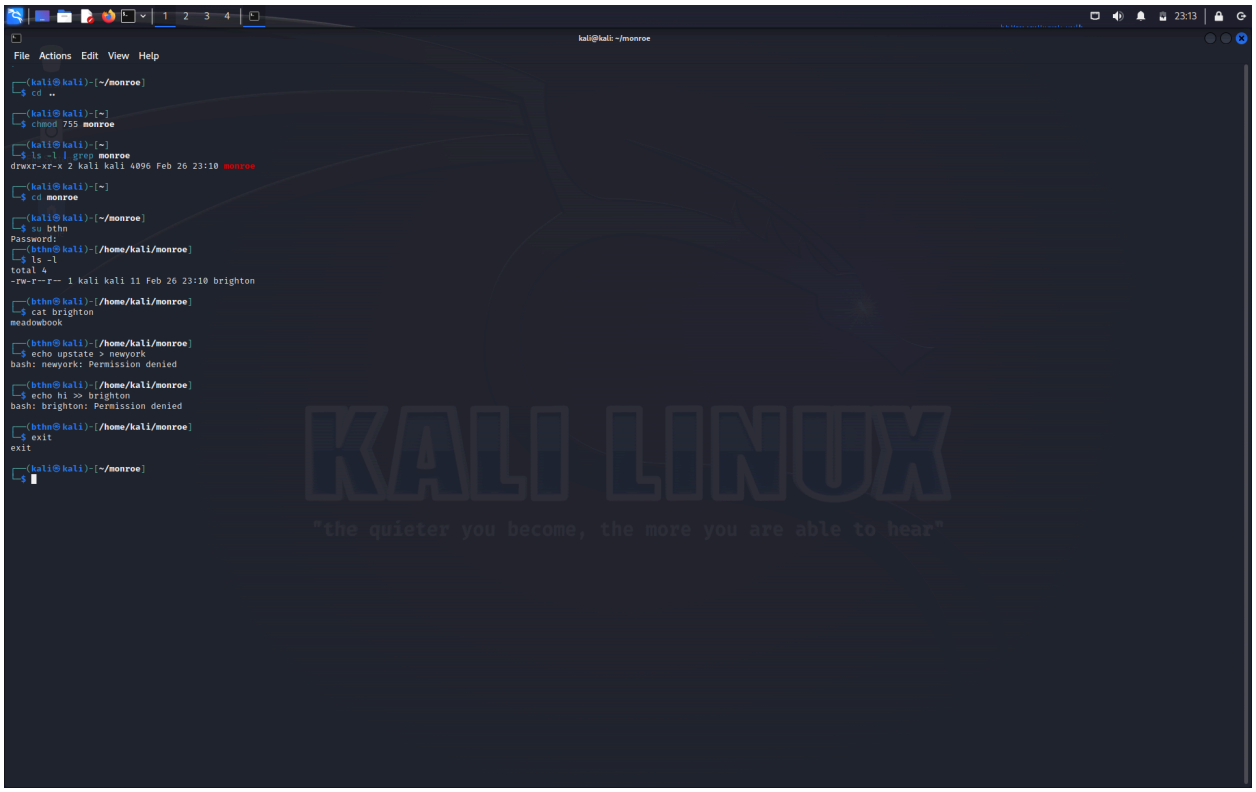
2,
Nội dung file bob


23:05
kali@kali: ~
File Actions Edit View Help
date
:wq

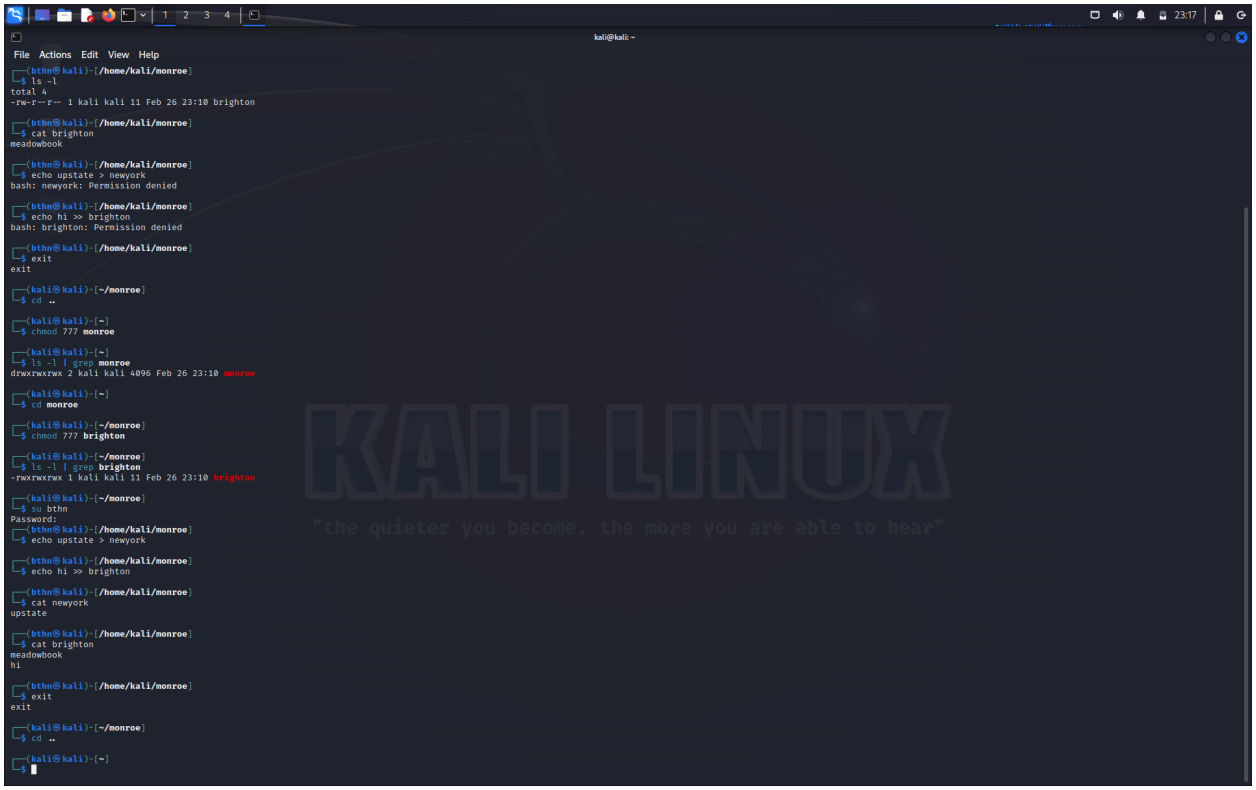

23:07
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ vim bob
(kali㉿kali)-[~]
$ bob
Command 'bob' not found, did you mean:
command 'bos' from deb openafs-client
command 'wob' from deb wob
Try: sudo apt install <deb name>
(kali㉿kali)-[~]
$ ./bob
zsh: permission denied: ./bob
(kali㉿kali)-[~]
$ ls -l bob
-rw-r--r-- 1 kali kali 5 Feb 26 23:05 bob
(kali㉿kali)-[~]
$ chmod 744 bob
(kali㉿kali)-[~]
$ ./bob
Mon Feb 26 23:07:56 +07 2024
(kali㉿kali)-[~]
$

3,


kali@kali: ~/monroe
File Actions Edit View Help
(kali㉿kali)-[~]
$ mkdir monroe
(kali㉿kali)-[~]
$ ls -l | grep monroe
drwxr-xr-x 2 kali kali 4096 Feb 26 23:08 monroe
(kali㉿kali)-[~]
$ chmod 754 monroe
(kali㉿kali)-[~]
$ ls -l | grep monroe
drwxr-xr-- 2 kali kali 4096 Feb 26 23:08 monroe
(kali㉿kali)-[~]
$ cd monroe
(kali㉿kali)-[~/monroe]
$ echo meadowbook > brighton
(kali㉿kali)-[~/monroe]
$ cat brighton
meadowbook
(kali㉿kali)-[~/monroe]
$ ls -l brighton
-rw-r--r-- 1 kali kali 11 Feb 26 23:10 brighton
(kali㉿kali)-[~/monroe]
$ su bthn
Password:
(bthn㉿kali)-[/home/kali/monroe]
$ ls -l
ls: cannot open directory '.': Permission denied
(bthn㉿kali)-[/home/kali/monroe]
$ exit
exit
(kali㉿kali)-[~/monroe]
$
"the quieter you become, the more you are able to hear"


kali@kali: ~/monroe
File Actions Edit View Help
(kali㉿kali)-[~/monroe]
$ cd ..
(kali㉿kali)-[~]
$ chmod 755 monroe
(kali㉿kali)-[~]
$ ls -l | grep monroe
drwxr-xr-x 2 kali kali 4096 Feb 26 23:10 monroe
(kali㉿kali)-[~]
$ cd monroe
(kali㉿kali)-[~/monroe]
$ su bthn
Password:
(bthn㉿kali)-[/home/kali/monroe]
$ ls -l
total 4
-rw-r--r-- 1 kali kali 11 Feb 26 23:10 brighton
(bthn㉿kali)-[/home/kali/monroe]
$ cat brighton
meadowbook
(bthn㉿kali)-[/home/kali/monroe]
$ echo upstate > newyork
bash: newyork: Permission denied
(bthn㉿kali)-[/home/kali/monroe]
$ echo hi >> brighton
bash: brighton: Permission denied
(bthn㉿kali)-[/home/kali/monroe]
$ exit
exit
(kali㉿kali)-[~/monroe]
$
"the quieter you become, the more you are able to hear"

4,


kali@kali: ~
File Actions Edit View Help
(bthn㉿kali)-[/home/kali/monroe]
$ ls -l
total 4
-rw-r--r-- 1 kali kali 11 Feb 26 23:10 brighton
(bthn㉿kali)-[/home/kali/monroe]
$ cat brighton
meadowbook
(bthn㉿kali)-[/home/kali/monroe]
$ echo upstate > newyork
bash: newyork: Permission denied
(bthn㉿kali)-[/home/kali/monroe]
$ echo hi >> brighton
bash: brighton: Permission denied
(bthn㉿kali)-[/home/kali/monroe]
$ exit
exit
(kali㉿kali)-[~/monroe]
$ cd ..
(kali㉿kali)-[~]
$ chmod 777 monroe
(kali㉿kali)-[~]
$ ls -l | grep monroe
drwxrwxrwx 2 kali kali 4096 Feb 26 23:10 monroe
(kali㉿kali)-[~]
$ cd monroe
(kali㉿kali)-[~/monroe]
$ chmod 777 brighton
(kali㉿kali)-[~/monroe]
$ ls -l | grep brighton
-rwxrwxrwx 1 kali kali 11 Feb 26 23:10 brighton
(kali㉿kali)-[~/monroe]
$ su bthn
Password:
(bthn㉿kali)-[/home/kali/monroe]
$ echo upstate > newyork
(bthn㉿kali)-[/home/kali/monroe]
$ echo hi >> brighton
(bthn㉿kali)-[/home/kali/monroe]
$ cat newyork
upstate
(bthn㉿kali)-[/home/kali/monroe]
$ cat brighton
meadowbook
hi
(bthn㉿kali)-[/home/kali/monroe]
$ exit
exit
(kali㉿kali)-[~/monroe]
$ cd ..
(kali㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

6,


kali@kali: ~
File Actions Edit View Help
$ ls -l pizza
-rwxr--r-- 1 kali kali 5 Feb 27 00:00 pizza
(kali㉿kali)-[~]
$ sudo chown bthn pizza
[sudo] password for kali:
(kali㉿kali)-[~]
$ ls -l pizza
-rwxr--r-- 1 bthn kali 5 Feb 27 00:00 pizza
(kali㉿kali)-[~]
$ sudo chgrp bthn pizza
(kali㉿kali)-[~]
$ ls -l pizza
-rwxr--r-- 1 bthn bthn 5 Feb 27 00:00 pizza
(kali㉿kali)-[~]
$ su bthn
Password:
(bthn㉿kali)-[/home/kali]
$ ./pizza
bash: ./pizza: Permission denied
(bthn㉿kali)-[/home/kali]
$ exit
exit
(kali㉿kali)-[~]
$ sudo chown kali:kali pizza
(kali㉿kali)-[~]
$ su bthn
Password:
(bthn㉿kali)-[/home/kali]
$ ./pizza
bash: ./pizza: Permission denied
(bthn㉿kali)-[/home/kali]
$ exit
exit
(kali㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

7,


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo addgroup pentesters1
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `pentesters1' (GID 1002) ...
(kali㉿kali)-[~]
$ sudo addgroup pentesters2
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `pentesters2' (GID 1003) ...
(kali㉿kali)-[~]
$ sudo usermod -a -G pentesters1,pentesters2 bthn
(kali㉿kali)-[~]
$ grep pentesters /etc/group
pentesters1:x:1002:bthn
pentesters2:x:1003:bthn
(kali㉿kali)-[~]
$ groups bthn
bthn : bthn users pentesters1 pentesters2
(kali㉿kali)-[~]
$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kali
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:kali
fax:x:21:
voice:x:22:
cdrom:x:24:kali
floppy:x:25:kali
tape:x:26:
sudo:x:27:kali
audio:x:29:pulse,kali
dip:x:30:kali
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo usermod -G pentesters1 bthn
(kali㉿kali)-[~]
$ groups bthn
bthn : bthn pentesters1
(kali㉿kali)-[~]
$ sudo usermod -a -G pentesters1,pentesters2 bthn
(kali㉿kali)-[~]
$ groups bthn
bthn : bthn pentesters1 pentesters2
(kali㉿kali)-[~]
$ sudo gpasswd -d bthn pentesters2
Removing user bthn from group pentesters2
(kali㉿kali)-[~]
$ groups bthn
bthn : bthn pentesters1
(kali㉿kali)-[~]
$ sudo adduser alice
info: Adding user `alice' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `alice' (1004) ...
info: Adding new user `alice' (1004) with group `alice (1004)' ...
info: Creating home directory `/home/alice' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n]
info: Adding new user `alice' to supplemental / extra groups `users' ...
info: Adding user `alice' to group `users' ...
(kali㉿kali)-[~]
$ sudo deluser alice
info: Removing crontab ...
info: Removing user `alice' ...
(kali㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo addgroup cryptographers
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `cryptographers' (GID 1004) ...
(kali㉿kali)-[~]
$ sudo delgroup cryptographers
info: Removing group `cryptographers' ...
(kali㉿kali)-[~]
$
Log Out...

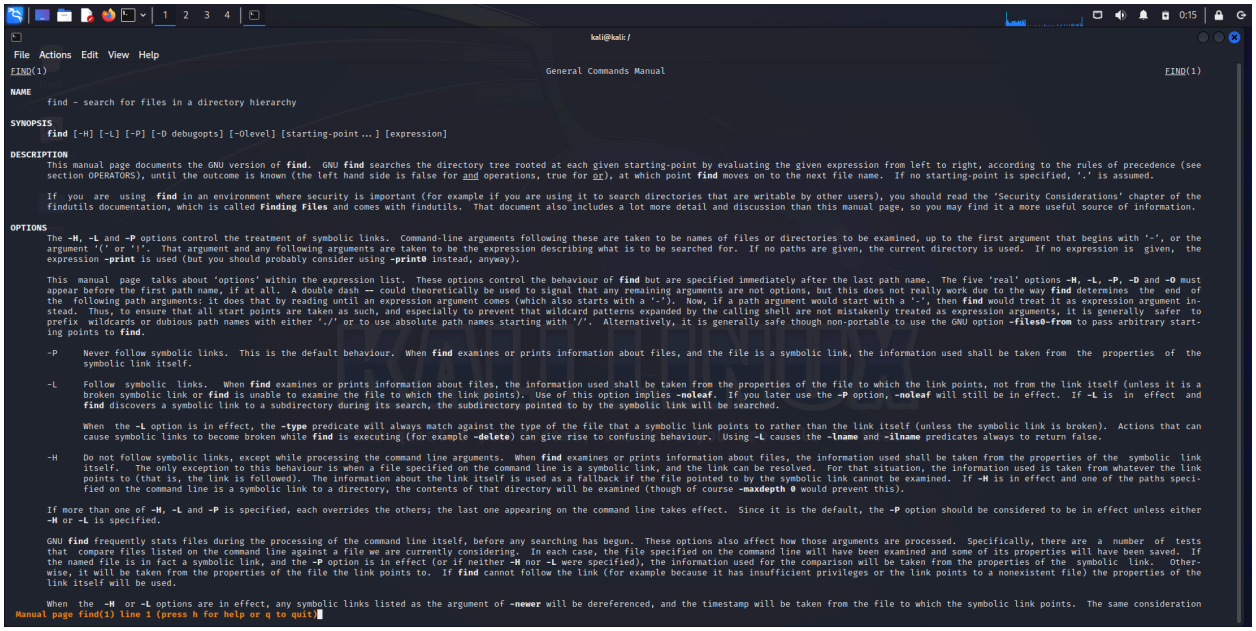
8,


kali@kali: /
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /
(kali㉿kali)-[/]
$ ls -a
. .. .cache bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
(kali㉿kali)-[/]
$ ls -A
.cache bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
(kali㉿kali)-[/]
$ ls -F
bin@ boot/ dev/ etc/ home/ initrd.img@ initrd.img.old@ lib@ lib32@ lib64@ libx32@ lost+found/ media/ mnt/ opt/ proc/ root/ run/ sbin@ srv/ sys/ tmp/ usr/ var/ vmlinuz@ vmlinuz.old@
(kali㉿kali)-[/]
$ ls -R
.:
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
./boot:
System.map-6.3.0-kali1-amd64 config-6.3.0-kali1-amd64 grub initrd.img-6.3.0-kali1-amd64 vmlinuz-6.3.0-kali1-amd64
./boot/grub:
fonts grub.cfg grubenv i386-pc locale themes unicode.pf2
./boot/grub/fonts:
unicode.pf2
./boot/grub/i386-pc:
915resolution.mod cbmemc.mod div_test.mod gcry_des.mod hashsum.mod lsmmap.mod mul_test.mod parttool.mod romfs.mod testload.mod video.mod
acpi.mod cbtable.mod dm_nv.mod gcry_dsa.mod hdparm.mod lspci.mod multiboot.mod password.mod scsi.mod testspeed.mod video_bochs.mod
adler32.mod cbtime.mod drivemap.mod gcry_idea.mod hello.mod luks.mod multiboot2.mod password_pbkdf2.mod search.mod tftp.mod video_cirrus.mod
affs.mod chain.mod echo.mod gcry_md4.mod help.mod luks2.mod nativedisk.mod pata.mod search_fs_file.mod tga.mod video_colors.mod
afs.mod cmdline_cat_test.mod efiemu.mod gcry_md5.mod hexdump.mod lvm.mod net.mod pbkdf2.mod search_fs_uuid.mod time.mod video_fb.mod
afsplitter.mod cmosdump.mod efiemu32.o gcry_rfc2268.mod hfs.mod lzopio.mod newc.mod pbkdf2_test.mod search_label.mod tr.mod videoinfo.mod
ahci.mod cmostest.mod efiemu64.o gcry_rijndael.mod hfsplus.mod macbless.mod nilfs2.mod pci.mod sendkey.mod trig.mod videotest.mod
all_video.mod cmp.mod ehci.mod gcry_rmd160.mod hfspluscomp.mod macho.mod normal.mod pcidump.mod serial.mod true.mod videotest_checksum.mod
aout.mod cmp_test.mod elf.mod gcry_rsa.mod http.mod mda_text.mod ntfs.mod pgp.mod setjmp.mod truecrypt.mod wrmsr.mod
archelp.mod command.lst eval.mod gcry_seed.mod hwmatch.mod mdraid09.mod ntfscomp.mod plan9.mod setjmp_test.mod udf.mod xfs.mod
at_keyboard.mod configfile.mod exfat.mod gcry_serpent.mod iorw.mod mdraid09_be.mod nltdr.mod play.mod setpci.mod ufs1.mod xnu.mod
ata.mod core.img exfctest.mod gcry_sha1.mod iso9660.mod mdraid1x.mod odc.mod png.mod sfs.mod ufs1_be.mod xnu_uuid.mod
backtrace.mod cpio.mod ext2.mod gcry_sha256.mod jfs.mod memdisk.mod offsetio.mod priority_queue.mod shift_test.mod ufs2.mod xnu_uuid_test.mod
bfs.mod cpio_be.mod extcmd.mod gcry_sha512.mod jpeg.mod memrw.mod ohci.mod probe.mod signature_test.mod uhci.mod xzio.mod
biosdisk.mod cpuid.mod f2fs.mod gcry_tiger.mod json.mod minicmd.mod part_acorn.mod procfs.mod sleep.mod usb.mod zfs.mod
bitmap.mod crc64.mod fat.mod gcry_twofish.mod keylayouts.mod minix.mod part_amiga.mod progress.mod sleep_test.mod usb_keyboard.mod zfscrypt.mod
bitmap_scale.mod crypto.lst file.mod gcry_whirlpool.mod keystatus.mod minix2.mod part_apple.mod pxe.mod smbios.mod usbms.mod zfsinfo.mod
blocklist.mod crypto.mod font.mod gdb.mod ldm.mod minix2_be.mod part_bsd.mod pxechain.mod spkmodem.mod usbserial_common.mod zstd.mod
boot.img cryptodisk.mod freedos.mod geli.mod legacy_password_test.mod minix3.mod part_dfly.mod raid5rec.mod squash4.mod usbserial_ftdi.mod
boot.mod cs5536.mod fs.lst gettext.mod legacycfg.mod minix3_be.mod part_dvh.mod raid6rec.mod strtoull_test.mod usbserial_pl2303.mod
bsd.mod ctz_test.mod fshelp.mod gfxmenu.mod linux.mod minix_be.mod part_gpt.mod random.mod syslinuxcfg.mod usbserial_usbdebug.mod
bswap_test.mod date.mod functional_test.mod gfxterm.mod linux16.mod mmap.mod part_msdos.mod rdmsr.mod tar.mod usbtest.mod


kali@kali: /
File Actions Edit View Help
┌──(kali㉿kali)-[/]
└─$ ls -R | more
ls: cannot open directory './etc/credstore': Permission denied
ls: cannot open directory './etc/credstore.encrypted': Permission denied
ls: cannot open directory './etc/ipsec.d/private': Permission denied
ls: cannot open directory './etc/openvas/gnupg': Permission denied
ls: cannot open directory './etc/polkit-1/rules.d': Permission denied
ls: cannot open directory './etc/redis': Permission denied
.:
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
./boot:
System.map-6.3.0-kali1-amd64
config-6.3.0-kali1-amd64
grub
initrd.img-6.3.0-kali1-amd64
vmlinuz-6.3.0-kali1-amd64
./boot/grub:
fonts
grub.cfg
grubenv
i386-pc
locale
themes
unicode.pf2
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: /
File Actions Edit View Help
bitmap_scale.mod
blocklist.mod
boot.img
boot.mod
bsd.mod
bswap_test.mod
btrfs.mod
bufio.mod
cat.mod
cbfs.mod
cbls.mod
cbmemc.mod
cbtable.mod
cbtime.mod
chain.mod
cmdline_cat_test.mod
cmosdump.mod
cmostest.mod
cmp.mod
cmp_test.mod
command.lst
configfile.mod
core.img
cpio.mod
cpio_be.mod
cpuid.mod
crc64.mod
crypto.lst
crypto.mod
cryptodisk.mod
cs5536.mod
ctz_test.mod
date.mod
datehook.mod
datetime.mod
disk.mod
diskfilter.mod
div.mod
div_test.mod
dm_nv.mod
┌──(kali㉿kali)-[/]
└─$ ls -R | less
ls: cannot open directory './etc/credstore': Permission denied
ls: cannot open directory './etc/credstore.encrypted': Permission denied
ls: cannot open directory './etc/ipsec.d/private': Permission denied
ls: cannot open directory './etc/openvas/gnupg': Permission denied
ls: cannot open directory './etc/polkit-1/rules.d': Permission denied
ls: cannot open directory './etc/redis': Permission denied
┌──(kali㉿kali)-[/]
└─$ clear
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: /
File Actions Edit View Help
(kali㉿kali)-[/]
$ find / -name ping 2>&1 | grep -v "Permission denied"
/usr/share/bash-completion/completions/ping
/usr/bin/ping
/usr/lib/python3/dist-packages/faraday_plugins/plugins/repo/ping
(kali㉿kali)-[/]
$
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: /
File Actions Edit View Help
FIND(1) General Commands Manual FIND(1)
NAME
find - search for files in a directory hierarchy
SYNOPSIS
find [-H] [-L] [-P] [-D debugopts] [-Olevel] [starting-point ...] [expression]
DESCRIPTION
This manual page documents the GNU version of find. GNU find searches the directory tree rooted at each given starting-point by evaluating the given expression from left to right, according to the rules of precedence (see section OPERATORS), until the outcome is known (the left hand side is false for and operations, true for or), at which point find moves on to the next file name. If no starting-point is specified, '.' is assumed.
If you are using find in an environment where security is important (for example if you are using it to search directories that are writable by other users), you should read the 'Security Considerations' chapter of the findutils documentation, which is called Finding Files and comes with findutils. That document also includes a lot more detail and discussion than this manual page, so you may find it a more useful source of information.
OPTIONS
The -H, -L and -P options control the treatment of symbolic links. Command-line arguments following these are taken to be names of files or directories to be examined, up to the first argument that begins with '-', or the argument '(' or '!'. That argument and any following arguments are taken to be the expression describing what is to be searched for. If no paths are given, the current directory is used. If no expression is given, the expression -print is used (but you should probably consider using -print0 instead, anyway).
This manual page talks about 'options' within the expression list. These options control the behaviour of find but are specified immediately after the last path name. The five 'real' options -H, -L, -P, -D and -O must appear before the first path name, if at all. A double dash -- could theoretically be used to signal that any remaining arguments are not options, but this does not really work due to the way find determines the end of the following path arguments: it does that by reading until an expression argument comes (which also starts with a '-'). Now, if a path argument would start with a '-', then find would treat it as expression argument instead. Thus, to ensure that all start points are taken as such, and especially to prevent that wildcard patterns expanded by the calling shell are not mistakenly treated as expression arguments, it is generally safer to prefix wildcards or dubious path names with either './' or to use absolute path names starting with '/'. Alternatively, it is generally safe though non-portable to use the GNU option -files0-from to pass arbitrary starting points to find.
-P Never follow symbolic links. This is the default behaviour. When find examines or prints information about files, and the file is a symbolic link, the information used shall be taken from the properties of the symbolic link itself.
-L Follow symbolic links. When find examines or prints information about files, the information used shall be taken from the properties of the file to which the link points, not from the link itself (unless it is a broken symbolic link or find is unable to examine the file to which the link points). Use of this option implies -noleaf. If you later use the -P option, -noleaf will still be in effect. If -L is in effect and find discovers a symbolic link to a subdirectory during its search, the subdirectory pointed to by the symbolic link will be searched.
When the -L option is in effect, the -type predicate will always match against the type of the file that a symbolic link points to rather than the link itself (unless the symbolic link is broken). Actions that can cause symbolic links to become broken while find is executing (for example -delete) can give rise to confusing behaviour. Using -L causes the -lname and -ilname predicates always to return false.
-H Do not follow symbolic links, except while processing the command line arguments. When find examines or prints information about files, the information used shall be taken from the properties of the symbolic link itself. The only exception to this behaviour is when a file specified on the command line is a symbolic link, and the link can be resolved. For that situation, the information used is taken from whatever the link points to (that is, the link is followed). The information about the link itself is used as a fallback if the file pointed to by the symbolic link cannot be examined. If -H is in effect and one of the paths specified on the command line is a symbolic link to a directory, the contents of that directory will be examined (though of course -maxdepth 0 would prevent this).
If more than one of -H, -L and -P is specified, each overrides the others; the last one appearing on the command line takes effect. Since it is the default, the -P option should be considered to be in effect unless either -H or -L is specified.
GNU find frequently stats files during the processing of the command line itself, before any searching has begun. These options also affect how those arguments are processed. Specifically, there are a number of tests that compare files listed on the command line against a file we are currently considering. In each case, the file specified on the command line will have been examined and some of its properties will have been saved. If the named file is in fact a symbolic link, and the -P option is in effect (or if neither -H nor -L were specified), the information used for the comparison will be taken from the properties of the symbolic link. Otherwise, it will be taken from the properties of the file the link points to. If find cannot follow the link (for example because it has insufficient privileges or the link points to a nonexistent file) the properties of the link itself will be used.
When the -H or -L options are in effect, any symbolic links listed as the argument of -newer will be dereferenced, and the timestamp will be taken from the file to which the symbolic link points. The same consideration
Manual page find(1) line 1 (press h for help or q to quit)


kali@kali: /
File Actions Edit View Help
Jan
Feb
March
April
May
June
July
August
Sept
Oct
Nov
Dec
:wq


kali@kali: /
File Actions Edit View Help
┌──(kali㉿kali)-[/]
└─$ find / -name ping 2>&1 | grep -v "Permission denied"
/usr/share/bash-completion/completions/ping
/usr/bin/ping
/usr/lib/python3/dist-packages/faraday_plugins/plugins/repo/ping
┌──(kali㉿kali)-[/]
└─$ man find
┌──(kali㉿kali)-[/]
└─$ vim months
┌──(kali㉿kali)-[/]
└─$ vim months
┌──(kali㉿kali)-[/]
└─$ head months
Jan
Feb
March
April
May
June
July
August
Sept
Oct
┌──(kali㉿kali)-[/]
└─$ head -7 months
Jan
Feb
March
April
May
June
July
┌──(kali㉿kali)-[/]
└─$ head -n -3 months
Jan
Feb
March
April
May
June
July
August
Sept
┌──(kali㉿kali)-[/]
└─$

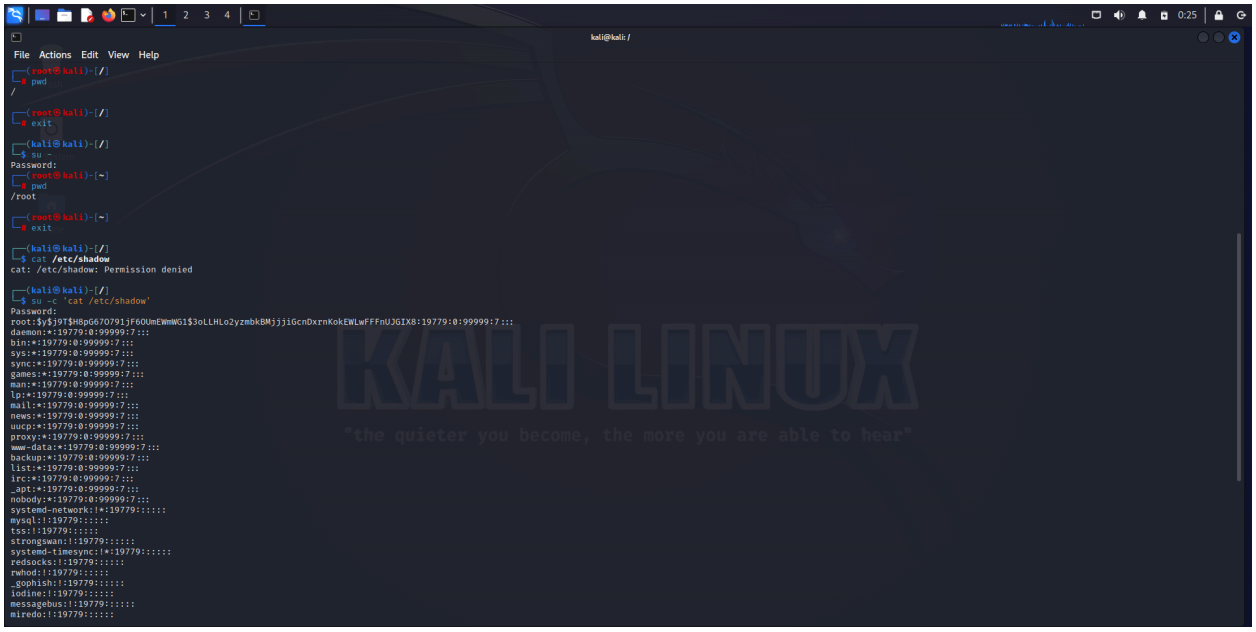

kali@kali: /
File Actions Edit View Help
Feb
March
April
May
June
July
(kali㉿kali)-[/]
$ head -n -3 months
Jan
Feb
March
April
May
June
July
August
Sept
(kali㉿kali)-[/]
$ tail months
March
April
May
June
July
August
Sept
Oct
Nov
Dec
(kali㉿kali)-[/]
$ tail -3 months
Oct
Nov
Dec
(kali㉿kali)-[/]
$ tail +3 months
March
April
May
June
July
August
Sept
Oct
Nov
Dec
(kali㉿kali)-[/]
$

Lab 2.04:

1,


root@kali: ~
File Actions Edit View Help
(kali㉿kali)-[/]
$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
(kali㉿kali)-[/]
$ sudo passwd -l root
passwd: password changed.
(kali㉿kali)-[/]
$ sudo passwd -u root
passwd: password changed.
(kali㉿kali)-[/]
$ su
Password:
(root㉿kali)-[/]
pws
Command 'pws' not found, did you mean:
command 'pwm' from deb python3-passwordmeter
command 'pts' from deb openafs-client
command 'pps' from deb libpmix-bin
command 'pvs' from deb lvm2
command 'pwsh' from deb powershell
command 'pwsh' from deb powershell-lts
command 'ps' from deb procps
command 'aws' from deb awscli
command 'rpws' from deb ratpoison
command 'psw' from deb wise
command 'pms' from deb pms
command 'pcs' from deb pcs
command 'pwd' from deb coreutils
Try: apt install <deb name>
(root㉿kali)-[/]
pwd
/
(root㉿kali)-[/]
exit
(kali㉿kali)-[/]
$ su -
Password:
(root㉿kali)-[~]
#

2,


kali@kali: /
File Actions Edit View Help
(root㉿kali)-[/]
pwd
/
(root㉿kali)-[/]
exit
(kali㉿kali)-[/]
$ su -
Password:
(root㉿kali)-[~]
pwd
/root
(root㉿kali)-[~]
exit
(kali㉿kali)-[/]
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
(kali㉿kali)-[/]
$ su -c 'cat /etc/shadow'
Password:
root:yj9T$H8pG67O791jF6OUmEWmWG1$3oLLHLo2yzmbkBMjjjiGcnDxrnKokEWLwFFFnUJGIX8:19779:0:99999:7:::
daemon:*:19779:0:99999:7:::
bin:*:19779:0:99999:7:::
sys:*:19779:0:99999:7:::
sync:*:19779:0:99999:7:::
games:*:19779:0:99999:7:::
man:*:19779:0:99999:7:::
lp:*:19779:0:99999:7:::
mail:*:19779:0:99999:7:::
news:*:19779:0:99999:7:::
uucp:*:19779:0:99999:7:::
proxy:*:19779:0:99999:7:::
www-data:*:19779:0:99999:7:::
backup:*:19779:0:99999:7:::
list:*:19779:0:99999:7:::
irc:*:19779:0:99999:7:::
_apt:*:19779:0:99999:7:::
nobody:*:19779:0:99999:7:::
systemd-network:!*:19779::::::
mysql:!!:19779::::::
tss:!!:19779::::::
strongswan:!!:19779::::::
systemd-timesync:!*:19779::::::
redsocks:!!:19779::::::
rwhod:!!:19779::::::
_gophish:!!:19779::::::
iodine:!!:19779::::::
messagebus:!!:19779::::::
miredo:!!:19779::::::
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: /
File Actions Edit View Help
(kali㉿kali)-[/]
$ sudo passwd -l root
passwd: password changed.
(kali㉿kali)-[/]
$ su -c 'cat /etc/shadow'
Password:
su: Authentication failure
(kali㉿kali)-[/]
$ sudo su
(root㉿kali)-[/]
exit
(kali㉿kali)-[/]
$
KALI LINUX
"the quieter you become, the more you are able to hear"

3,


Firefox ESR
Browse the World Wide Web
kali@kali: /
/etc/sudoers.d/alice.tmp *
alice ALL=(ALL:ALL) /usr/bin/passwd, /usr/bin/cat
/etc/shadow
KALI LINUX
"the quieter you become, the more you are able to hear"


kali@kali: /
File Actions Edit View Help
(kali㉿kali)-[/]
$ sudo visudo -f /etc/sudoers.d/alice
/etc/sudoers.d/alice:2:13: syntax error
/etc/shadow
^
What now?
Options are:
(e)dit sudoers file again
e(x)it without saving changes to sudoers file
(Q)uit and save changes to sudoers file (DANGER!)
What now?
KALI LINUX
"the quieter you become, the more you are able to hear"