LINUX FUNDAMENTALS – FINAL PROJECT

Abstract

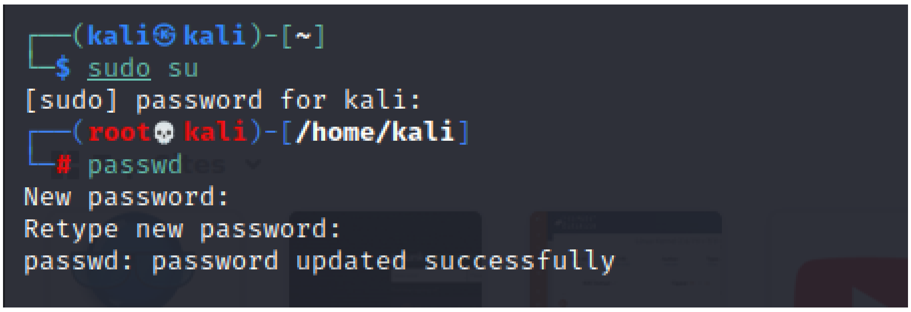
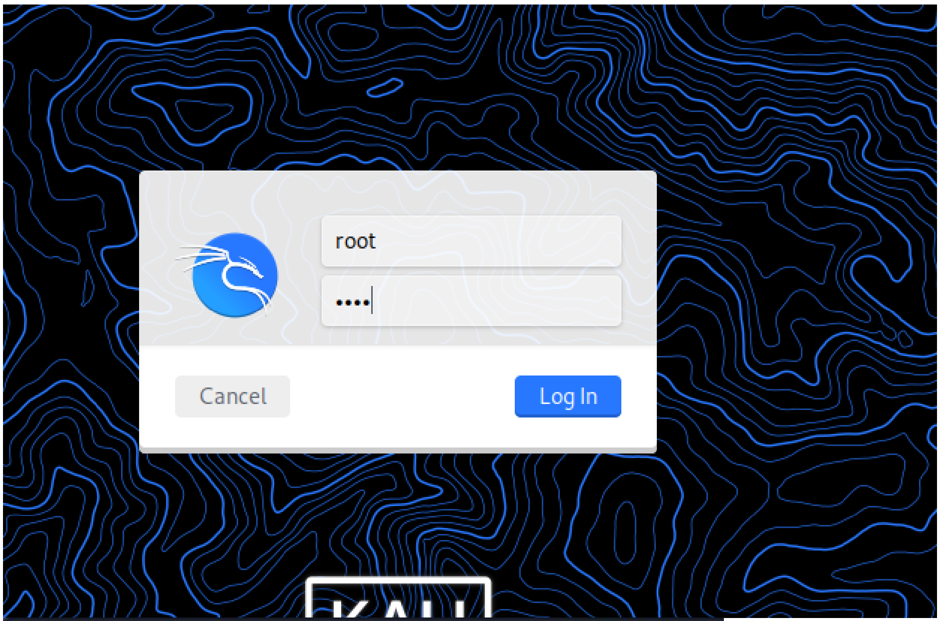
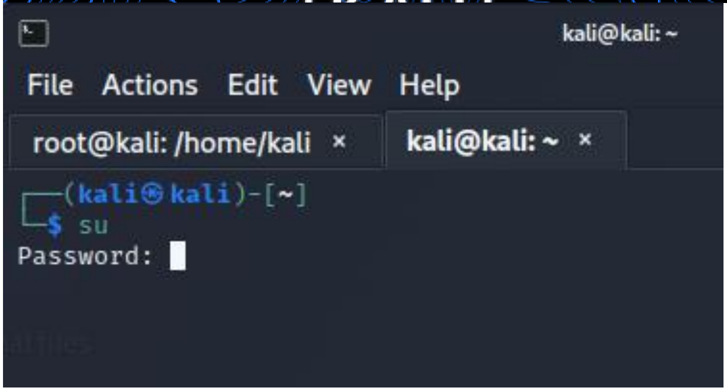
This Document illustrates the student knowledge on basic linux commands and configuration of essential services in Linux

DEKSHINAMURTHY MEENAKSHI

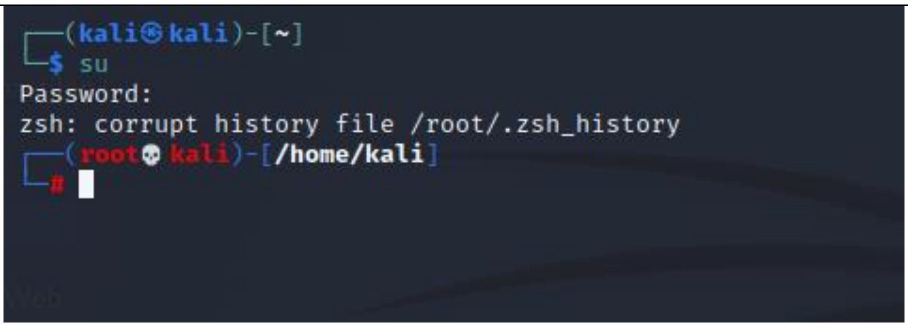
Sstudy2016@gmail.com

Table of Contents

Part 1: Basic Commands

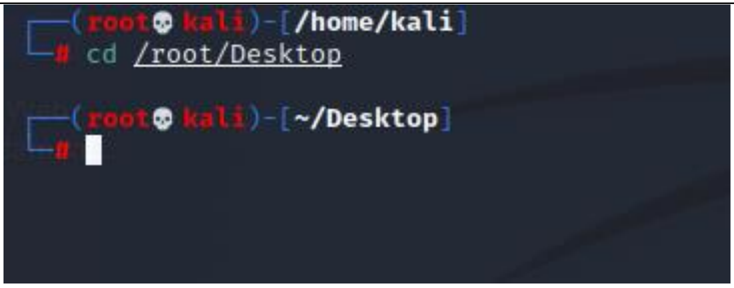
Log in to su User	 ┌──(kali㉿kali)-[~] └─$ sudo su [sudo] password for kali: ┌──(root💀kali)-[/home/kali] └─# passwd New password: Retype new password: passwd: password updated successfully   kali@kali: ~ File Actions Edit View Help root@kali: /home/kali × kali@kali: ~ × ┌──(kali㉿kali)-[~] └─$ su Password: There are two ways to access the root privileges. Here logged in as kali and SU

<table>
<tr>
<td></td>
<td>



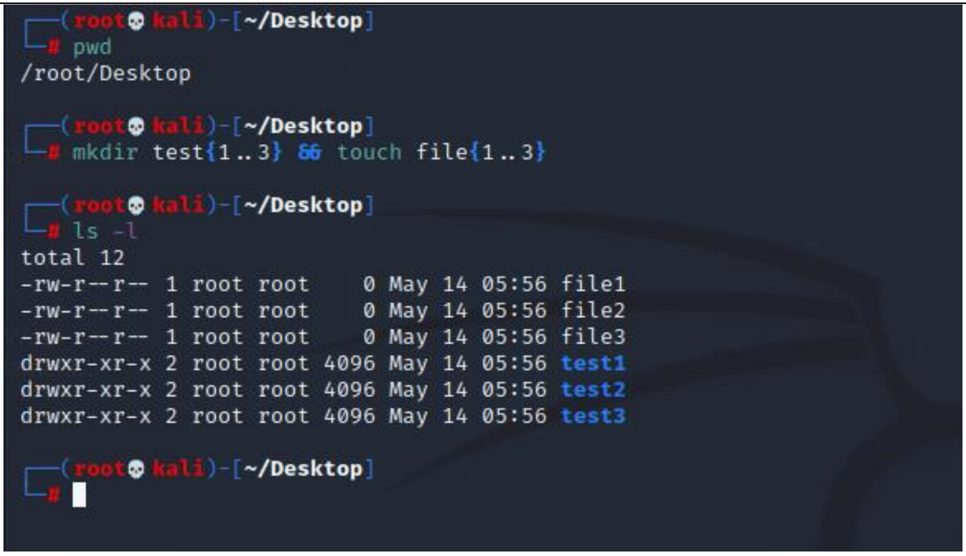
```
┌──(kali㉿kali)-[~]
└─$ su
Password:
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali)-[/home/kali]
└─# 
```

</td>
</tr>
<tr>
<td>Home/Desktop Folder</td>
<td>



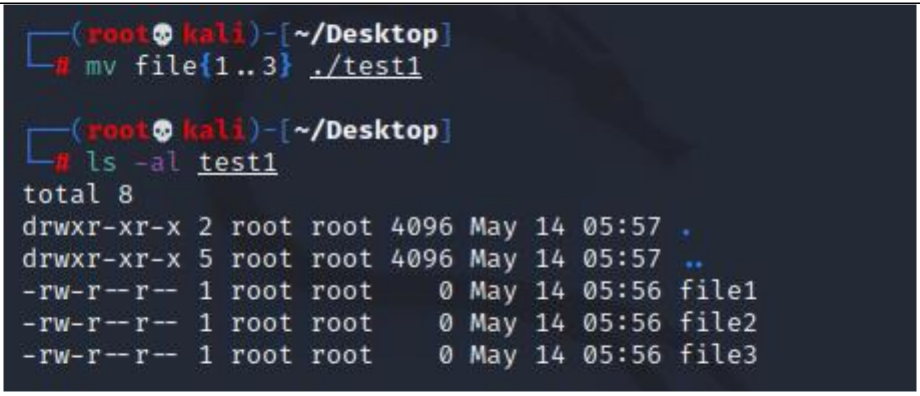
```
┌──(root💀kali)-[/home/kali]
└─# cd /root/Desktop

┌──(root💀kali)-[~/Desktop]
└─# 
```

</td>
</tr>
<tr>
<td>Create three new directories and three new files in single command</td>
<td>



```
┌──(root💀kali)-[~/Desktop]
└─# pwd
/root/Desktop

┌──(root💀kali)-[~/Desktop]
└─# mkdir test{1..3} && touch file{1..3}

┌──(root💀kali)-[~/Desktop]
└─# ls -l
total 12
-rw-r--r-- 1 root root    0 May 14 05:56 file1
-rw-r--r-- 1 root root    0 May 14 05:56 file2
-rw-r--r-- 1 root root    0 May 14 05:56 file3
drwxr-xr-x 2 root root 4096 May 14 05:56 test1
drwxr-xr-x 2 root root 4096 May 14 05:56 test2
drwxr-xr-x 2 root root 4096 May 14 05:56 test3

┌──(root💀kali)-[~/Desktop]
└─# 
```

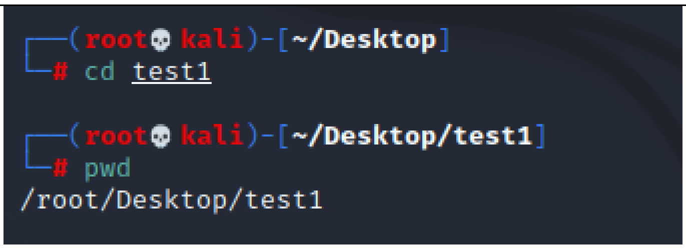
</td>
</tr>
<tr>
<td>Move the files to one of the directories (test1)</td>
<td>



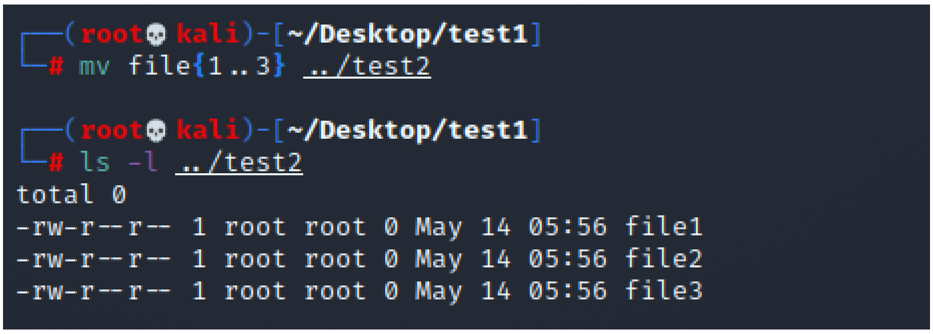
```
┌──(root💀kali)-[~/Desktop]
└─# mv file{1..3} ./test1

┌──(root💀kali)-[~/Desktop]
└─# ls -al test1
total 8
drwxr-xr-x 2 root root 4096 May 14 05:57 .
drwxr-xr-x 5 root root 4096 May 14 05:57 ..
-rw-r--r-- 1 root root    0 May 14 05:56 file1
-rw-r--r-- 1 root root    0 May 14 05:56 file2
-rw-r--r-- 1 root root    0 May 14 05:56 file3
```

</td>
</tr>
</table>

Navigate to the test1 containing files and move it to another directory (test2)

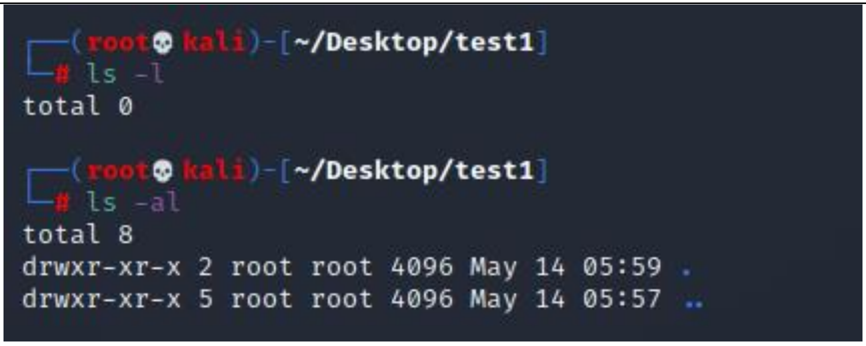


```
┌──(root💀kali)-[~/Desktop]
└─# cd test1

┌──(root💀kali)-[~/Desktop/test1]
└─# pwd
/root/Desktop/test1
```



```
┌──(root💀kali)-[~/Desktop/test1]
└─# mv file{1..3} ../test2

┌──(root💀kali)-[~/Desktop/test1]
└─# ls -l ../test2
total 0
-rw-r--r-- 1 root root 0 May 14 05:56 file1
-rw-r--r-- 1 root root 0 May 14 05:56 file2
-rw-r--r-- 1 root root 0 May 14 05:56 file3
```

After moving files test1

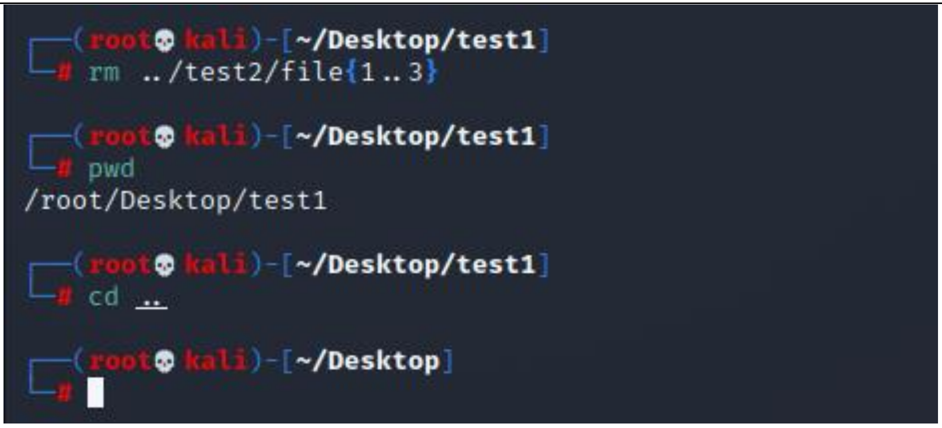


```
┌──(root💀kali)-[~/Desktop/test1]
└─# ls -l
total 0

┌──(root💀kali)-[~/Desktop/test1]
└─# ls -al
total 8
drwxr-xr-x 2 root root 4096 May 14 05:59 .
drwxr-xr-x 5 root root 4096 May 14 05:57 ..
```

Deleting files from test2

Check the path of the current directory

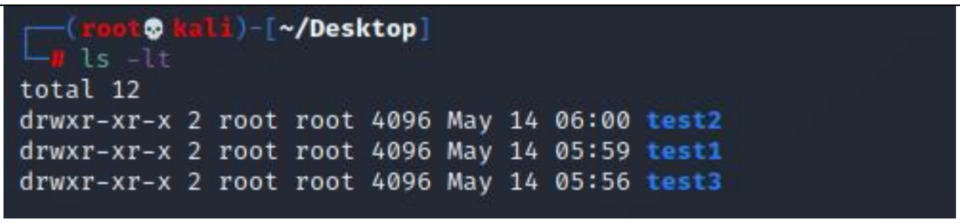
Navigate to Desktop and



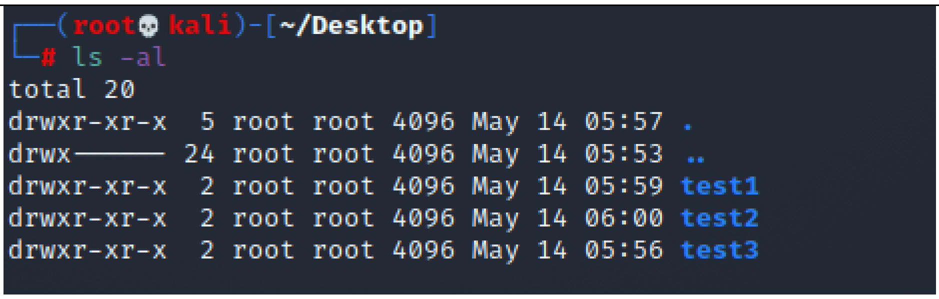
```
┌──(root💀kali)-[~/Desktop/test1]
└─# rm ../test2/file{1..3}

┌──(root💀kali)-[~/Desktop/test1]
└─# pwd
/root/Desktop/test1

┌──(root💀kali)-[~/Desktop/test1]
└─# cd ..

┌──(root💀kali)-[~/Desktop]
└─# █
```

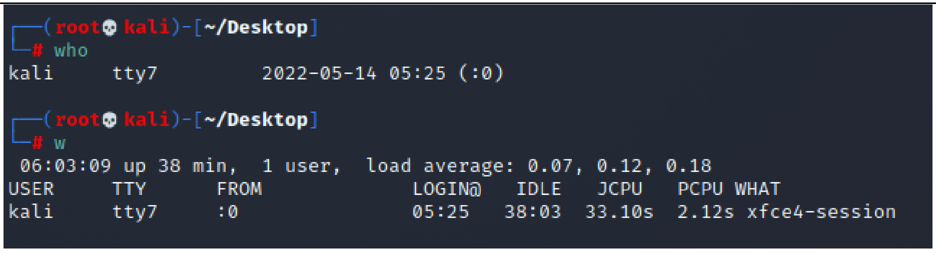
List files and folders

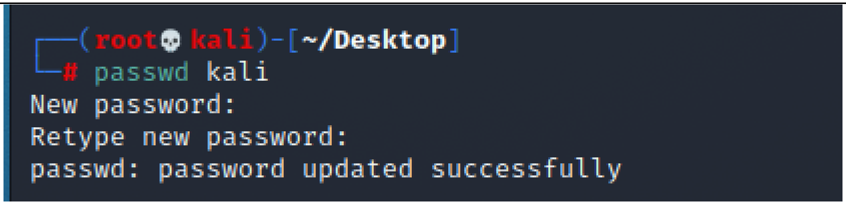
Files are seen with – at start and Folders with d

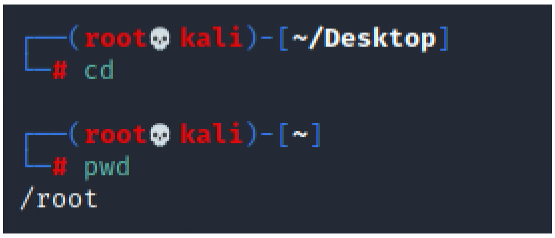


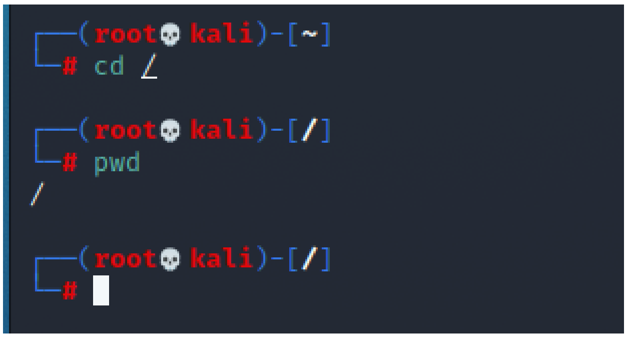
```
┌──(root💀kali)-[~/Desktop]
└─# ls -lt
total 12
drwxr-xr-x 2 root root 4096 May 14 06:00 test2
drwxr-xr-x 2 root root 4096 May 14 05:59 test1
drwxr-xr-x 2 root root 4096 May 14 05:56 test3
```

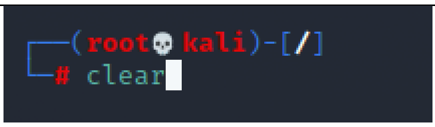
To see hidden files/folders
 	
(there are none in Desktop)
	
	`┌──(root💀kali)-[~/Desktop]`
	`└─# ls -al`
	`total 20`
	`drwxr-xr-x  5 root root 4096 May 14 05:57 .`
	`drwx------ 24 root root 4096 May 14 05:53 ..`
	`drwxr-xr-x  2 root root 4096 May 14 05:59 test1`
	`drwxr-xr-x  2 root root 4096 May 14 06:00 test2`
	`drwxr-xr-x  2 root root 4096 May 14 05:56 test3`

Check which users are connected to system	
	`┌──(root💀kali)-[~/Desktop]`
	`└─# who`
	`kali     tty7         2022-05-14 05:25 (:0)`
	
	`┌──(root💀kali)-[~/Desktop]`
	`└─# w`
	` 06:03:09 up 38 min,  1 user,  load average: 0.07, 0.12, 0.18`
	`USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT`
	`kali     tty7     :0               05:25   38:03  33.10s  2.12s xfce4-session`

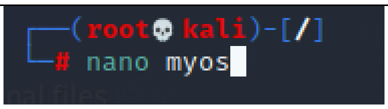
Change a users passwd	
	`┌──(root💀kali)-[~/Desktop]`
	`└─# passwd kali`
	`New password:`
	`Retype new password:`
	`passwd: password updated successfully`

Cd command	
	`┌──(root💀kali)-[~/Desktop]`
	`└─# cd`
	
	`┌──(root💀kali)-[~]`
	`└─# pwd`
	`/root`
	Changes to the users home directory

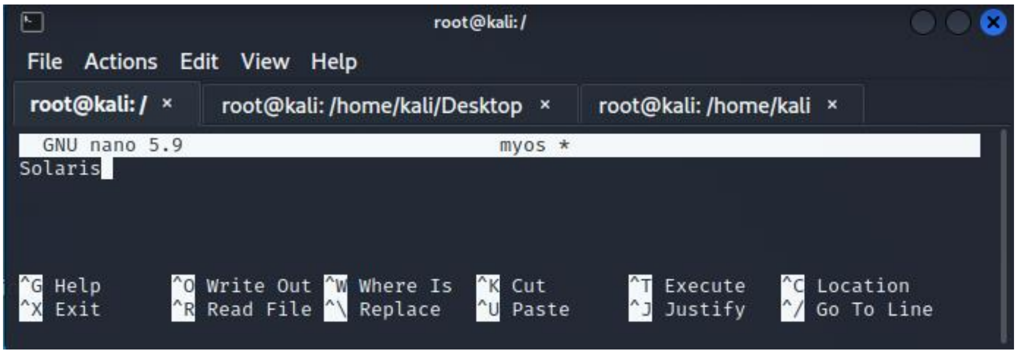
Cd /	
	`┌──(root💀kali)-[~]`
	`└─# cd /`
	
	`┌──(root💀kali)-[/]`
	`└─# pwd`
	`/`
	
	`┌──(root💀kali)-[/]`
	`└─#`
	Changes directory to the system root

Clear the terminal from output	
	`┌──(root💀kali)-[/]`
	`└─# clear`

Create file using nano Write the name of your favourite OS

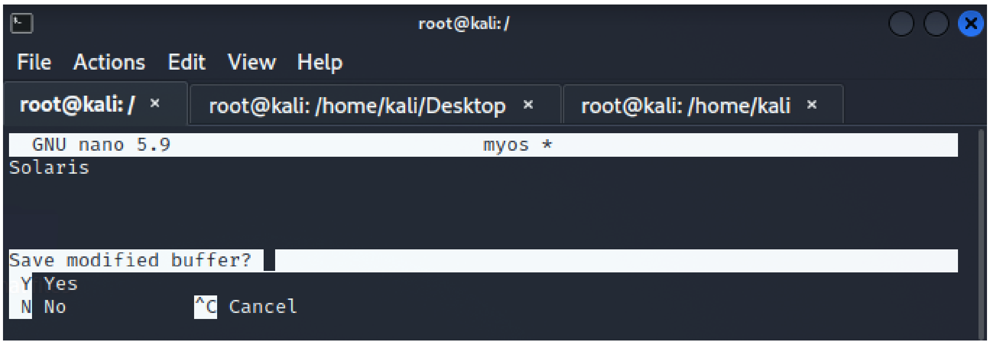


```
┌──(root💀kali)-[/]
└─# nano myos
```



```
  GNU nano 5.9                              myos *
Solaris

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

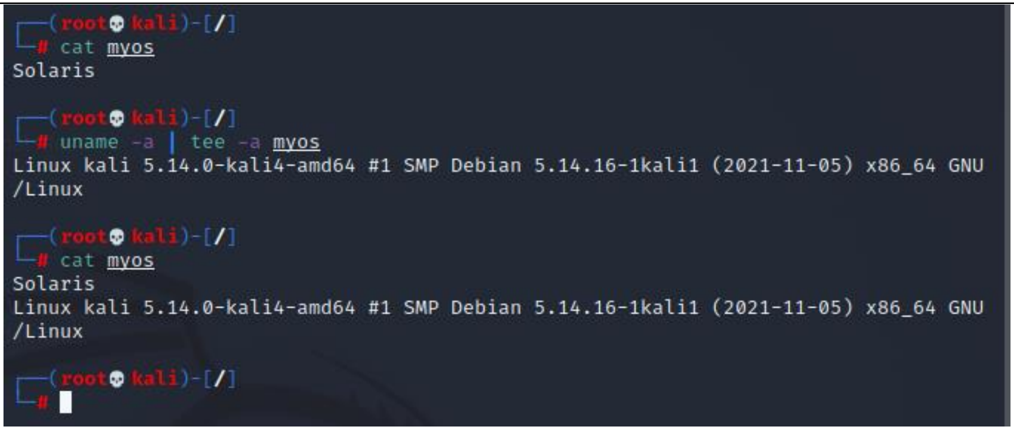
Y



```
  GNU nano 5.9                              myos *
Solaris


Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

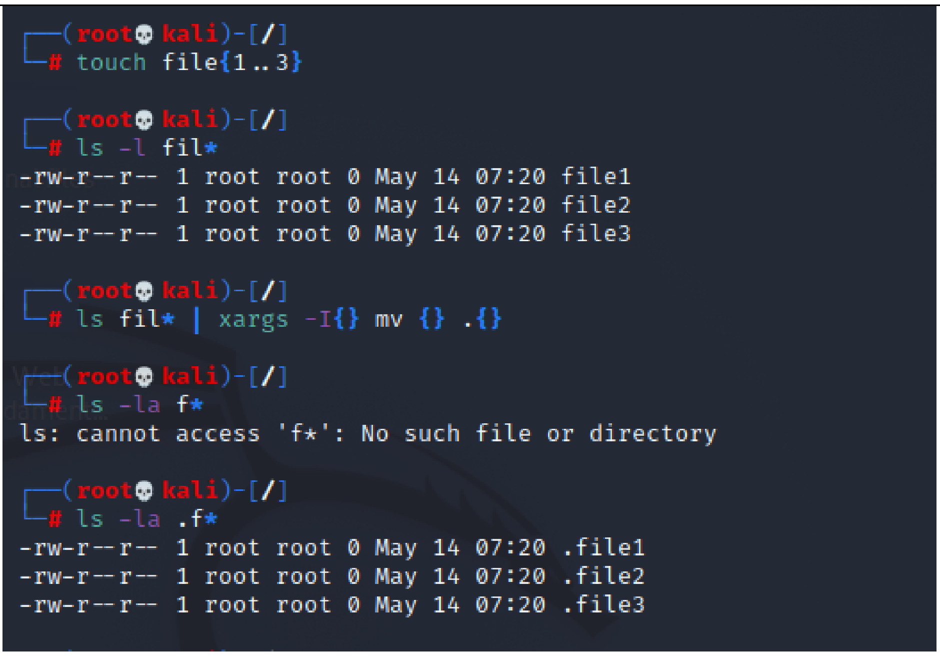
Display current os and add output to file

Execute a cmd that display the file content



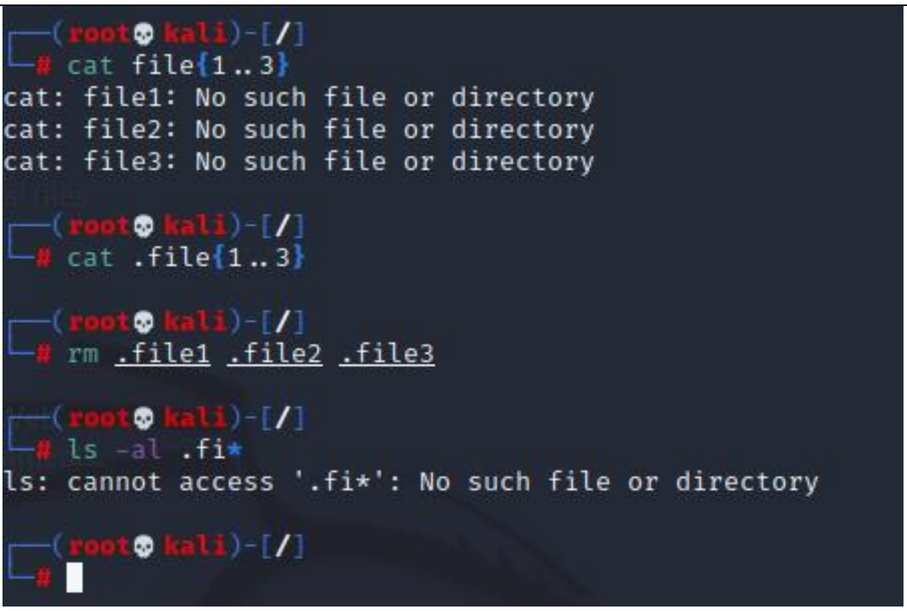
```
┌──(root💀kali)-[/]
└─# cat myos
Solaris

┌──(root💀kali)-[/]
└─# uname -a | tee -a myos
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64 GNU
/Linux

┌──(root💀kali)-[/]
└─# cat myos
Solaris
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64 GNU
/Linux

┌──(root💀kali)-[/]
└─# 
```

<table>
<tr>
<td>Create three hidden files</td>
<td>



```
┌──(root💀kali)-[/]
└─# touch file{1..3}

┌──(root💀kali)-[/]
└─# ls -l fil*
-rw-r--r-- 1 root root 0 May 14 07:20 file1
-rw-r--r-- 1 root root 0 May 14 07:20 file2
-rw-r--r-- 1 root root 0 May 14 07:20 file3

┌──(root💀kali)-[/]
└─# ls fil* | xargs -I{} mv {} .{}

┌──(root💀kali)-[/]
└─# ls -la f*
ls: cannot access 'f*': No such file or directory

┌──(root💀kali)-[/]
└─# ls -la .f*
-rw-r--r-- 1 root root 0 May 14 07:20 .file1
-rw-r--r-- 1 root root 0 May 14 07:20 .file2
-rw-r--r-- 1 root root 0 May 14 07:20 .file3
```

</td>
</tr>
<tr>
<td>Display and delete hidden files</td>
<td>



```
┌──(root💀kali)-[/]
└─# cat file{1..3}
cat: file1: No such file or directory
cat: file2: No such file or directory
cat: file3: No such file or directory

┌──(root💀kali)-[/]
└─# cat .file{1..3}

┌──(root💀kali)-[/]
└─# rm .file1 .file2 .file3

┌──(root💀kali)-[/]
└─# ls -al .fi*
ls: cannot access '.fi*': No such file or directory

┌──(root💀kali)-[/]
└─# 
```

</td>
</tr>
</table>

Part 2: The Find Command

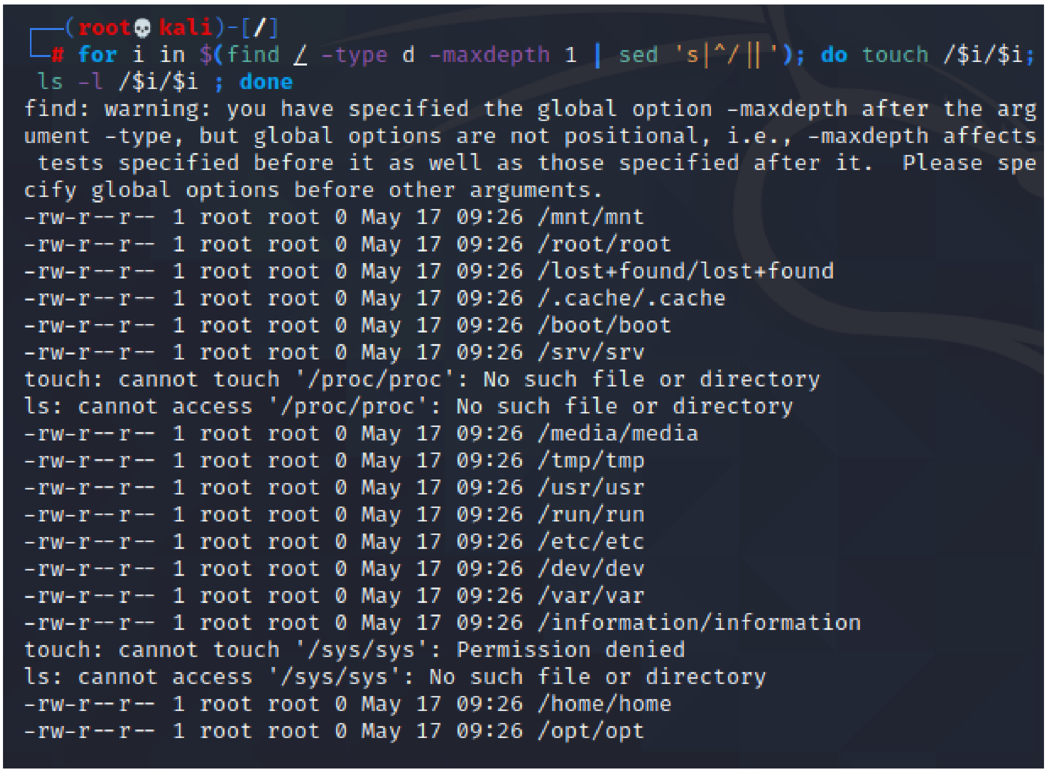
<table>
<tr>
<td>Create files in each system directory and display the path</td>
<td>

The System directories are under the root folder (/)
A one liner script is used to get the directory names

for i in $(find / -type d -maxdepth 1 | sed 's|^/||'); do echo $i
the above line will output the system directory names when run as root in the “/” folder
Sed removes the leading / and gives the directory names as string

for i in $(find / -type d -maxdepth 1 | sed 's|^/||'); do touch /$i/$i; ls -l /$i/$i ; done
A file with the same name as the system directory is created under the individual directories using the above command

Ls -l command lists the path of each of the files
The directories sys and proc have no permission.
Rest of the directories have files with same name as directory created in them.



```
┌──(root💀kali)-[/]
└─# for i in $(find / -type d -maxdepth 1 | sed 's|^/||'); do touch /$i/$i;
 ls -l /$i/$i ; done
find: warning: you have specified the global option -maxdepth after the arg
ument -type, but global options are not positional, i.e., -maxdepth affects
 tests specified before it as well as those specified after it.  Please spe
cify global options before other arguments.
-rw-r--r-- 1 root root 0 May 17 09:26 /mnt/mnt
-rw-r--r-- 1 root root 0 May 17 09:26 /root/root
-rw-r--r-- 1 root root 0 May 17 09:26 /lost+found/lost+found
-rw-r--r-- 1 root root 0 May 17 09:26 /.cache/.cache
-rw-r--r-- 1 root root 0 May 17 09:26 /boot/boot
-rw-r--r-- 1 root root 0 May 17 09:26 /srv/srv
touch: cannot touch '/proc/proc': No such file or directory
ls: cannot access '/proc/proc': No such file or directory
-rw-r--r-- 1 root root 0 May 17 09:26 /media/media
-rw-r--r-- 1 root root 0 May 17 09:26 /tmp/tmp
-rw-r--r-- 1 root root 0 May 17 09:26 /usr/usr
-rw-r--r-- 1 root root 0 May 17 09:26 /run/run
-rw-r--r-- 1 root root 0 May 17 09:26 /etc/etc
-rw-r--r-- 1 root root 0 May 17 09:26 /dev/dev
-rw-r--r-- 1 root root 0 May 17 09:26 /var/var
-rw-r--r-- 1 root root 0 May 17 09:26 /information/information
touch: cannot touch '/sys/sys': Permission denied
ls: cannot access '/sys/sys': No such file or directory
-rw-r--r-- 1 root root 0 May 17 09:26 /home/home
-rw-r--r-- 1 root root 0 May 17 09:26 /opt/opt
```

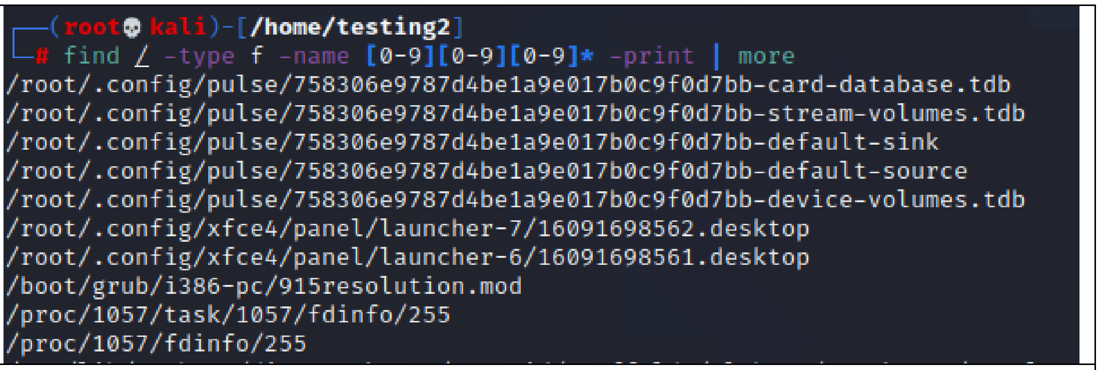
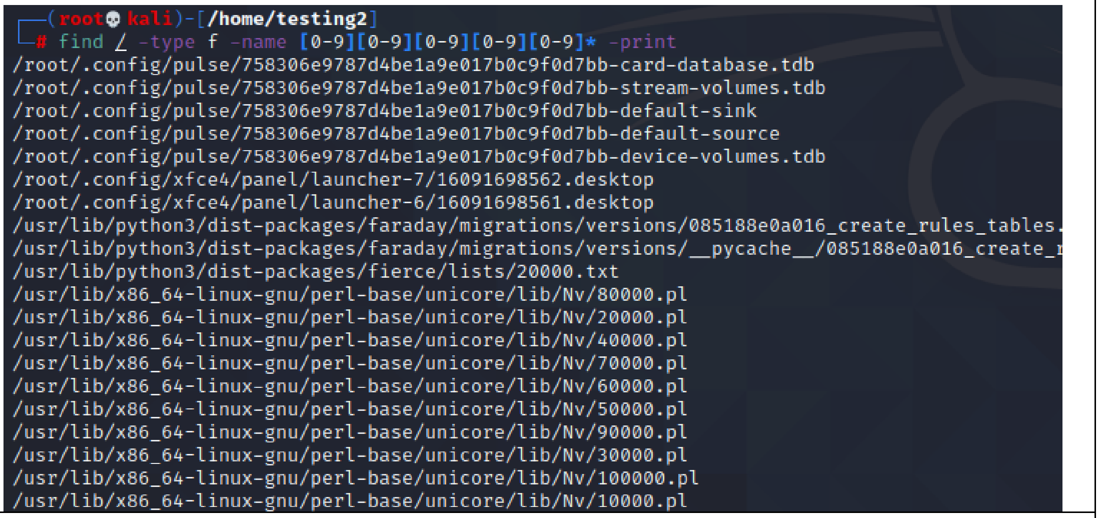
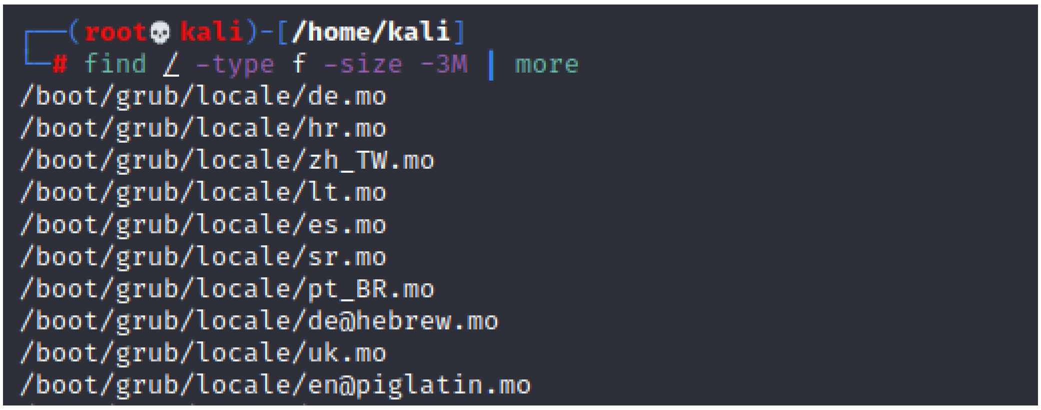
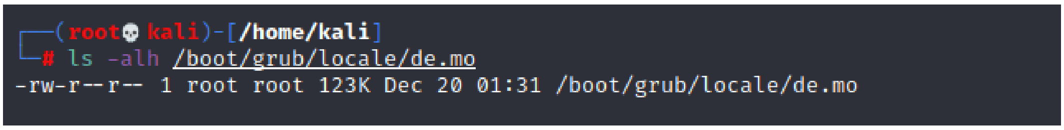
</td>
</tr>
<tr>
<td>Navigate to root directory and display all files that begin with three digit</td>
<td>

Command Used: find / -type f -name [0-9][0-9][0-9]* -print | more

Note: Square brackets (*[string]*): any of the characters of the string within square brackets return a positive match:

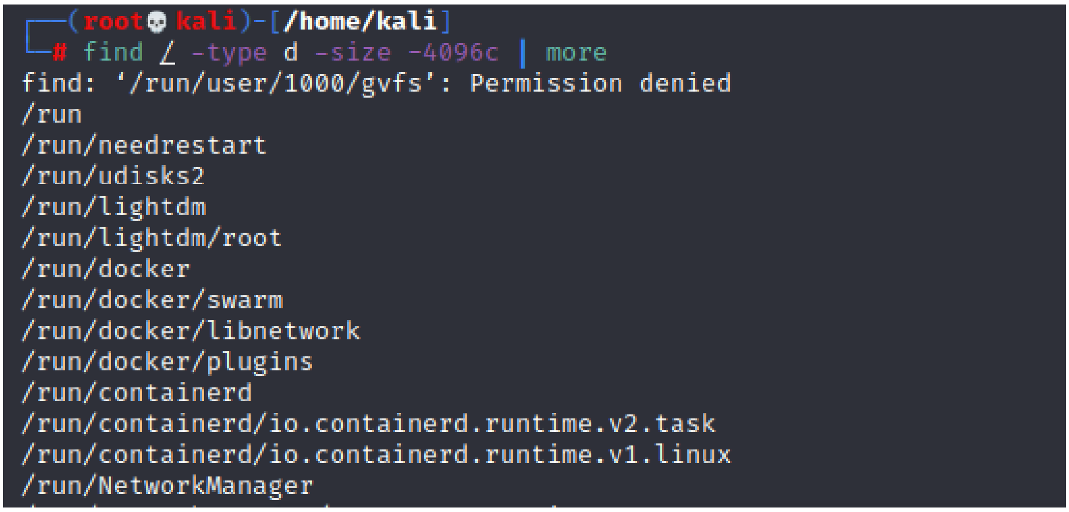
A huge list is displayed as output. Note that only the beginning of the output is shown

</td>
</tr>
</table>

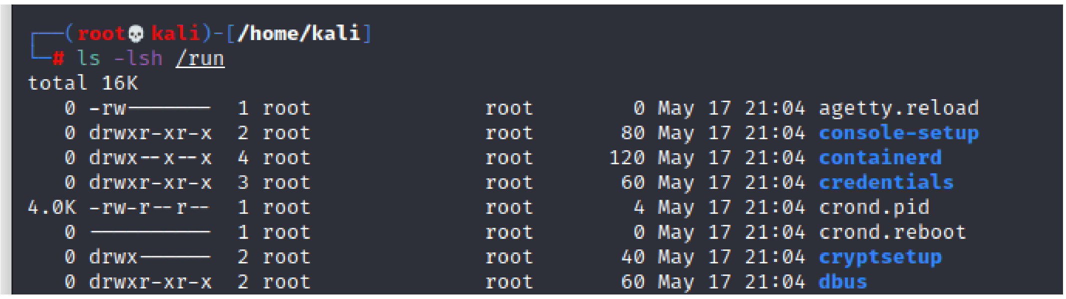
	 ┌──(root💀kali)-[/home/testing2] └─# find / -type f -name [0-9][0-9][0-9]* -print | more /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-card-database.tdb /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-stream-volumes.tdb /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-default-sink /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-default-source /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-device-volumes.tdb /root/.config/xfce4/panel/launcher-7/16091698562.desktop /root/.config/xfce4/panel/launcher-6/16091698561.desktop /boot/grub/i386-pc/915resolution.mod /proc/1057/task/1057/fdinfo/255 /proc/1057/fdinfo/255
Filenames that begin with five numbers	A hug list is displayed. Note that only the part of the output is shown  ┌──(root💀kali)-[/home/testing2] └─# find / -type f -name [0-9][0-9][0-9][0-9][0-9]* -print /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-card-database.tdb /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-stream-volumes.tdb /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-default-sink /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-default-source /root/.config/pulse/758306e9787d4be1a9e017b0c9f0d7bb-device-volumes.tdb /root/.config/xfce4/panel/launcher-7/16091698562.desktop /root/.config/xfce4/panel/launcher-6/16091698561.desktop /usr/lib/python3/dist-packages/faraday/migrations/versions/085188e0a016_create_rules_tables. /usr/lib/python3/dist-packages/faraday/migrations/versions/__pycache__/085188e0a016_create_r /usr/lib/python3/dist-packages/fierce/lists/20000.txt /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/80000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/20000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/40000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/70000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/60000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/50000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/90000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/30000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/100000.pl /usr/lib/x86_64-linux-gnu/perl-base/unicore/lib/Nv/10000.pl
Files smalle than 3 MB	find . -type f -size -3M A huge list is displayed. The screenshot shows a few  ┌──(root💀kali)-[/home/kali] └─# find / -type f -size -3M | more /boot/grub/locale/de.mo /boot/grub/locale/hr.mo /boot/grub/locale/zh_TW.mo /boot/grub/locale/lt.mo /boot/grub/locale/es.mo /boot/grub/locale/sr.mo /boot/grub/locale/pt_BR.mo /boot/grub/locale/de@hebrew.mo /boot/grub/locale/uk.mo /boot/grub/locale/en@piglatin.mo  ┌──(root💀kali)-[/home/kali] └─# ls -alh /boot/grub/locale/de.mo -rw-r--r-- 1 root root 123K Dec 20 01:31 /boot/grub/locale/de.mo

<table>
<tr>
<td>Directories smaller than 4MB</td>
<td>

Find -type d -size -4M. a huge list is generated. The top few are shown and a sample directory with size less than 4MB shown



```
┌──(root💀kali)-[/home/kali]
└─# find / -type d -size -4096c | more
find: '/run/user/1000/gvfs': Permission denied
/run
/run/needrestart
/run/udisks2
/run/lightdm
/run/lightdm/root
/run/docker
/run/docker/swarm
/run/docker/libnetwork
/run/docker/plugins
/run/containerd
/run/containerd/io.containerd.runtime.v2.task
/run/containerd/io.containerd.runtime.v1.linux
/run/NetworkManager
```

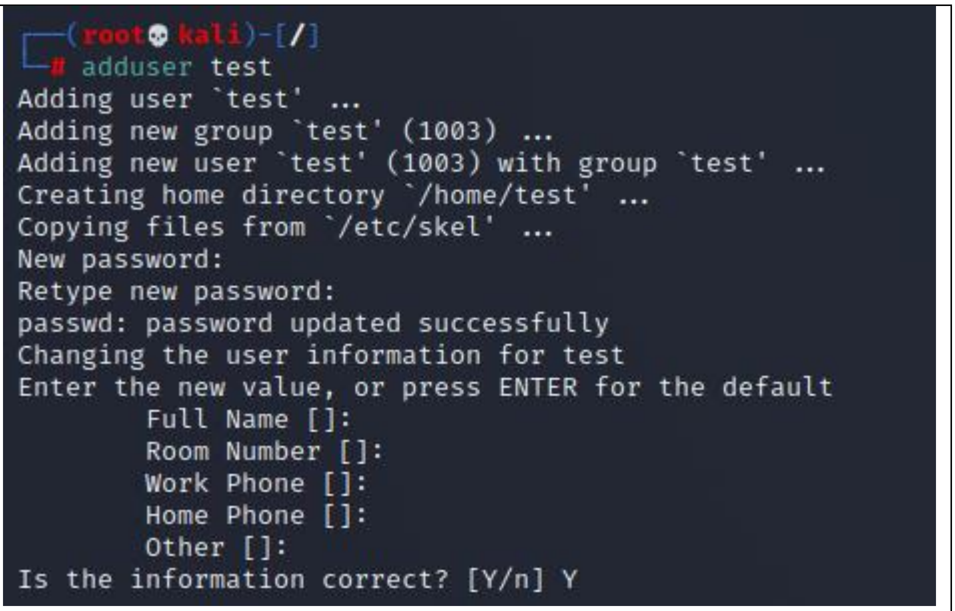


```
┌──(root💀kali)-[/home/kali]
└─# ls -lsh /run
total 16K
   0 -rw-------  1 root            root         0 May 17 21:04 agetty.reload
   0 drwxr-xr-x  2 root            root        80 May 17 21:04 console-setup
   0 drwx--x--x  4 root            root       120 May 17 21:04 containerd
   0 drwxr-xr-x  3 root            root        60 May 17 21:04 credentials
4.0K -rw-r--r--  1 root            root         4 May 17 21:04 crond.pid
   0 ----------  1 root            root         0 May 17 21:04 crond.reboot
   0 drwx------  2 root            root        40 May 17 21:04 cryptsetup
   0 drwxr-xr-x  2 root            root        60 May 17 21:04 dbus
```

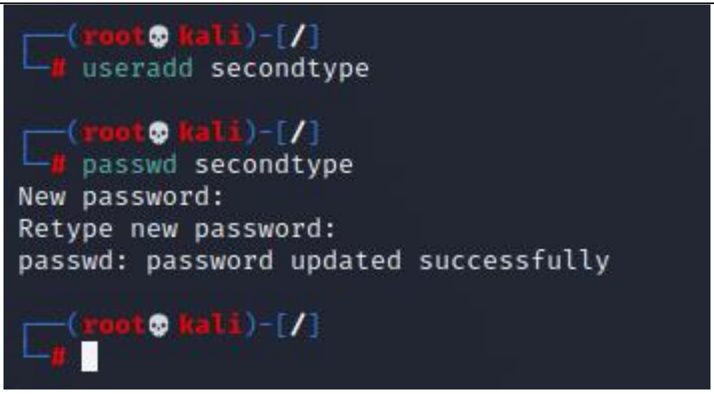
</td>
</tr>
</table>

Part 3: User & Group Management

Add user

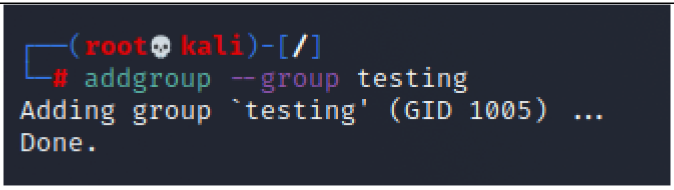


```
┌──(root💀kali)-[/]
└─# adduser test
Adding user `test' ...
Adding new group `test' (1003) ...
Adding new user `test' (1003) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
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] Y
```



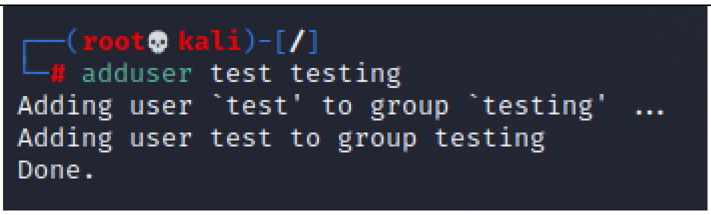
```
┌──(root💀kali)-[/]
└─# useradd secondtype

┌──(root💀kali)-[/]
└─# passwd secondtype
New password:
Retype new password:
passwd: password updated successfully

┌──(root💀kali)-[/]
└─# 
```

Add a group



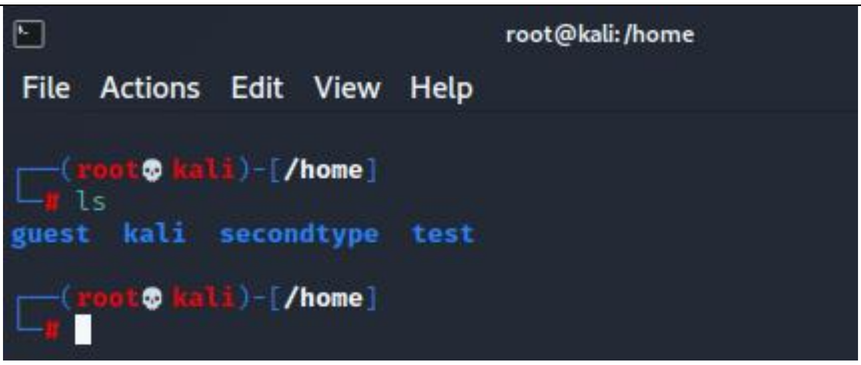
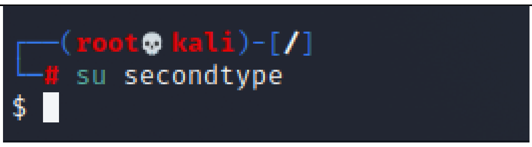
```
┌──(root💀kali)-[/]
└─# addgroup --group testing
Adding group `testing' (GID 1005) ...
Done.
```

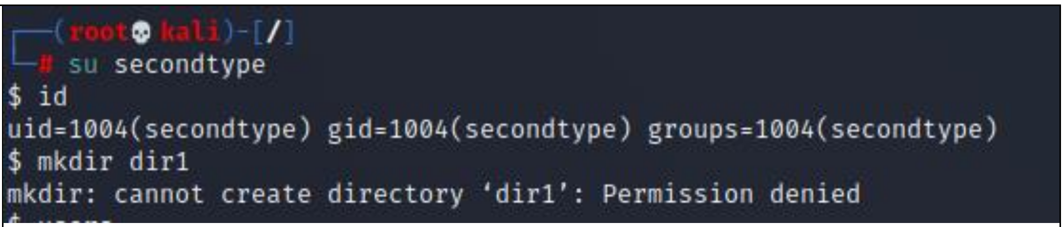
Moved the user test to testing

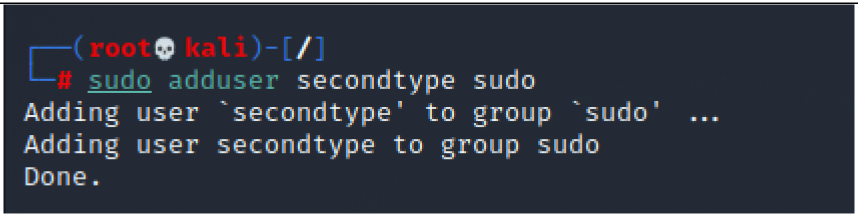


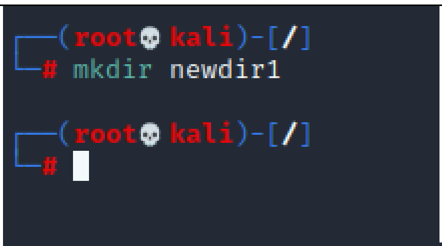
```
┌──(root💀kali)-[/]
└─# adduser test testing
Adding user `test' to group `testing' ...
Adding user test to group testing
Done.
```

Command to see all users and their groups – cat /etc/passwd
Location of all user directories - /home

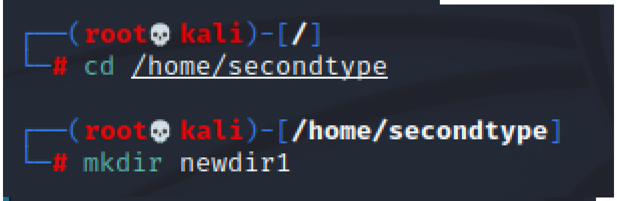
	 root@kali: /home ┌──(root💀kali)-[/home] └─# ls guest kali secondtype test ┌──(root💀kali)-[/home] └─#
Switch to other user	 ┌──(root💀kali)-[/] └─# su secondtype $

How to create a directory with the user	
	┌──(root💀kali)-[/]
	└─# su secondtype
	$ id
	uid=1004(secondtype) gid=1004(secondtype) groups=1004(secondtype)
	$ mkdir dir1
	mkdir: cannot create directory ‘dir1’: Permission denied
	since the user is not added sudoer list, he cannot create directory in location other thanhis home directory

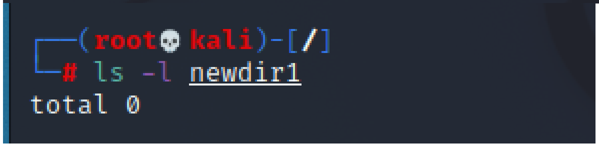
Adding the user in the sudo group allows the user to create a directory anywhere	 ┌──(root💀kali)-[/] └─# sudo adduser secondtype sudo Adding user `secondtype' to group `sudo' ... Adding user secondtype to group sudo Done.



```
┌──(root💀kali)-[/]
└─# mkdir newdir1

┌──(root💀kali)-[/]
└─# 
```

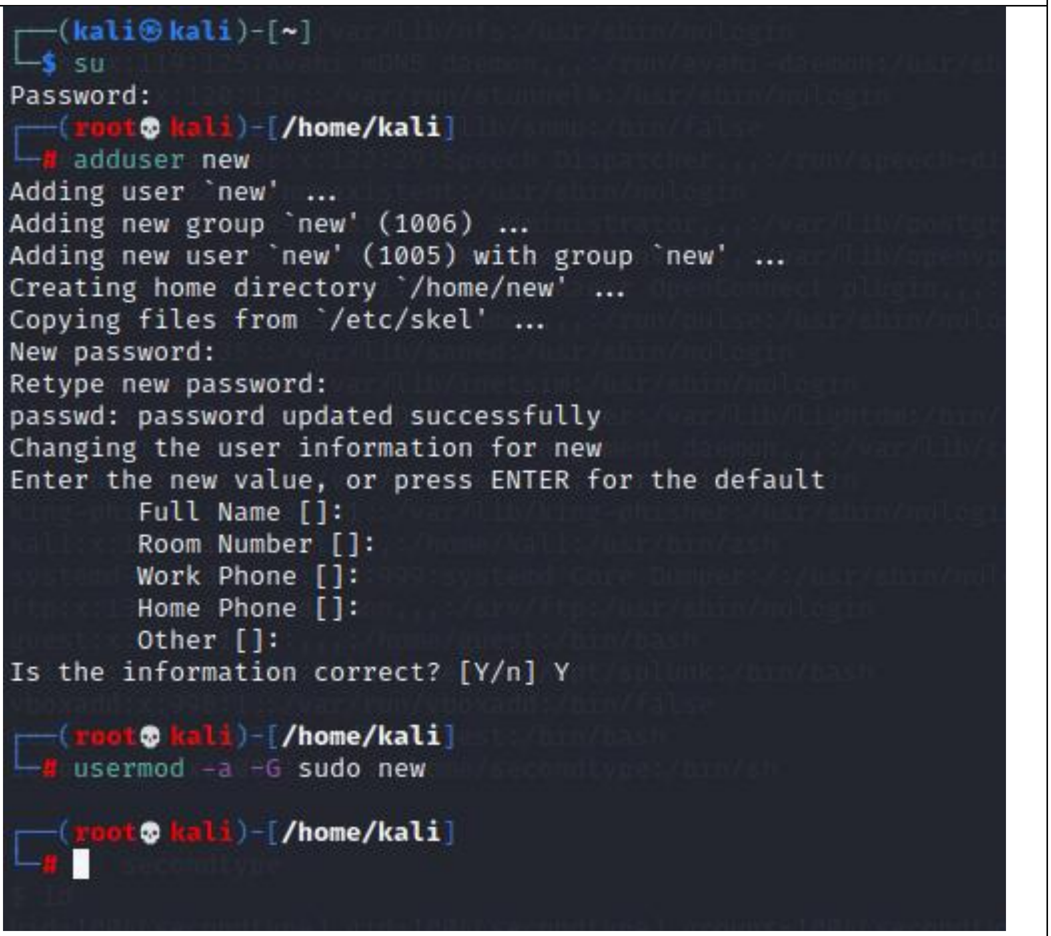


```
┌──(root💀kali)-[/]
└─# cd /home/secondtype

┌──(root💀kali)-[/home/secondtype]
└─# mkdir newdir1
```

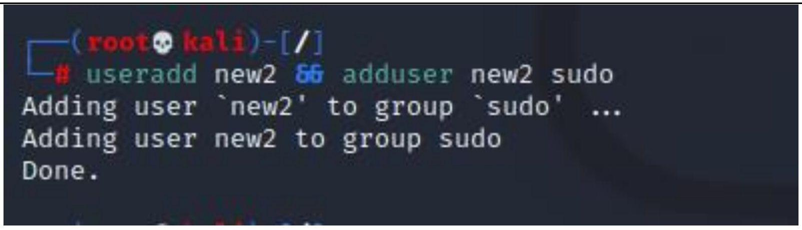
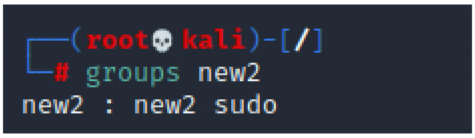


```
┌──(root💀kali)-[/]
└─# ls -l newdir1
total 0
```

Swirtch to root
Create a new user
Add him to sudo group in single command



```
┌──(kali㉿kali)-[~]
└─$ su
Password:
┌──(root💀kali)-[/home/kali]
└─# adduser new
Adding user `new' ...
Adding new group `new' (1006) ...
Adding new user `new' (1005) with group `new' ...
Creating home directory `/home/new' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for new
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] Y

┌──(root💀kali)-[/home/kali]
└─# usermod -a -G sudo new

┌──(root💀kali)-[/home/kali]
└─# 
```

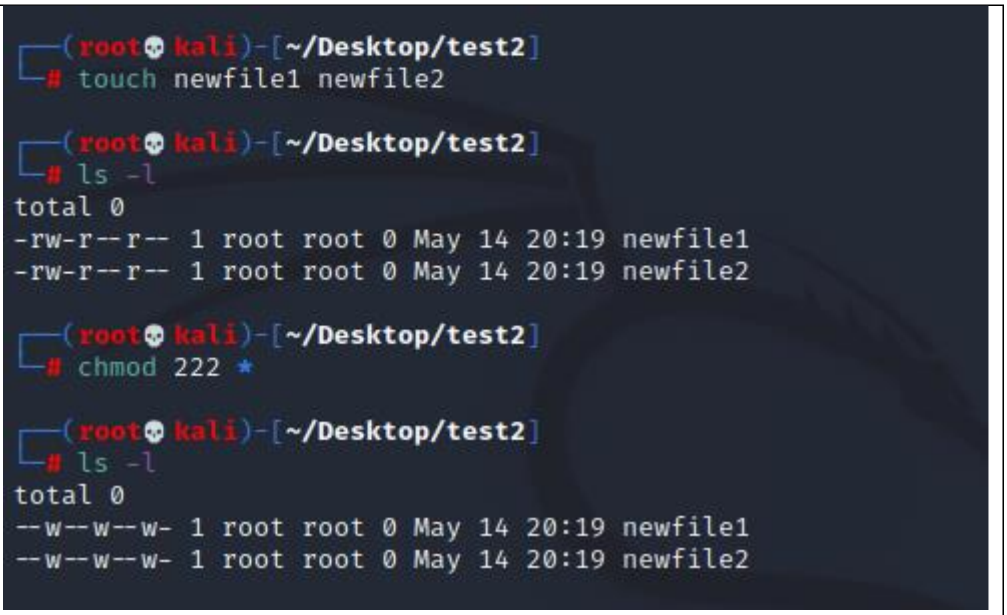
Single command	 

```
┌──(root💀kali)-[/]
└─# useradd new2 && adduser new2 sudo
Adding user `new2' to group `sudo' ...
Adding user new2 to group sudo
Done.
```

```
┌──(root💀kali)-[/]
└─# groups new2
new2 : new2 sudo
```

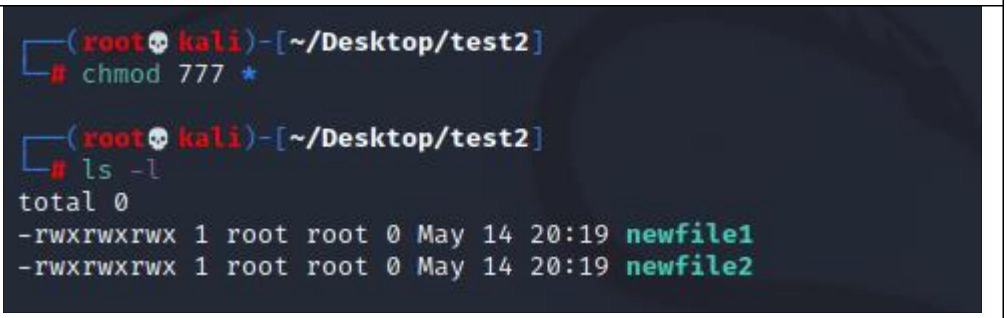
Part 4: Permissions

<table>
<tr>
<td>Grant only write permission to all files in the direectory</td>
<td>



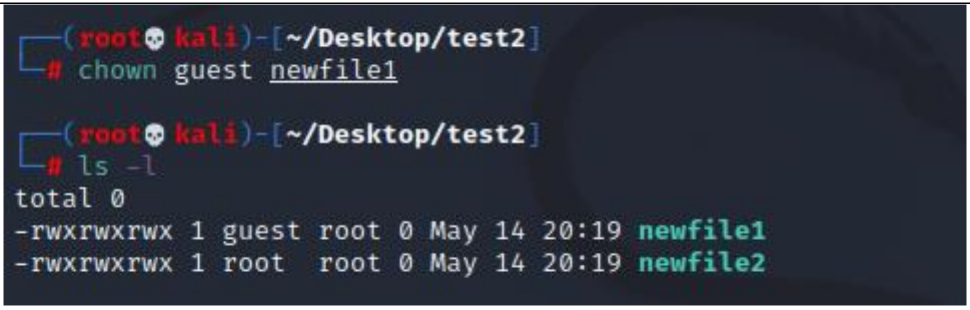
```
┌──(root💀kali)-[~/Desktop/test2]
└─# touch newfile1 newfile2

┌──(root💀kali)-[~/Desktop/test2]
└─# ls -l
total 0
-rw-r--r-- 1 root root 0 May 14 20:19 newfile1
-rw-r--r-- 1 root root 0 May 14 20:19 newfile2

┌──(root💀kali)-[~/Desktop/test2]
└─# chmod 222 *

┌──(root💀kali)-[~/Desktop/test2]
└─# ls -l
total 0
--w--w--w- 1 root root 0 May 14 20:19 newfile1
--w--w--w- 1 root root 0 May 14 20:19 newfile2
```

</td>
</tr>
<tr>
<td>Giving highest level of perm</td>
<td>



```
┌──(root💀kali)-[~/Desktop/test2]
└─# chmod 777 *

┌──(root💀kali)-[~/Desktop/test2]
└─# ls -l
total 0
-rwxrwxrwx 1 root root 0 May 14 20:19 newfile1
-rwxrwxrwx 1 root root 0 May 14 20:19 newfile2
```

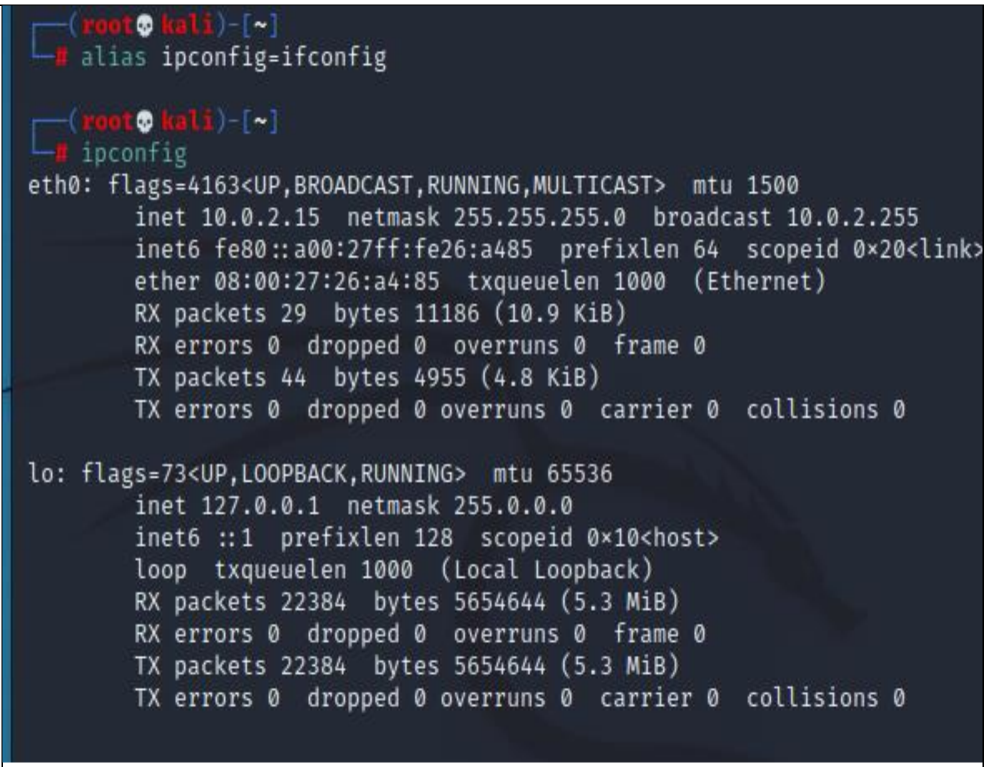
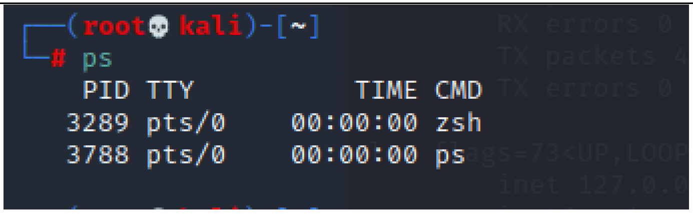
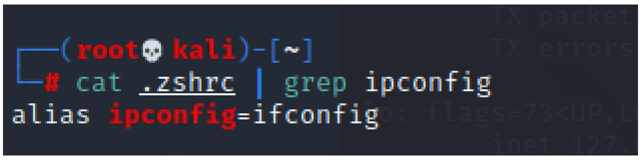
</td>
</tr>
<tr>
<td>Change owner to new owner</td>
<td>



```
┌──(root💀kali)-[~/Desktop/test2]
└─# chown guest newfile1

┌──(root💀kali)-[~/Desktop/test2]
└─# ls -l
total 0
-rwxrwxrwx 1 guest root 0 May 14 20:19 newfile1
-rwxrwxrwx 1 root  root 0 May 14 20:19 newfile2
```

</td>
</tr>
</table>

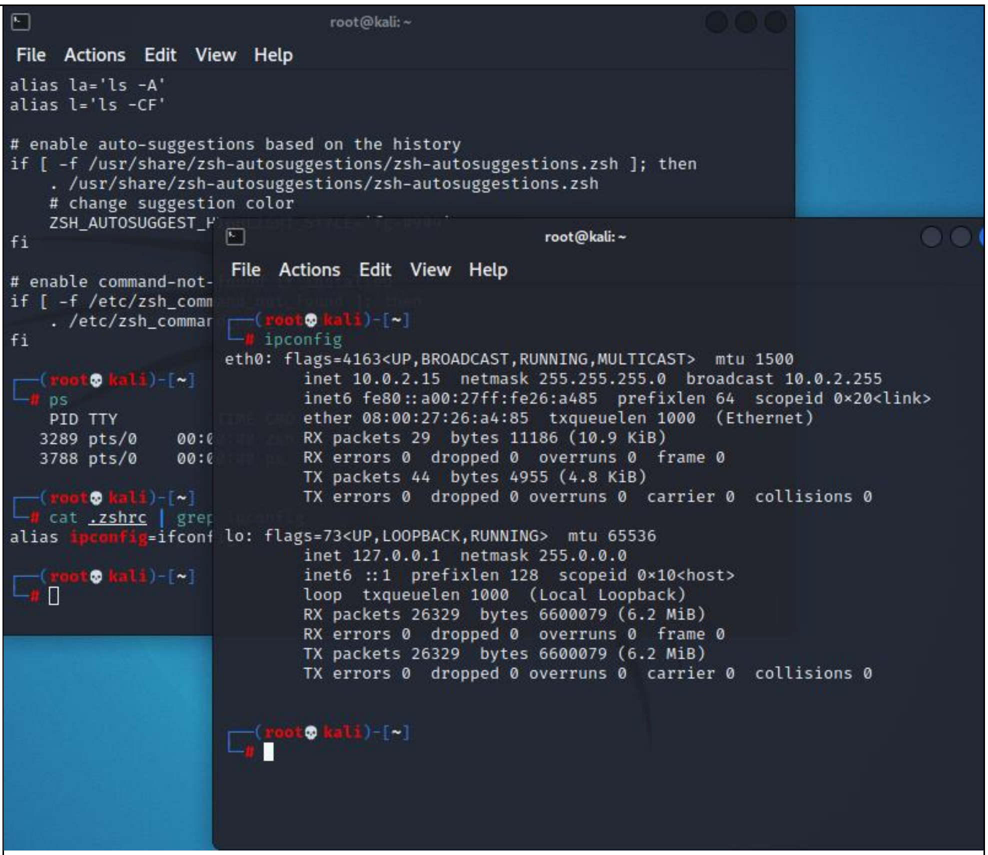
Part 5: Alias

Alias ifconfig to ipconfig	
	 

```
┌──(root💀kali)-[~]
└─# alias ipconfig=ifconfig

┌──(root💀kali)-[~]
└─# ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe26:a485  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:26:a4:85  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 11186 (10.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 4955 (4.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 22384  bytes 5654644 (5.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22384  bytes 5654644 (5.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

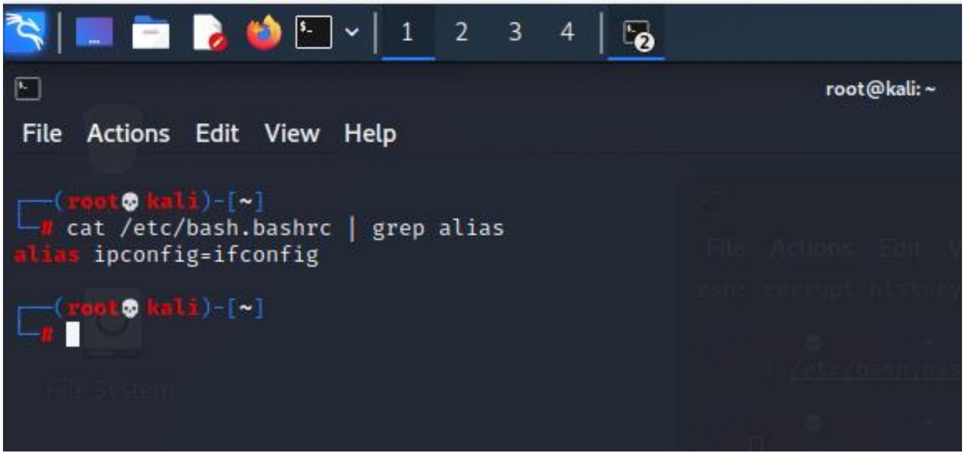
```
┌──(root💀kali)-[~]
└─# ps
    PID TTY          TIME CMD
   3289 pts/0    00:00:00 zsh
   3788 pts/0    00:00:00 ps
```

```
┌──(root💀kali)-[~]
└─# cat .zshrc | grep ipconfig
alias ipconfig=ifconfig
```

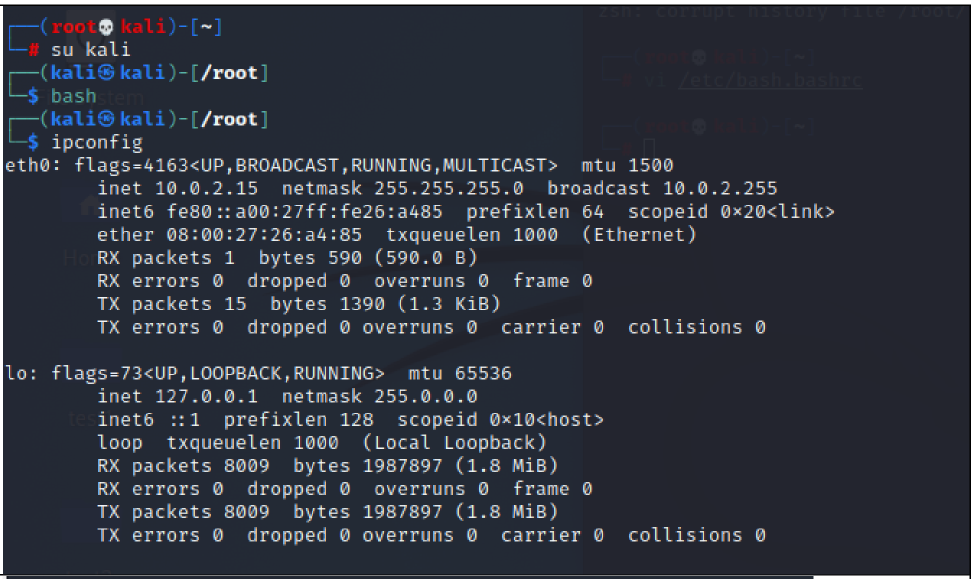
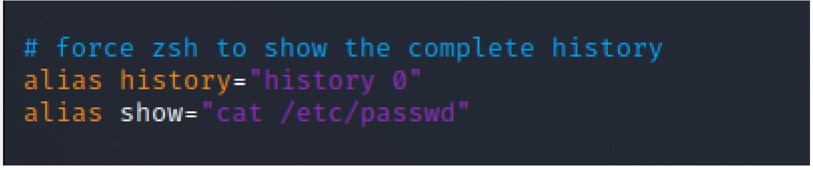
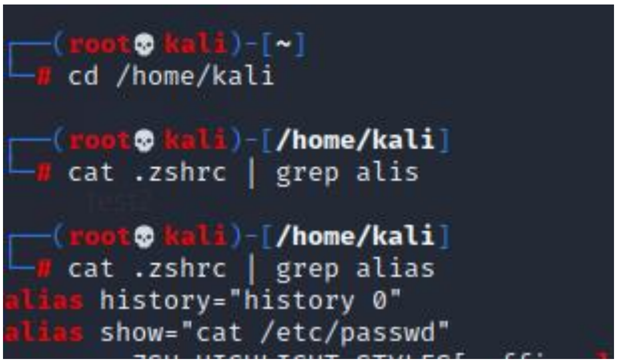
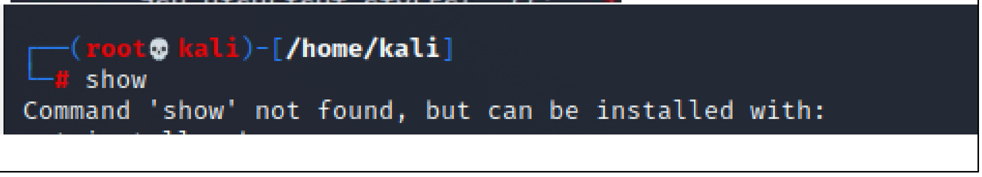


```
alias la='ls -A'
alias l='ls -CF'

# enable auto-suggestions based on the history
if [ -f /usr/share/zsh-autosuggestions/zsh-autosuggestions.zsh ]; then
    . /usr/share/zsh-autosuggestions/zsh-autosuggestions.zsh
    # change suggestion color
    ZSH_AUTOSUGGEST_H
fi

# enable command-not-
if [ -f /etc/zsh_comm
    . /etc/zsh_commar
fi

┌──(root💀kali)-[~]
└─# ps
    PID TTY
   3289 pts/0    00:0
   3788 pts/0    00:0

┌──(root💀kali)-[~]
└─# cat .zshrc | grep
alias ipconfig=ifconf

┌──(root💀kali)-[~]
└─# ▯
```

```
┌──(root💀kali)-[~]
└─# ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe26:a485  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:26:a4:85  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 11186 (10.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 4955 (4.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26329  bytes 6600079 (6.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26329  bytes 6600079 (6.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀kali)-[~]
└─# █
```



```
┌──(root💀kali)-[~]
└─# cat /etc/bash.bashrc | grep alias
alias ipconfig=ifconfig

┌──(root💀kali)-[~]
└─# █
```

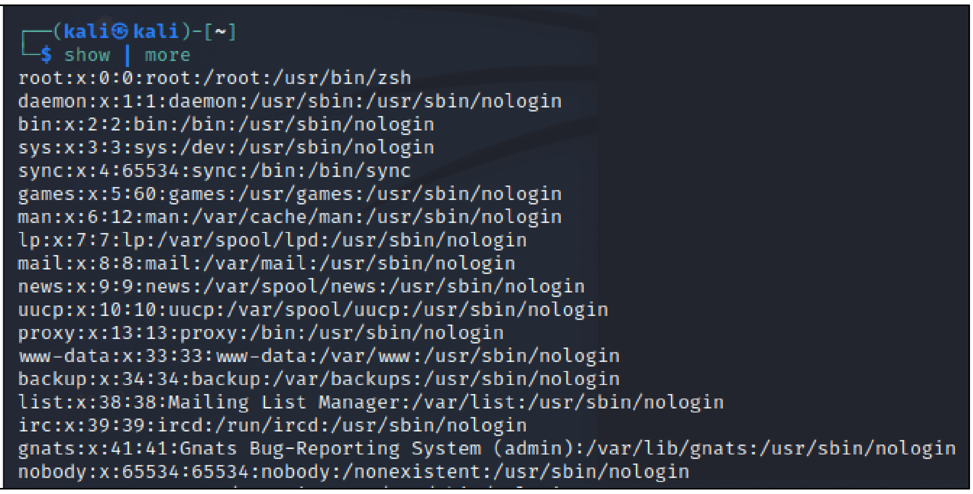
Adding alias for all users in /etc/bash.bashrc	
Change ~/.zshrc for kali user Only for user kali, the show alias shows /etc/passwd	  

```
┌──(root💀kali)-[~]
└─# su kali
┌──(kali㉿kali)-[/root]
└─$ bash
┌──(kali㉿kali)-[/root]
└─$ ipconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe26:a485  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:26:a4:85  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1390 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8009  bytes 1987897 (1.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8009  bytes 1987897 (1.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
# force zsh to show the complete history
alias history="history 0"
alias show="cat /etc/passwd"
```

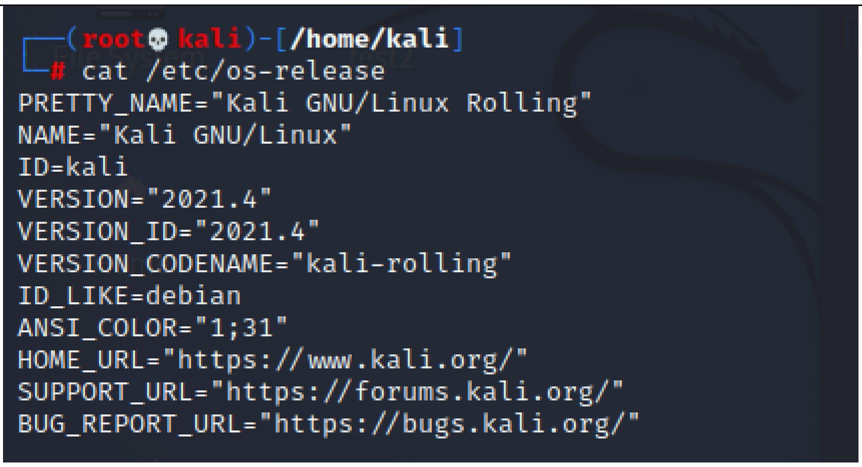
```
┌──(root💀kali)-[~]
└─# cd /home/kali

┌──(root💀kali)-[/home/kali]
└─# cat .zshrc | grep alis

┌──(root💀kali)-[/home/kali]
└─# cat .zshrc | grep alias
alias history="history 0"
alias show="cat /etc/passwd"
```

```
┌──(root💀kali)-[/home/kali]
└─# show
Command 'show' not found, but can be installed with:
```

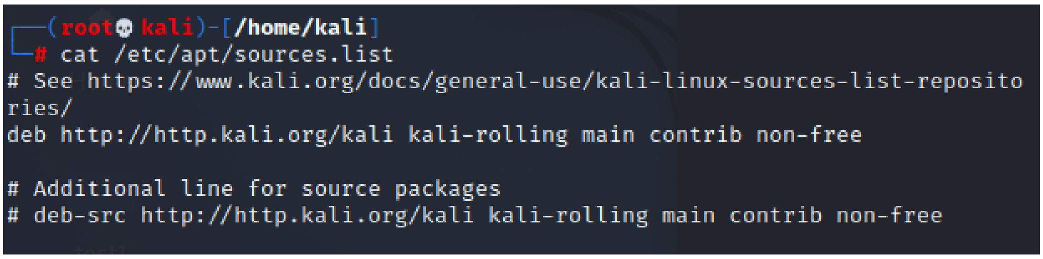


```
┌──(kali㉿kali)-[~]
└─$ show | more
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

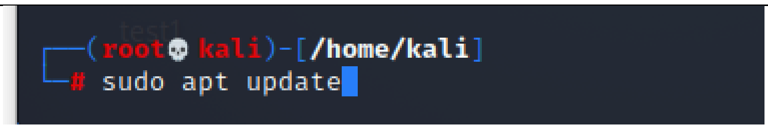
Part 6 : System Update and Apt Usage



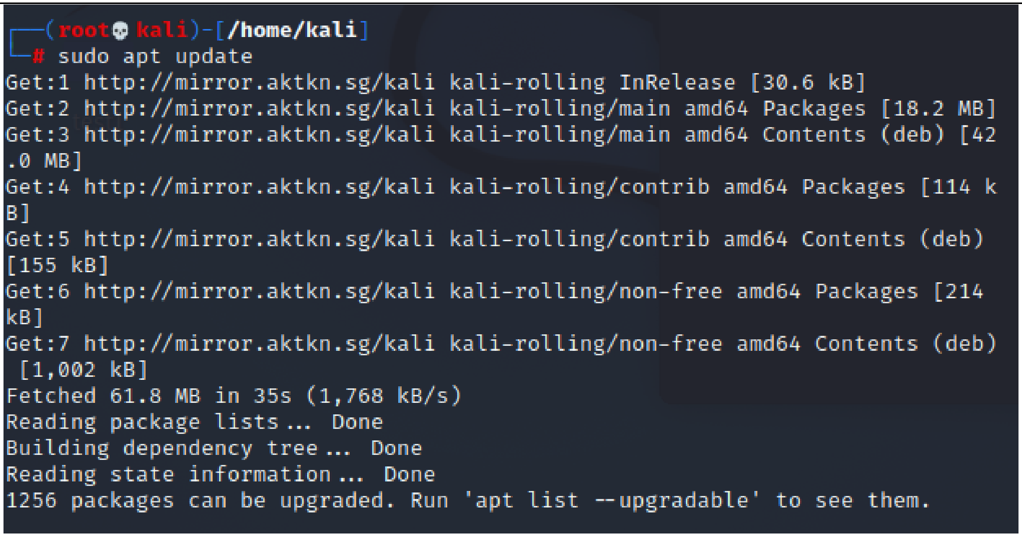
```
┌──(root💀kali)-[/home/kali]
└─# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2021.4"
VERSION_ID="2021.4"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
```



```
┌──(root💀kali)-[/home/kali]
└─# cat /etc/apt/sources.list
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-reposito
ries/
deb http://http.kali.org/kali kali-rolling main contrib non-free

# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

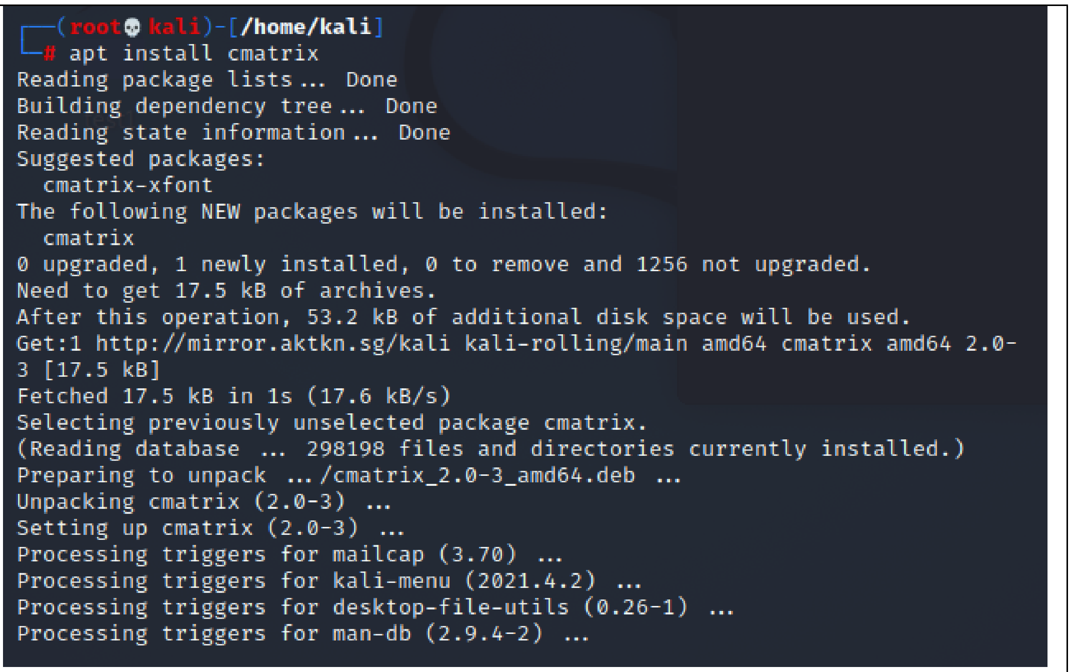


```
┌──(root💀kali)-[/home/kali]
└─# sudo apt update
```



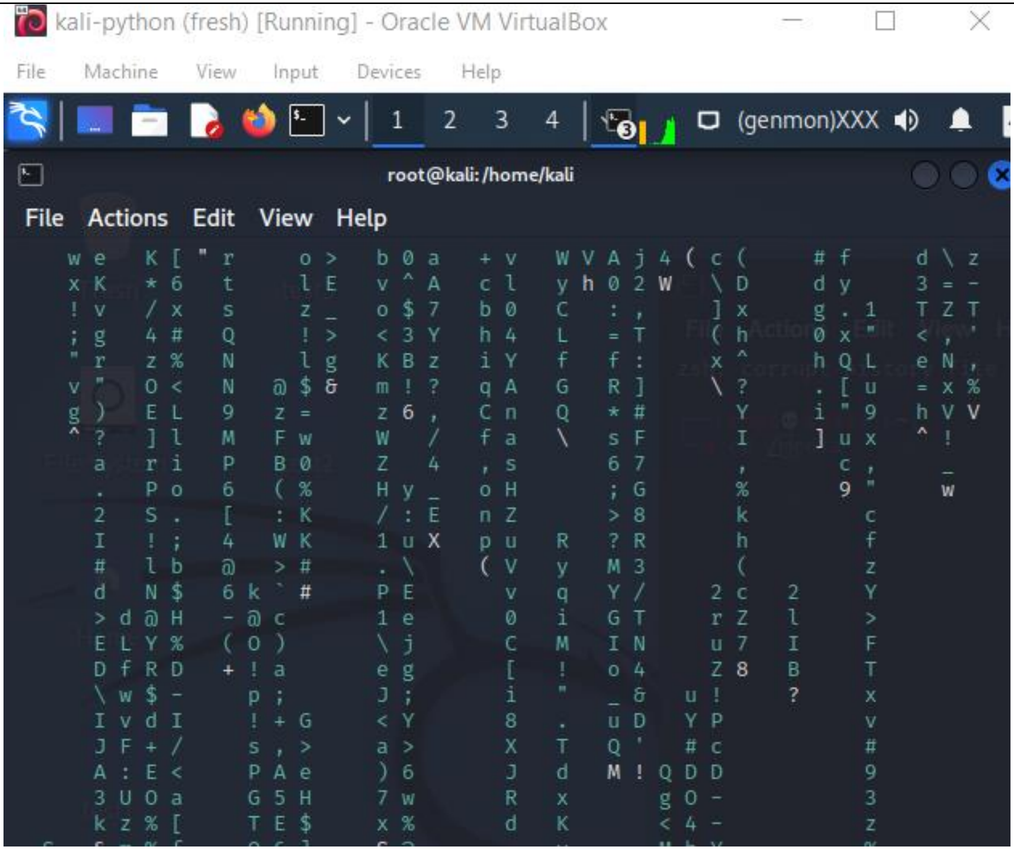
```
┌──(root💀kali)-[/home/kali]
└─# sudo apt update
Get:1 http://mirror.aktkn.sg/kali kali-rolling InRelease [30.6 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Packages [18.2 MB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 Contents (deb) [42
.0 MB]
Get:4 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Packages [114 k
B]
Get:5 http://mirror.aktkn.sg/kali kali-rolling/contrib amd64 Contents (deb)
[155 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Packages [214
kB]
Get:7 http://mirror.aktkn.sg/kali kali-rolling/non-free amd64 Contents (deb)
 [1,002 kB]
Fetched 61.8 MB in 35s (1,768 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1256 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

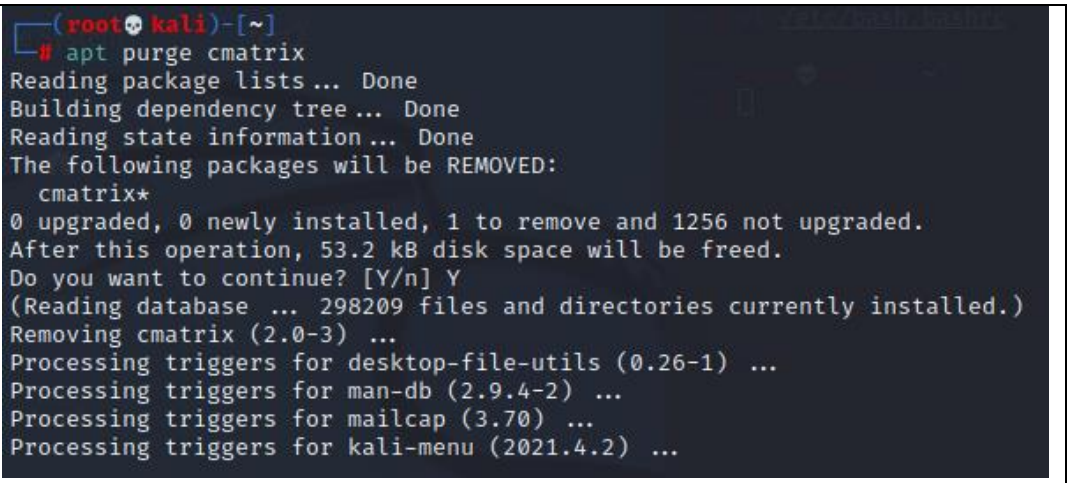
This command updates the source . Software Updates/ Newer packages will become available for install. Downloads package information from the configured sources.The packages can be installed or updated using apt install command



```
┌──(root💀 kali)-[/home/kali]
└─# apt install cmatrix
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  cmatrix-xfont
The following NEW packages will be installed:
  cmatrix
0 upgraded, 1 newly installed, 0 to remove and 1256 not upgraded.
Need to get 17.5 kB of archives.
After this operation, 53.2 kB of additional disk space will be used.
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 cmatrix amd64 2.0-
3 [17.5 kB]
Fetched 17.5 kB in 1s (17.6 kB/s)
Selecting previously unselected package cmatrix.
(Reading database ... 298198 files and directories currently installed.)
Preparing to unpack .../cmatrix_2.0-3_amd64.deb ...
Unpacking cmatrix (2.0-3) ...
Setting up cmatrix (2.0-3) ...
Processing triggers for mailcap (3.70) ...
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for man-db (2.9.4-2) ...
```

Execute cmatrix

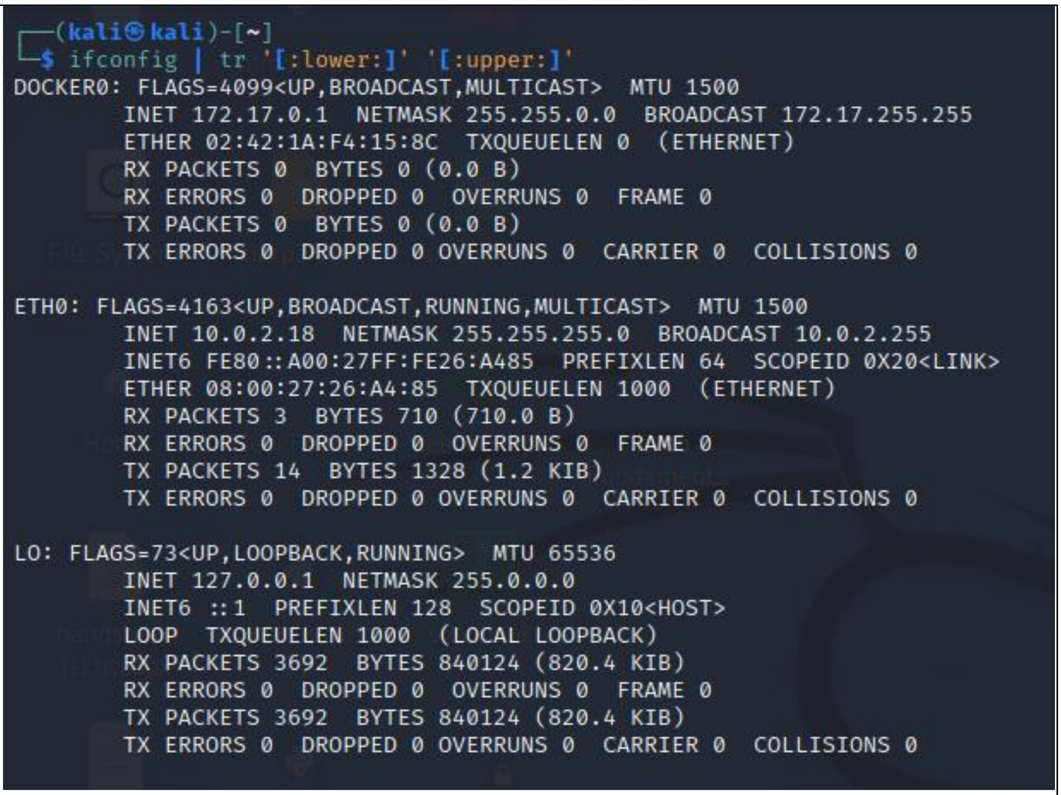


Remove cmatrix	

```
┌──(root💀kali)-[~]
└─# apt purge cmatrix
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  cmatrix*
0 upgraded, 0 newly installed, 1 to remove and 1256 not upgraded.
After this operation, 53.2 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 298209 files and directories currently installed.)
Removing cmatrix (2.0-3) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for mailcap (3.70) ...
Processing triggers for kali-menu (2021.4.2) ...
```

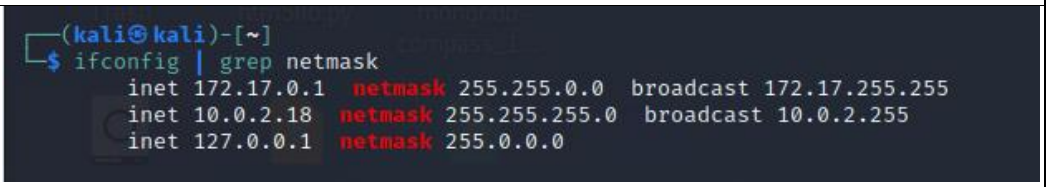
Part 7: Ifconfig and Address Settings

<table>
<tr>
<td>Ifconfig output to upper case</td>
<td>



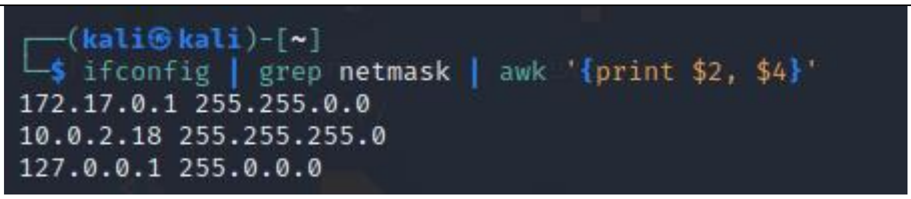
```
┌──(kali㉿kali)-[~]
└─$ ifconfig | tr '[:lower:]' '[:upper:]'
DOCKER0: FLAGS=4099<UP,BROADCAST,MULTICAST>  MTU 1500
        INET 172.17.0.1  NETMASK 255.255.0.0  BROADCAST 172.17.255.255
        ETHER 02:42:1A:F4:15:8C  TXQUEUELEN 0  (ETHERNET)
        RX PACKETS 0  BYTES 0 (0.0 B)
        RX ERRORS 0  DROPPED 0  OVERRUNS 0  FRAME 0
        TX PACKETS 0  BYTES 0 (0.0 B)
        TX ERRORS 0  DROPPED 0 OVERRUNS 0  CARRIER 0  COLLISIONS 0

ETH0: FLAGS=4163<UP,BROADCAST,RUNNING,MULTICAST>  MTU 1500
        INET 10.0.2.18  NETMASK 255.255.255.0  BROADCAST 10.0.2.255
        INET6 FE80::A00:27FF:FE26:A485  PREFIXLEN 64  SCOPEID 0X20<LINK>
        ETHER 08:00:27:26:A4:85  TXQUEUELEN 1000  (ETHERNET)
        RX PACKETS 3  BYTES 710 (710.0 B)
        RX ERRORS 0  DROPPED 0  OVERRUNS 0  FRAME 0
        TX PACKETS 14  BYTES 1328 (1.2 KIB)
        TX ERRORS 0  DROPPED 0 OVERRUNS 0  CARRIER 0  COLLISIONS 0

LO: FLAGS=73<UP,LOOPBACK,RUNNING>  MTU 65536
        INET 127.0.0.1  NETMASK 255.0.0.0
        INET6 ::1  PREFIXLEN 128  SCOPEID 0X10<HOST>
        LOOP  TXQUEUELEN 1000  (LOCAL LOOPBACK)
        RX PACKETS 3692  BYTES 840124 (820.4 KIB)
        RX ERRORS 0  DROPPED 0  OVERRUNS 0  FRAME 0
        TX PACKETS 3692  BYTES 840124 (820.4 KIB)
        TX ERRORS 0  DROPPED 0 OVERRUNS 0  CARRIER 0  COLLISIONS 0
```

</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>



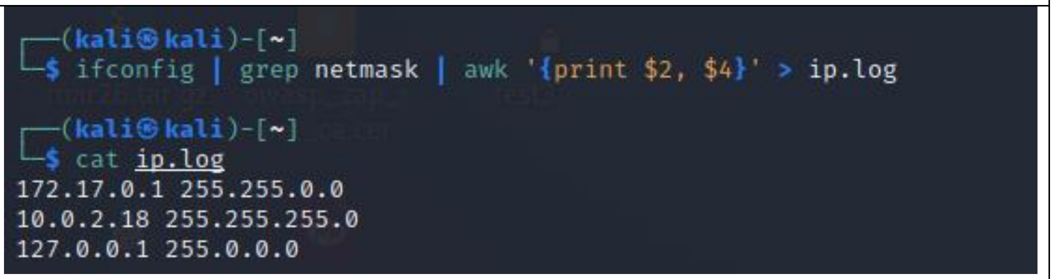
```
┌──(kali㉿kali)-[~]
└─$ ifconfig | grep netmask
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet 10.0.2.18  netmask 255.255.255.0  broadcast 10.0.2.255
        inet 127.0.0.1  netmask 255.0.0.0
```

</td>
</tr>
<tr>
<td></td>
<td>



```
┌──(kali㉿kali)-[~]
└─$ ifconfig | grep netmask | awk '{print $2, $4}'
172.17.0.1 255.255.0.0
10.0.2.18 255.255.255.0
127.0.0.1 255.0.0.0
```

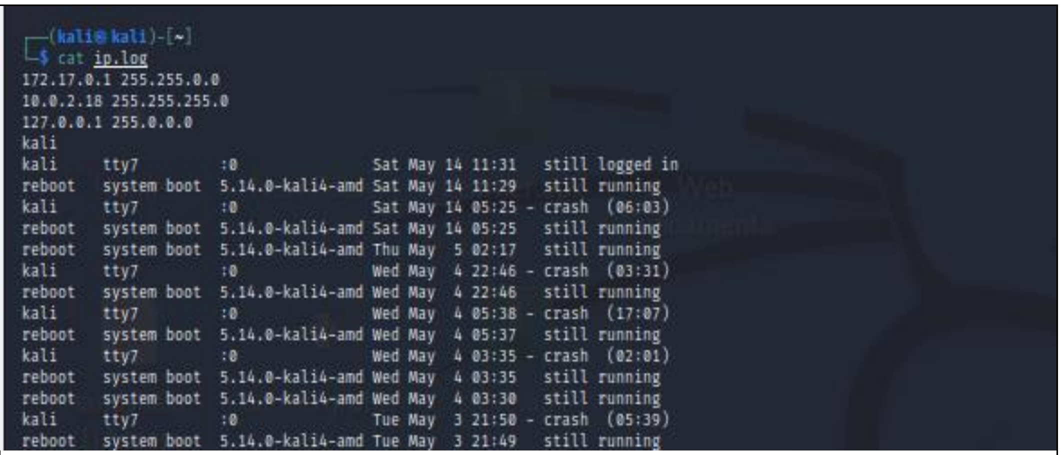
</td>
</tr>
<tr>
<td></td>
<td>



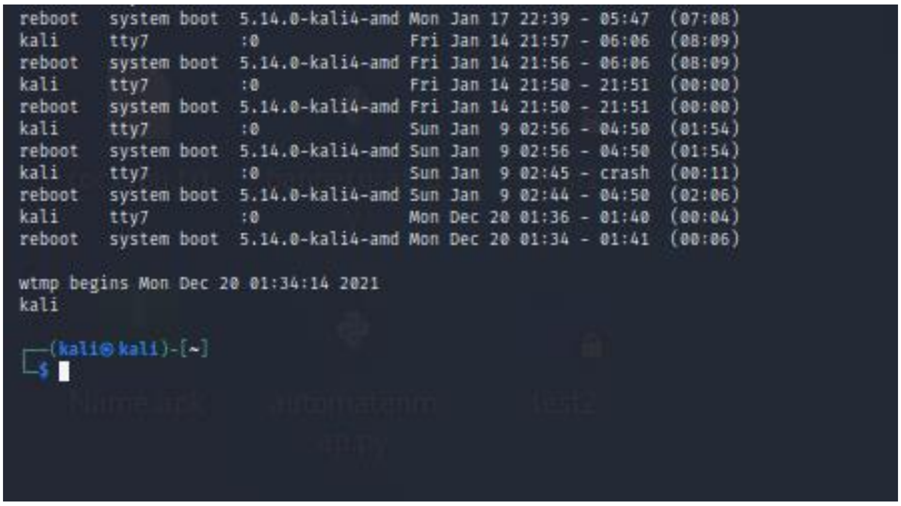
```
┌──(kali㉿kali)-[~]
└─$ ifconfig | grep netmask | awk '{print $2, $4}' > ip.log

┌──(kali㉿kali)-[~]
└─$ cat ip.log
172.17.0.1 255.255.0.0
10.0.2.18 255.255.255.0
127.0.0.1 255.0.0.0
```

</td>
</tr>
</table>

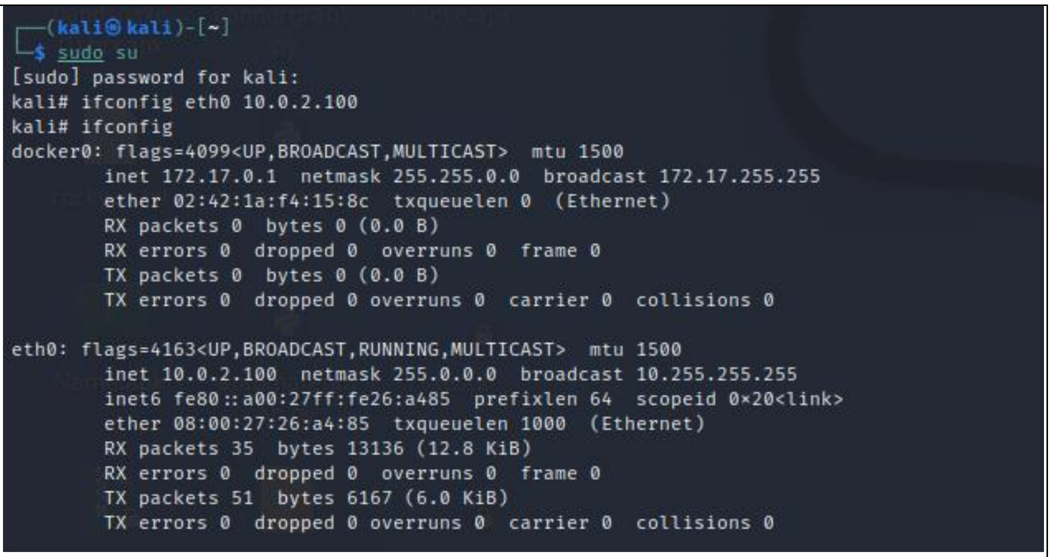
Append whomai, last, hostname



```
┌──(kali㉿kali)-[~]
└─$ cat ip.log
172.17.0.1 255.255.0.0
10.0.2.18 255.255.255.0
127.0.0.1 255.0.0.0
kali
kali     tty7         :0               Sat May 14 11:31   still logged in
reboot   system boot  5.14.0-kali4-amd Sat May 14 11:29   still running
kali     tty7         :0               Sat May 14 05:25 - crash  (06:03)
reboot   system boot  5.14.0-kali4-amd Sat May 14 05:25   still running
reboot   system boot  5.14.0-kali4-amd Thu May  5 02:17   still running
kali     tty7         :0               Wed May  4 22:46 - crash  (03:31)
reboot   system boot  5.14.0-kali4-amd Wed May  4 22:46   still running
kali     tty7         :0               Wed May  4 05:38 - crash  (17:07)
reboot   system boot  5.14.0-kali4-amd Wed May  4 05:37   still running
kali     tty7         :0               Wed May  4 03:35 - crash  (02:01)
reboot   system boot  5.14.0-kali4-amd Wed May  4 03:35   still running
reboot   system boot  5.14.0-kali4-amd Wed May  4 03:30   still running
kali     tty7         :0               Tue May  3 21:50 - crash  (05:39)
reboot   system boot  5.14.0-kali4-amd Tue May  3 21:49   still running
```



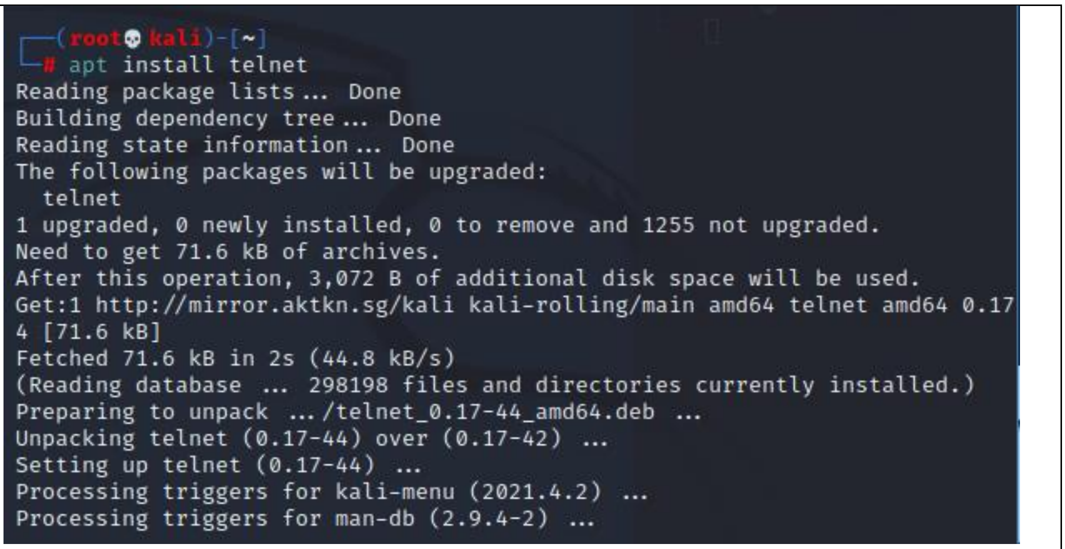
```
reboot   system boot  5.14.0-kali4-amd Mon Jan 17 22:39 - 05:47  (07:08)
kali     tty7         :0               Fri Jan 14 21:57 - 06:06  (08:09)
reboot   system boot  5.14.0-kali4-amd Fri Jan 14 21:56 - 06:06  (08:09)
kali     tty7         :0               Fri Jan 14 21:50 - 21:51  (00:00)
reboot   system boot  5.14.0-kali4-amd Fri Jan 14 21:50 - 21:51  (00:00)
kali     tty7         :0               Sun Jan  9 02:56 - 04:50  (01:54)
reboot   system boot  5.14.0-kali4-amd Sun Jan  9 02:56 - 04:50  (01:54)
kali     tty7         :0               Sun Jan  9 02:45 - crash  (00:11)
reboot   system boot  5.14.0-kali4-amd Sun Jan  9 02:44 - 04:50  (02:06)
kali     tty7         :0               Mon Dec 20 01:36 - 01:40  (00:04)
reboot   system boot  5.14.0-kali4-amd Mon Dec 20 01:34 - 01:41  (00:06)

wtmp begins Mon Dec 20 01:34:14 2021
kali

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
kali# ifconfig eth0 10.0.2.100
kali# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:1a:f4:15:8c  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.100  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::a00:27ff:fe26:a485  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:26:a4:85  txqueuelen 1000  (Ethernet)
        RX packets 35  bytes 13136 (12.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 51  bytes 6167 (6.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

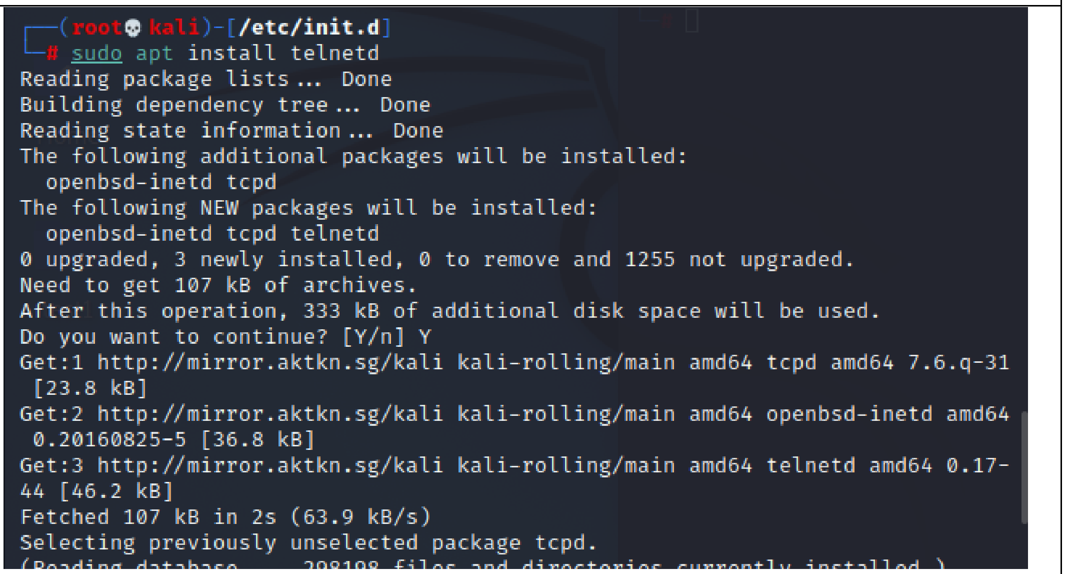
Part 8: Remote Control and Telnet Services

<table>
<tr>
<td>Install telnet</td>
<td>



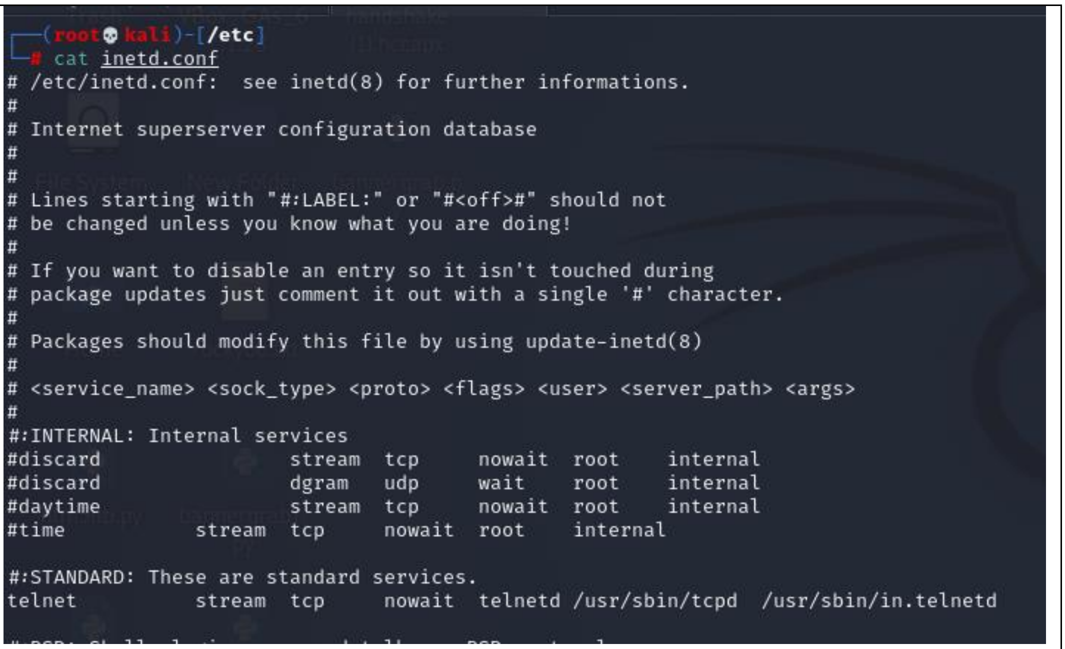
```
┌──(root💀kali)-[~]
└─# apt install telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  telnet
1 upgraded, 0 newly installed, 0 to remove and 1255 not upgraded.
Need to get 71.6 kB of archives.
After this operation, 3,072 B of additional disk space will be used.
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 telnet amd64 0.17-
4 [71.6 kB]
Fetched 71.6 kB in 2s (44.8 kB/s)
(Reading database ... 298198 files and directories currently installed.)
Preparing to unpack .../telnet_0.17-44_amd64.deb ...
Unpacking telnet (0.17-44) over (0.17-42) ...
Setting up telnet (0.17-44) ...
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for man-db (2.9.4-2) ...
```

</td>
</tr>
<tr>
<td>telnetd</td>
<td>

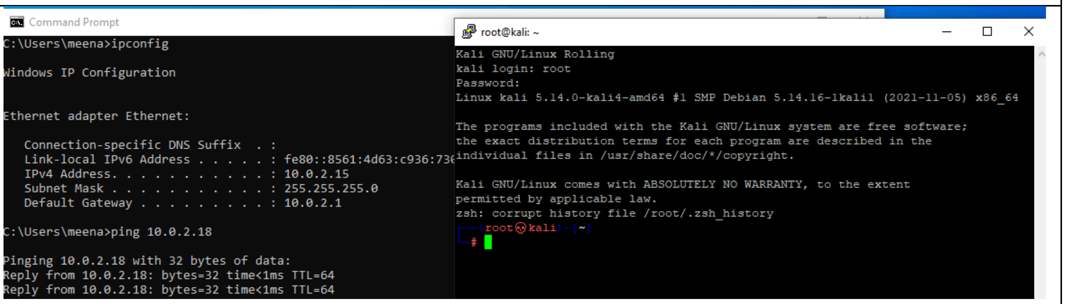


```
┌──(root💀kali)-[/etc/init.d]
└─# sudo apt install telnetd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  openbsd-inetd tcpd
The following NEW packages will be installed:
  openbsd-inetd tcpd telnetd
0 upgraded, 3 newly installed, 0 to remove and 1255 not upgraded.
Need to get 107 kB of archives.
After this operation, 333 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 tcpd amd64 7.6.q-31
 [23.8 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 openbsd-inetd amd64
 0.20160825-5 [36.8 kB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 telnetd amd64 0.17-
44 [46.2 kB]
Fetched 107 kB in 2s (63.9 kB/s)
Selecting previously unselected package tcpd.
(Reading database ... 298198 files and directories currently installed.)
```

</td>
</tr>
<tr>
<td></td>
<td>Telnet is the command installed. Telnetd is the service installed. But it is configured to start from inetd, a daemon which manages telnet and other services. The inetd listens for connections and when a connection is found , it decides the service the socket corresponds to and invokes the program to service the request.</td>
</tr>
</table>



```
┌──(root💀kali)-[/etc]
└─# cat inetd.conf
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet superserver configuration database
#
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#discard                stream  tcp     nowait  root    internal
#discard                dgram   udp     wait    root    internal
#daytime                stream  tcp     nowait  root    internal
#time           stream  tcp     nowait  root    internal

#:STANDARD: These are standard services.
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
```

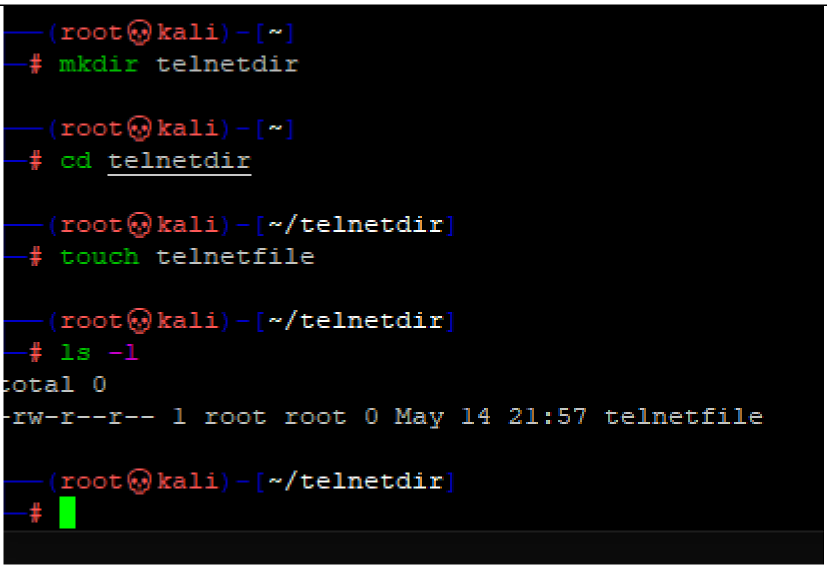


Command Prompt

```
C:\Users\meena>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8561:4d63:c936:73
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

C:\Users\meena>ping 10.0.2.18

Pinging 10.0.2.18 with 32 bytes of data:
Reply from 10.0.2.18: bytes=32 time<1ms TTL=64
Reply from 10.0.2.18: bytes=32 time<1ms TTL=64
```

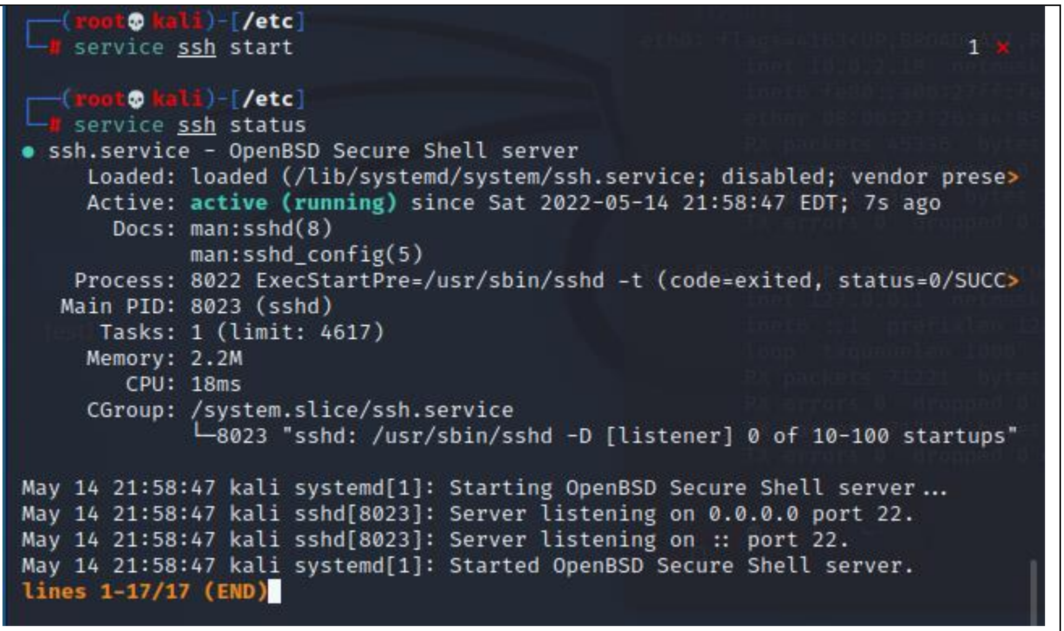
root@kali: ~

```
Kali GNU/Linux Rolling
kali login: root
Password:
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali)-[~]
└─#
```

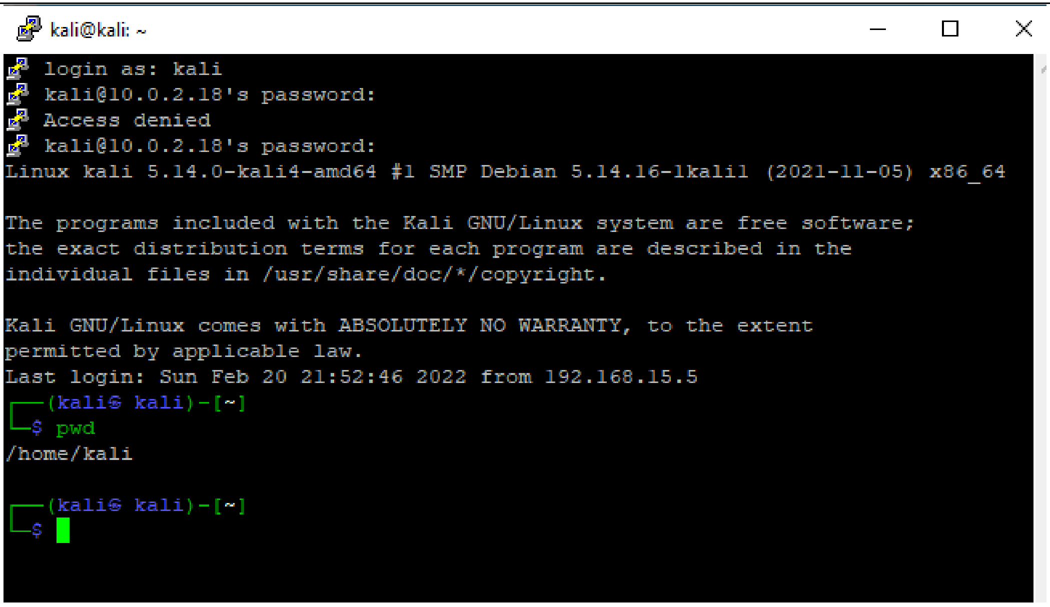


```
┌──(root💀kali)-[~]
└─# mkdir telnetdir

┌──(root💀kali)-[~]
└─# cd telnetdir

┌──(root💀kali)-[~/telnetdir]
└─# touch telnetfile

┌──(root💀kali)-[~/telnetdir]
└─# ls -l
total 0
-rw-r--r-- 1 root root 0 May 14 21:57 telnetfile

┌──(root💀kali)-[~/telnetdir]
└─#
```

Part 9: SSH Connection

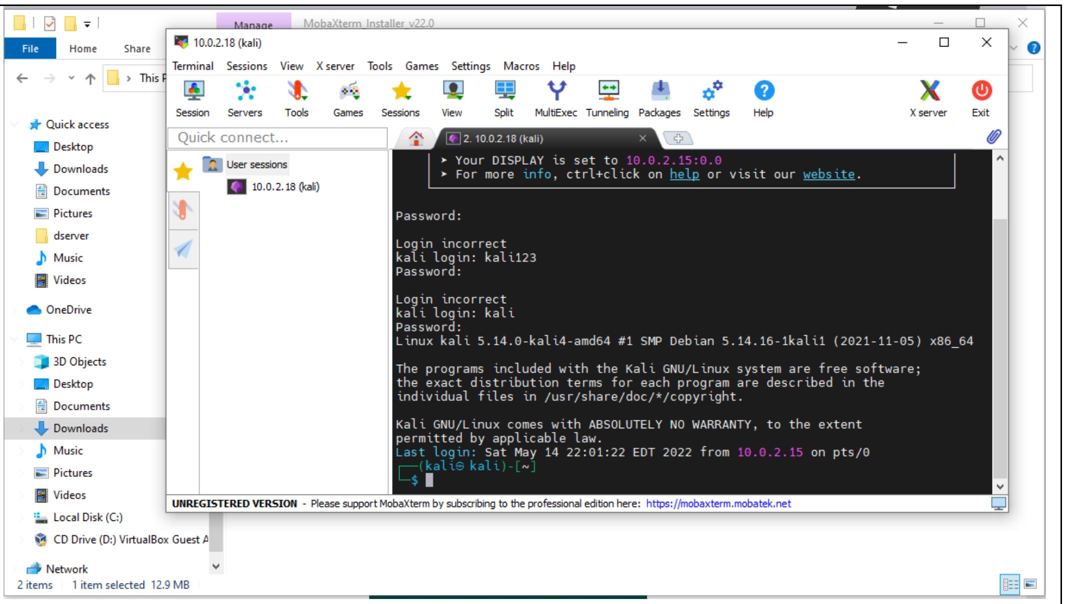


```
┌──(root💀kali)-[/etc]
└─# service ssh start                                              1 ×

┌──(root💀kali)-[/etc]
└─# service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor prese>
     Active: active (running) since Sat 2022-05-14 21:58:47 EDT; 7s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 8022 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCC>
   Main PID: 8023 (sshd)
      Tasks: 1 (limit: 4617)
     Memory: 2.2M
        CPU: 18ms
     CGroup: /system.slice/ssh.service
             └─8023 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 14 21:58:47 kali systemd[1]: Starting OpenBSD Secure Shell server...
May 14 21:58:47 kali sshd[8023]: Server listening on 0.0.0.0 port 22.
May 14 21:58:47 kali sshd[8023]: Server listening on :: port 22.
May 14 21:58:47 kali systemd[1]: Started OpenBSD Secure Shell server.
lines 1-17/17 (END)
```



```
login as: kali
kali@10.0.2.18's password:
Access denied
kali@10.0.2.18's password:
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb 20 21:52:46 2022 from 192.168.15.5
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$
```

<table>
<tr>
<td></td>
<td>

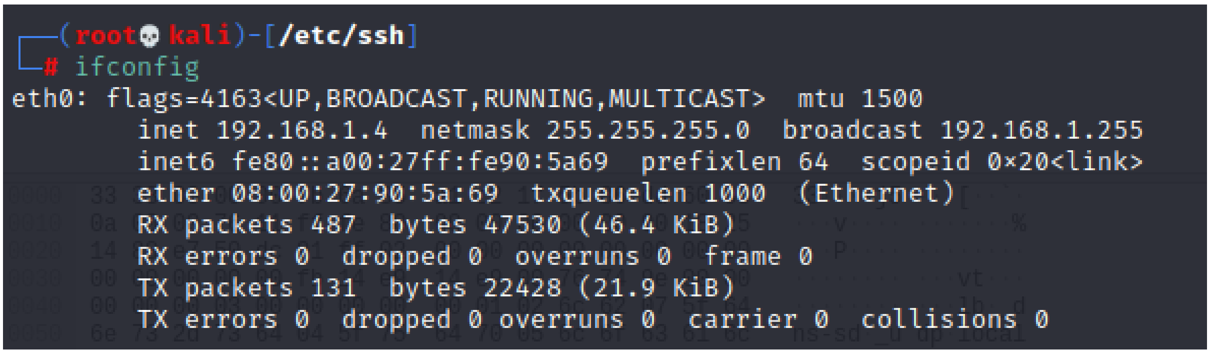


```
 ➤ Your DISPLAY is set to 10.0.2.15:0.0
 ➤ For more info, ctrl+click on help or visit our website.

Password:

Login incorrect
kali login: kali123
Password:

Login incorrect
kali login: kali
Password:
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 14 22:01:22 EDT 2022 from 10.0.2.15 on pts/0
┌──(kali㉿kali)-[~]
└─$ 
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

</td>
</tr>
<tr>
<td>Connect to kali from phone</td>
<td>Install iTerminal in IPhone from Appstore. Plugin Iphone to the host.
Keep kali VM in bridged network

Run the app in the iphone</td>
</tr>
</table>

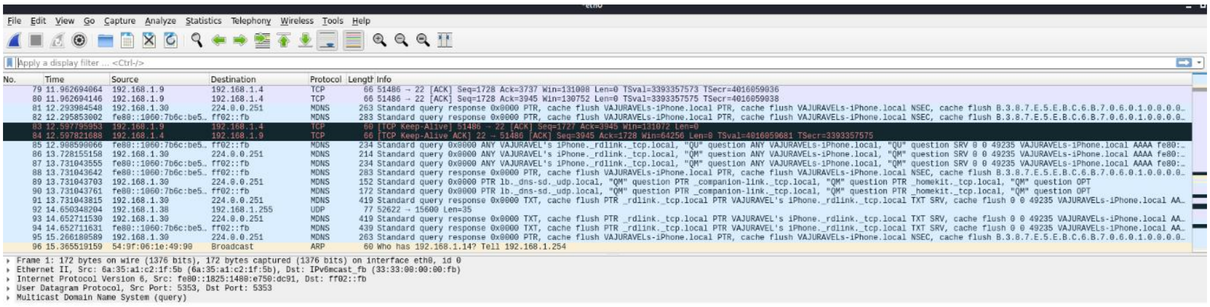


```
┌──(root💀kali)-[/etc/ssh]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.4  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe90:5a69  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:90:5a:69  txqueuelen 1000  (Ethernet)
        RX packets 487  bytes 47530 (46.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 131  bytes 22428 (21.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

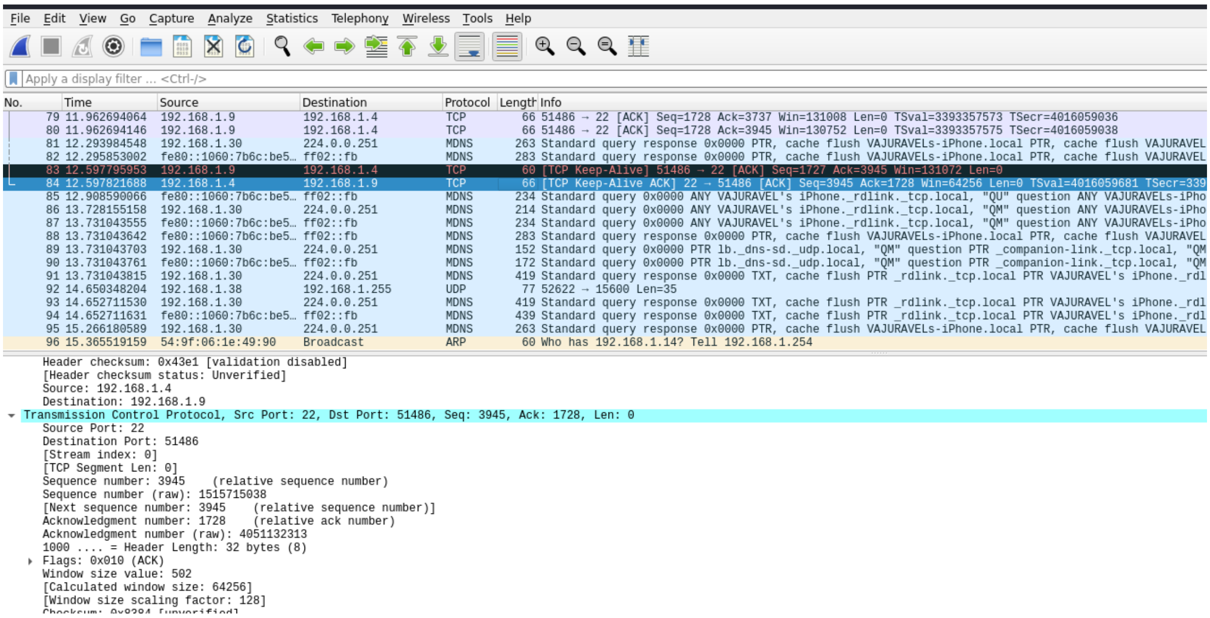
Iphone Ip: 192.168.1.9

Enter the ip of kali . user name testing2 and password in the iTerminal App in the Iphone

The ssh session is established


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

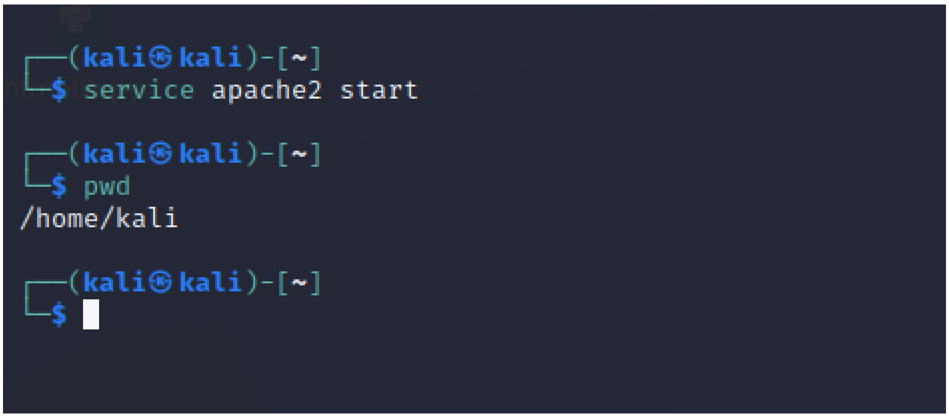
```
No.   Time          Source                Destination      Protocol Length Info
   79 11.962694064 192.168.1.9           192.168.1.4      TCP       66 51486 → 22 [ACK] Seq=1728 Ack=3737 Win=131008 Len=0 TSval=3393357573 TSecr=4016059036
   80 11.962694146 192.168.1.9           192.168.1.4      TCP       66 51486 → 22 [ACK] Seq=1728 Ack=3945 Win=130752 Len=0 TSval=3393357575 TSecr=4016059038
   81 12.293984548 192.168.1.30          224.0.0.251      MDNS     263 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVELs-iPhone.local NSEC, cache flush B.3.8.7.E.5.E.B.C.6.B.7.0.6.0.1.0.0.0.0…
   82 12.295853002 fe80::1060:7b6c:be5… ff02::fb         MDNS     283 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVELs-iPhone.local NSEC, cache flush B.3.8.7.E.5.E.B.C.6.B.7.0.6.0.1.0.0.0.0…
   83 12.597795953 192.168.1.9           192.168.1.4      TCP       60 [TCP Keep-Alive] 51486 → 22 [ACK] Seq=1727 Ack=3945 Win=131072 Len=0
   84 12.597821688 192.168.1.4           192.168.1.9      TCP       66 [TCP Keep-Alive ACK] 22 → 51486 [ACK] Seq=3945 Ack=1728 Win=64256 Len=0 TSval=4016059681 TSecr=3393357575
   85 12.908590066 fe80::1060:7b6c:be5… ff02::fb         MDNS     234 Standard query 0x0000 ANY VAJURAVEL's iPhone._rdlink._tcp.local, "QU" question ANY VAJURAVELs-iPhone.local, "QU" question SRV 0 0 49235 VAJURAVELs-iPhone.local AAAA fe80:…
   86 13.728155158 192.168.1.30          224.0.0.251      MDNS     214 Standard query 0x0000 ANY VAJURAVEL's iPhone._rdlink._tcp.local, "QM" question ANY VAJURAVELs-iPhone.local, "QM" question SRV 0 0 49235 VAJURAVELs-iPhone.local AAAA fe80:…
   87 13.731043555 fe80::1060:7b6c:be5… ff02::fb         MDNS     234 Standard query 0x0000 ANY VAJURAVEL's iPhone._rdlink._tcp.local, "QM" question ANY VAJURAVELs-iPhone.local, "QM" question SRV 0 0 49235 VAJURAVELs-iPhone.local AAAA fe80:…
   88 13.731043642 fe80::1060:7b6c:be5… ff02::fb         MDNS     283 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVELs-iPhone.local NSEC, cache flush B.3.8.7.E.5.E.B.C.6.B.7.0.6.0.1.0.0.0.0…
   89 13.731043703 192.168.1.30          224.0.0.251      MDNS     152 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question OPT
   90 13.731043761 fe80::1060:7b6c:be5… ff02::fb         MDNS     172 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question OPT
   91 13.731043815 192.168.1.30          224.0.0.251      MDNS     419 Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR VAJURAVEL's iPhone._rdlink._tcp.local TXT SRV, cache flush 0 0 49235 VAJURAVELs-iPhone.local AA…
   92 14.650348204 192.168.1.38          192.168.1.255    UDP       77 52622 → 15600 Len=35
   93 14.652711530 192.168.1.30          224.0.0.251      MDNS     419 Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR VAJURAVEL's iPhone._rdlink._tcp.local TXT SRV, cache flush 0 0 49235 VAJURAVELs-iPhone.local AA…
   94 14.652711631 fe80::1060:7b6c:be5… ff02::fb         MDNS     439 Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR VAJURAVEL's iPhone._rdlink._tcp.local TXT SRV, cache flush 0 0 49235 VAJURAVELs-iPhone.local AA…
   95 15.266180589 192.168.1.30          224.0.0.251      MDNS     263 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVELs-iPhone.local NSEC, cache flush B.3.8.7.E.5.E.B.C.6.B.7.0.6.0.1.0.0.0.0…
   96 15.365519159 54:9f:06:1e:49:90     Broadcast        ARP       60 Who has 192.168.1.14? Tell 192.168.1.254

▸ Frame 1: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface eth0, id 0
▸ Ethernet II, Src: 6a:35:a1:c2:1f:5b (6a:35:a1:c2:1f:5b), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
▸ Internet Protocol Version 6, Src: fe80::1825:1480:e750:dc91, Dst: ff02::fb
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (query)
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

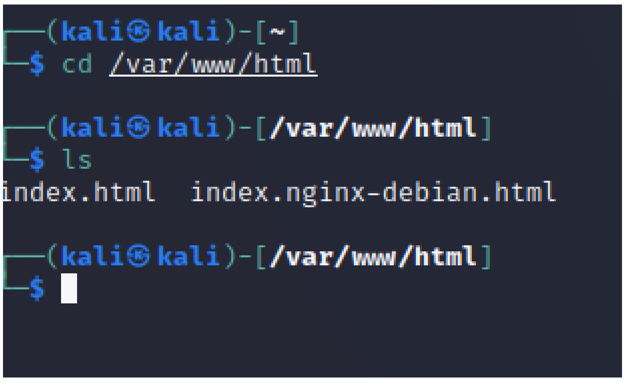
```
No.   Time          Source                Destination      Protocol Length Info
   79 11.962694064 192.168.1.9           192.168.1.4      TCP       66 51486 → 22 [ACK] Seq=1728 Ack=3737 Win=131008 Len=0 TSval=3393357573 TSecr=4016059036
   80 11.962694146 192.168.1.9           192.168.1.4      TCP       66 51486 → 22 [ACK] Seq=1728 Ack=3945 Win=130752 Len=0 TSval=3393357575 TSecr=4016059038
   81 12.293984548 192.168.1.30          224.0.0.251      MDNS     263 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVEL
   82 12.295853002 fe80::1060:7b6c:be5… ff02::fb         MDNS     283 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVEL
   83 12.597795953 192.168.1.9           192.168.1.4      TCP       60 [TCP Keep-Alive] 51486 → 22 [ACK] Seq=1727 Ack=3945 Win=131072 Len=0
   84 12.597821688 192.168.1.4           192.168.1.9      TCP       66 [TCP Keep-Alive ACK] 22 → 51486 [ACK] Seq=3945 Ack=1728 Win=64256 Len=0 TSval=4016059681 TSecr=339
   85 12.908590066 fe80::1060:7b6c:be5… ff02::fb         MDNS     234 Standard query 0x0000 ANY VAJURAVEL's iPhone._rdlink._tcp.local, "QU" question ANY VAJURAVELs-iPho
   86 13.728155158 192.168.1.30          224.0.0.251      MDNS     214 Standard query 0x0000 ANY VAJURAVEL's iPhone._rdlink._tcp.local, "QM" question ANY VAJURAVELs-iPho
   87 13.731043555 fe80::1060:7b6c:be5… ff02::fb         MDNS     234 Standard query 0x0000 ANY VAJURAVEL's iPhone._rdlink._tcp.local, "QM" question ANY VAJURAVELs-iPho
   88 13.731043642 fe80::1060:7b6c:be5… ff02::fb         MDNS     283 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVEL
   89 13.731043703 192.168.1.30          224.0.0.251      MDNS     152 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-link._tcp.local, "QM
   90 13.731043761 fe80::1060:7b6c:be5… ff02::fb         MDNS     172 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-link._tcp.local, "QM
   91 13.731043815 192.168.1.30          224.0.0.251      MDNS     419 Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR VAJURAVEL's iPhone._rdl
   92 14.650348204 192.168.1.38          192.168.1.255    UDP       77 52622 → 15600 Len=35
   93 14.652711530 192.168.1.30          224.0.0.251      MDNS     419 Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR VAJURAVEL's iPhone._rdl
   94 14.652711631 fe80::1060:7b6c:be5… ff02::fb         MDNS     439 Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR VAJURAVEL's iPhone._rdl
   95 15.266180589 192.168.1.30          224.0.0.251      MDNS     263 Standard query response 0x0000 PTR, cache flush VAJURAVELs-iPhone.local PTR, cache flush VAJURAVEL
   96 15.365519159 54:9f:06:1e:49:90     Broadcast        ARP       60 Who has 192.168.1.14? Tell 192.168.1.254

      Header checksum: 0x43e1 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.4
      Destination: 192.168.1.9
▾ Transmission Control Protocol, Src Port: 22, Dst Port: 51486, Seq: 3945, Ack: 1728, Len: 0
      Source Port: 22
      Destination Port: 51486
      [Stream index: 0]
      [TCP Segment Len: 0]
      Sequence number: 3945    (relative sequence number)
      Sequence number (raw): 1515715038
      [Next sequence number: 3945    (relative sequence number)]
      Acknowledgment number: 1728    (relative ack number)
      Acknowledgment number (raw): 4051132313
      1000 .... = Header Length: 32 bytes (8)
    ▸ Flags: 0x010 (ACK)
      Window size value: 502
      [Calculated window size: 64256]
      [Window size scaling factor: 128]
      Checksum: 0x8384 [unverified]
```

Captured traffic using wireshark

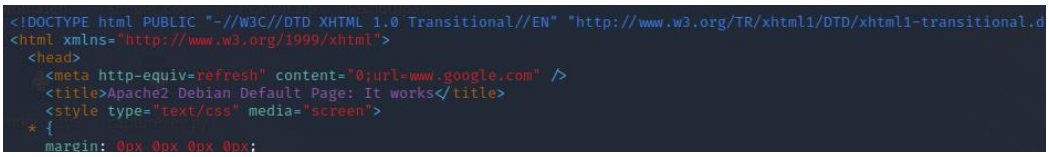
Part 10: Apache Webserver



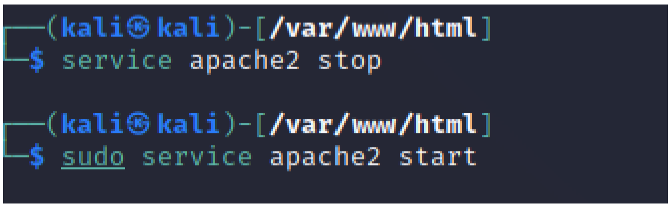
```
┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$ 
```



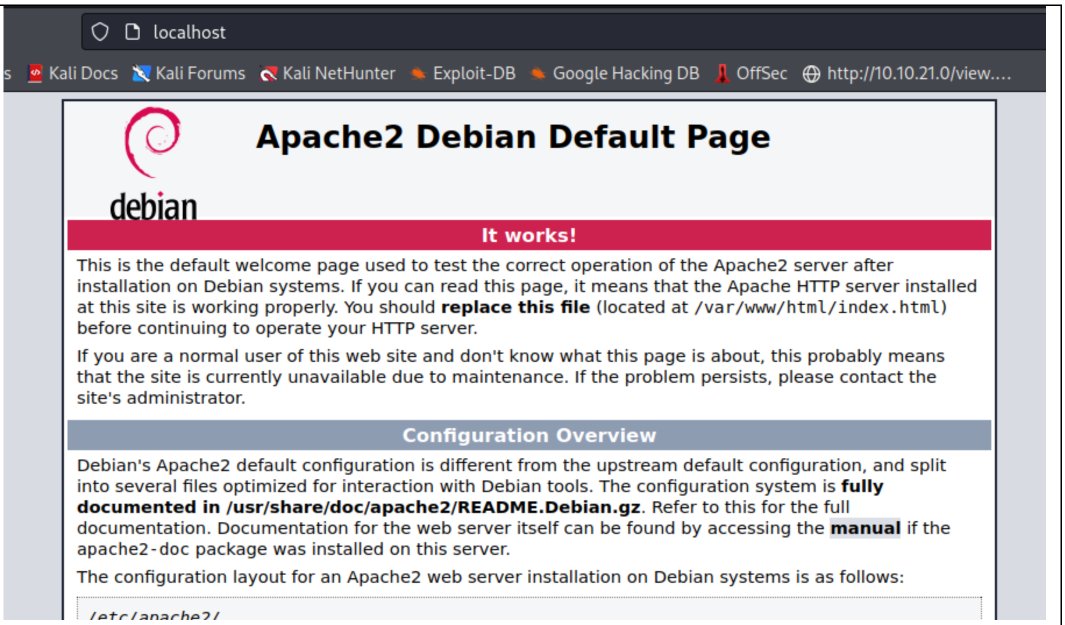
```
──(kali㉿kali)-[~]
─$ cd /var/www/html

──(kali㉿kali)-[/var/www/html]
─$ ls
index.html   index.nginx-debian.html

──(kali㉿kali)-[/var/www/html]
─$ 
```



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.d
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv=refresh" content="0;url=www.google.com" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
```



```
──(kali㉿kali)-[/var/www/html]
─$ service apache2 stop

──(kali㉿kali)-[/var/www/html]
─$ sudo service apache2 start
```



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

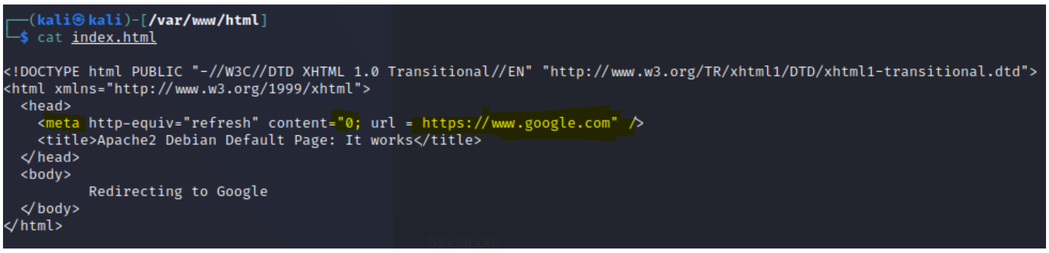
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

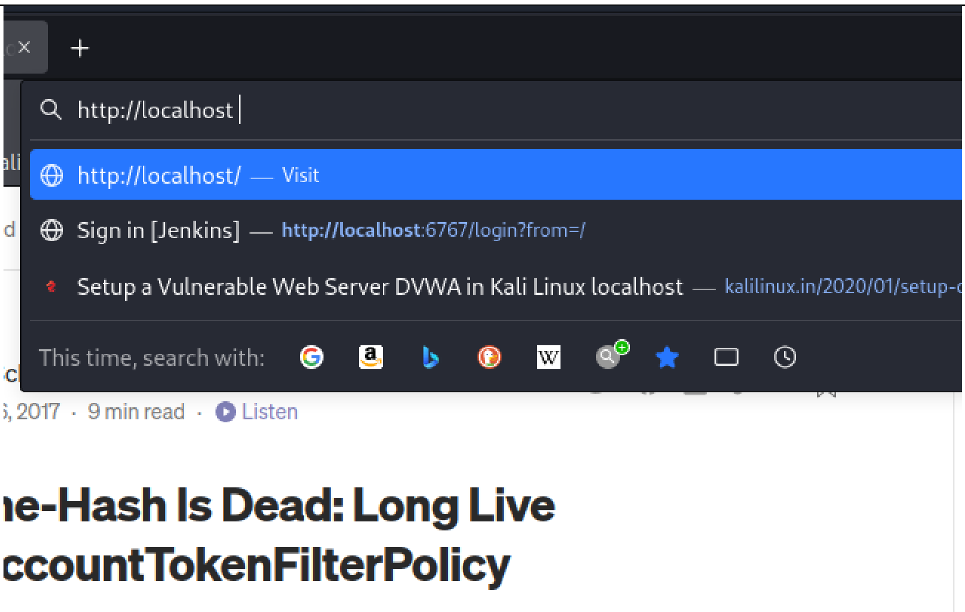
```
/etc/apache2/
```

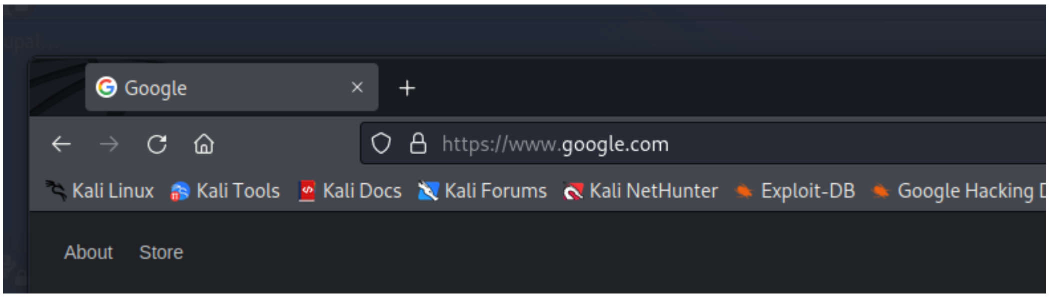
To redirect from one html to another page the <meta> tag is used. The URL is specified in the link attribute. The value in content attrinute is specified in seconds.



```
┌──(kali㉿kali)-[/var/www/html]
└─$ cat index.html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="refresh" content="0; url = https://www.google.com" />
    <title>Apache2 Debian Default Page: It works</title>
  </head>
  <body>
        Redirecting to Google
  </body>
</html>
```

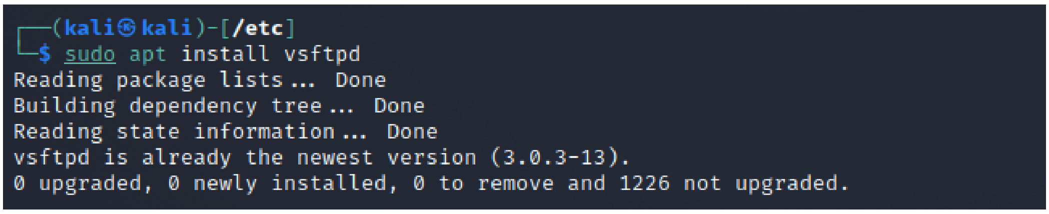
For the changes to take effect the apache server needs to stop /start


http://localhost
http://localhost/ — Visit
Sign in [Jenkins] — http://localhost:6767/login?from=/
Setup a Vulnerable Web Server DVWA in Kali Linux localhost — kalilinux.in/2020/01/setup-
This time, search with:
, 2017 · 9 min read · Listen
ne-Hash Is Dead: Long Live
ccountTokenFilterPolicy

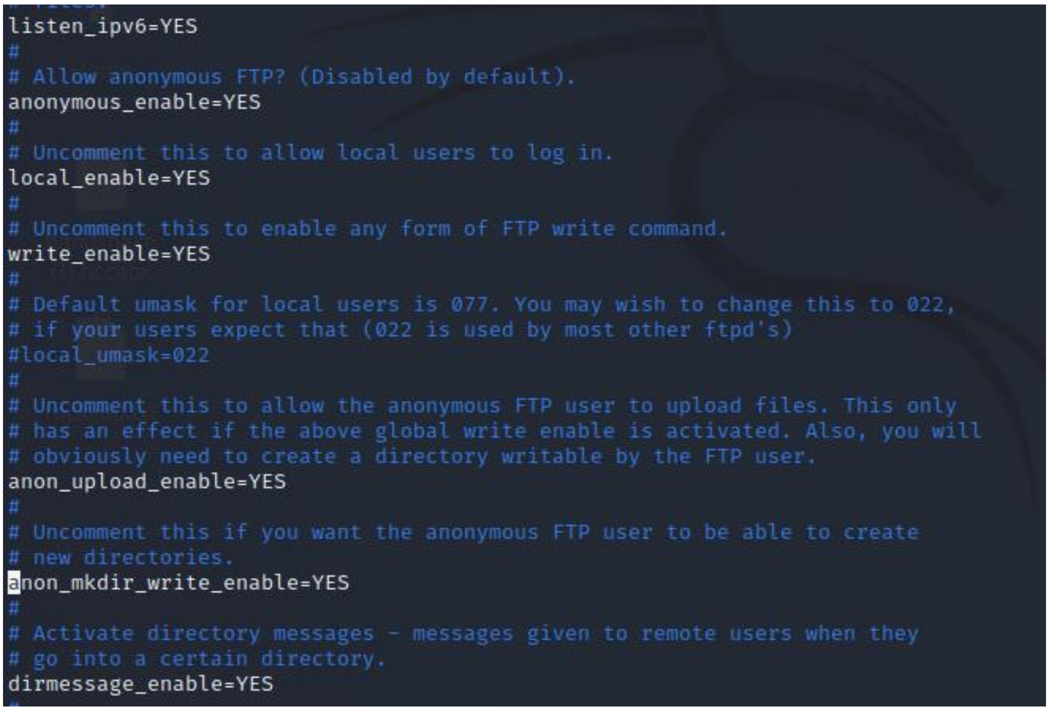
	

Google
https://www.google.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking D
About
Store

Part 11: VSFTPD

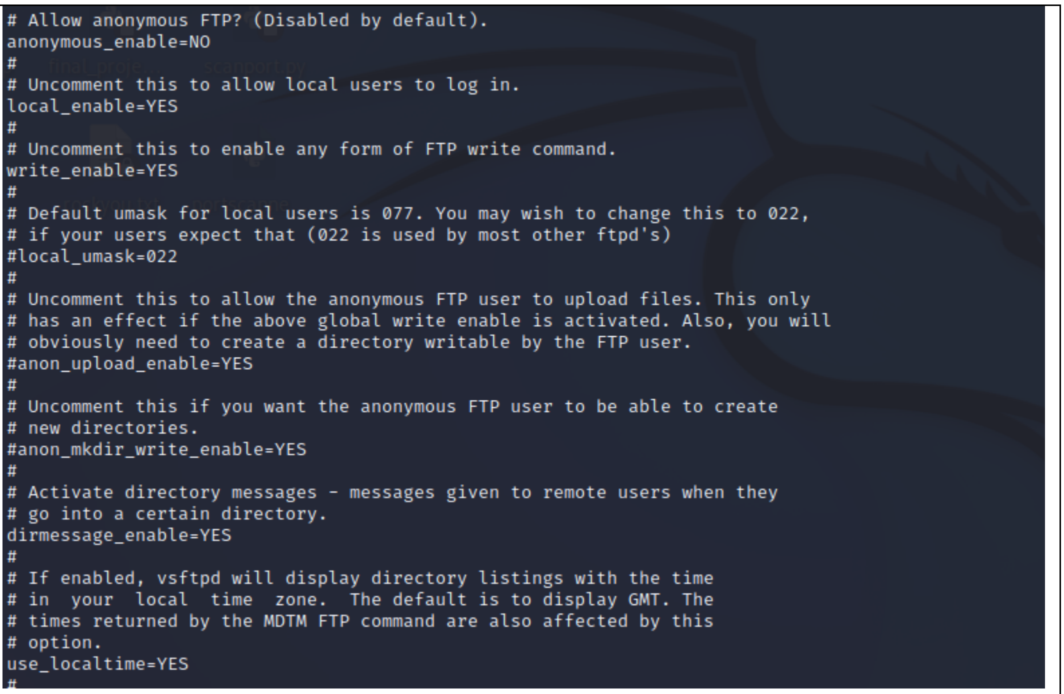


```
┌──(kali㉿kali)-[/etc]
└─$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13).
0 upgraded, 0 newly installed, 0 to remove and 1226 not upgraded.
```



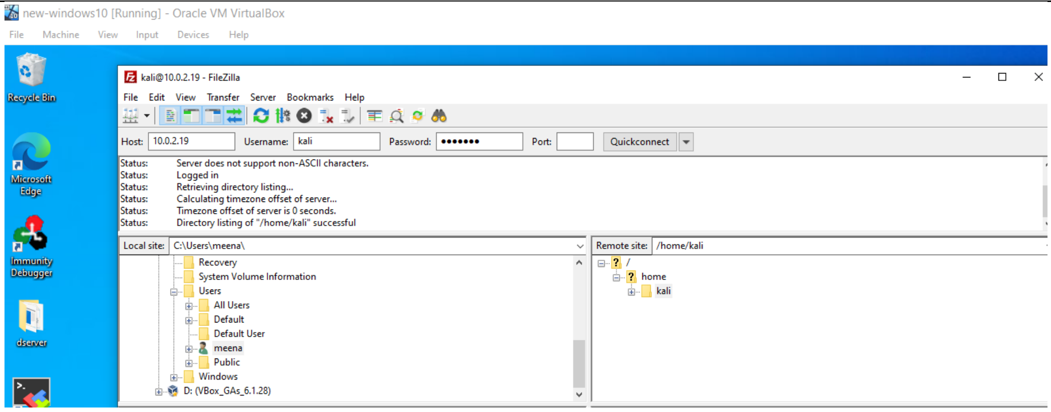
```
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
```

From windows



```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in  your  local  time  zone.  The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
```

Connect using Filezilla



new-windows10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
Immunity Debugger
dserver
kali@10.0.2.19 - FileZilla
File Edit View Transfer Server Bookmarks Help

Host: 10.0.2.19 Username: kali Password: ••••••• Port: Quickconnect

```
Status:    Server does not support non-ASCII characters.
Status:    Logged in
Status:    Retrieving directory listing...
Status:    Calculating timezone offset of server...
Status:    Timezone offset of server is 0 seconds.
Status:    Directory listing of "/home/kali" successful
```

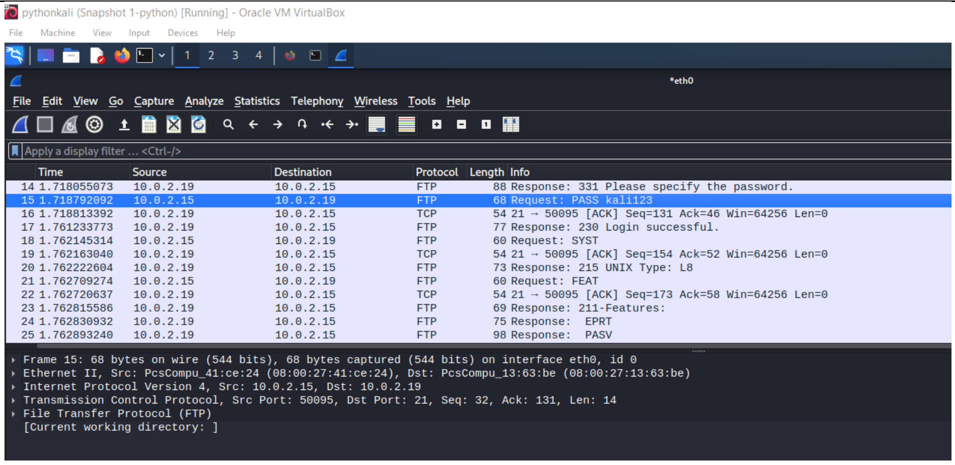
Local site: C:\Users\meena\

```
Recovery
System Volume Information
Users
  All Users
  Default
  Default User
  meena
  Public
Windows
D: (VBox_GAs_6.1.28)
```

Remote site: /home/kali

```
/
  home
    kali
```

Passwd captured using Filiezilla tramsfer

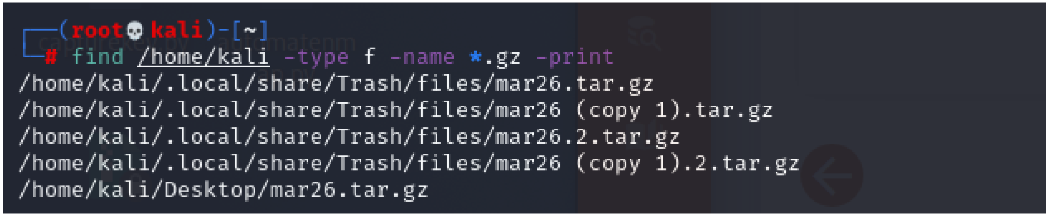
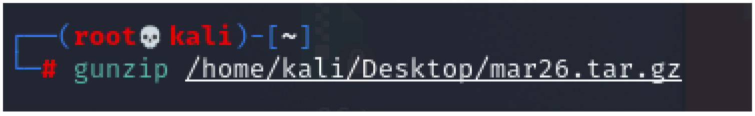
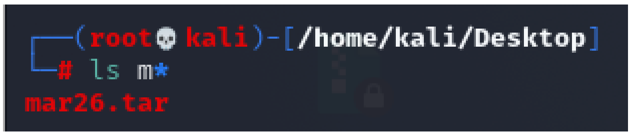
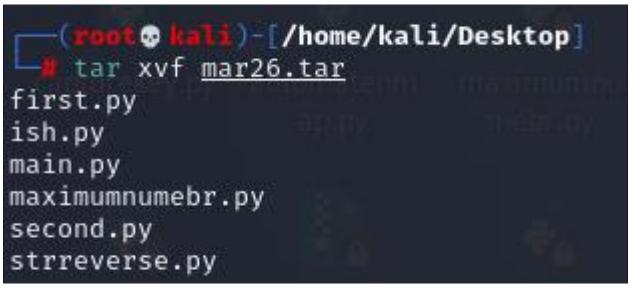


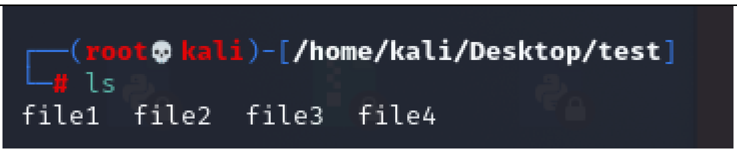
pythonkali (Snapshot 1-python) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

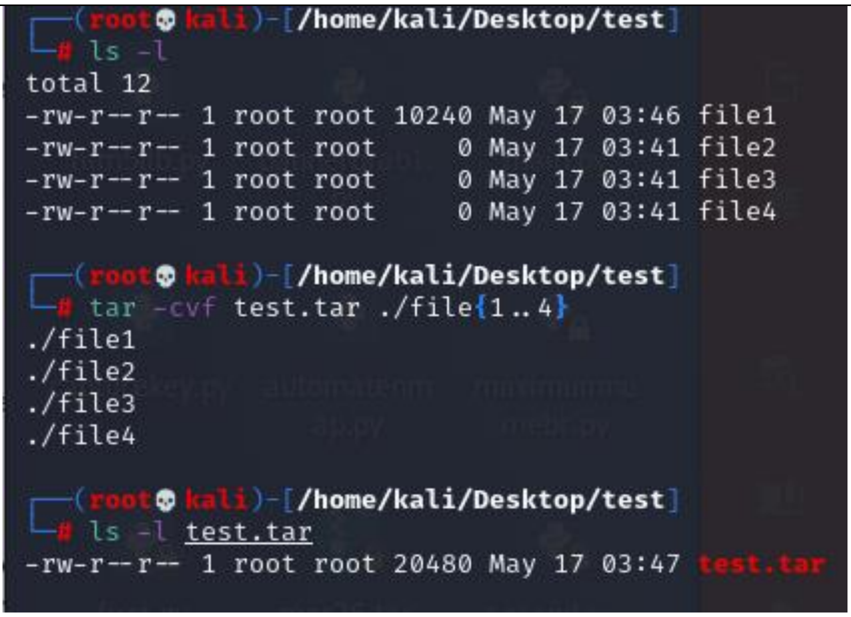
```
    Time          Source       Destination    Protocol  Length Info
 14 1.718055073   10.0.2.19    10.0.2.15      FTP       88 Response: 331 Please specify the password.
 15 1.718792092   10.0.2.15    10.0.2.19      FTP       68 Request: PASS kali123
 16 1.718813392   10.0.2.19    10.0.2.15      TCP       54 21 → 50095 [ACK] Seq=131 Ack=46 Win=64256 Len=0
 17 1.761233773   10.0.2.19    10.0.2.15      FTP       77 Response: 230 Login successful.
 18 1.762145314   10.0.2.15    10.0.2.19      FTP       60 Request: SYST
 19 1.762163040   10.0.2.19    10.0.2.15      TCP       54 21 → 50095 [ACK] Seq=154 Ack=52 Win=64256 Len=0
 20 1.762222604   10.0.2.19    10.0.2.15      FTP       73 Response: 215 UNIX Type: L8
 21 1.762709274   10.0.2.15    10.0.2.19      FTP       60 Request: FEAT
 22 1.762720637   10.0.2.19    10.0.2.15      TCP       54 21 → 50095 [ACK] Seq=173 Ack=58 Win=64256 Len=0
 23 1.762815586   10.0.2.19    10.0.2.15      FTP       69 Response: 211-Features:
 24 1.762830932   10.0.2.19    10.0.2.15      FTP       75 Response:  EPRT
 25 1.762893240   10.0.2.19    10.0.2.15      FTP       98 Response:  PASV

› Frame 15: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_41:ce:24 (08:00:27:41:ce:24), Dst: PcsCompu_13:63:be (08:00:27:13:63:be)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.19
› Transmission Control Protocol, Src Port: 50095, Dst Port: 21, Seq: 32, Ack: 131, Len: 14
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

Ftp protocol has security concerns as it sends password in clear text

Part 12: Gzip

Locate files with gz extension	Find command is used to locate gzip files under home/kali
	
	`┌──(root💀kali)-[~]`
	`└─# find /home/kali -type f -name *.gz -print`
	`/home/kali/.local/share/Trash/files/mar26.tar.gz`
	`/home/kali/.local/share/Trash/files/mar26 (copy 1).tar.gz`
	`/home/kali/.local/share/Trash/files/mar26.2.tar.gz`
	`/home/kali/.local/share/Trash/files/mar26 (copy 1).2.tar.gz`
	`/home/kali/Desktop/mar26.tar.gz`
	Mar26.tar.gz is chosen. Unzipping the files is donw using the gunzip
	
	`┌──(root💀kali)-[~]`
	`└─# gunzip /home/kali/Desktop/mar26.tar.gz`
	This gives a tar file
	
	`┌──(root💀kali)-[/home/kali/Desktop]`
	`└─# ls m*`
	`mar26.tar`
	
	`┌──(root💀kali)-[/home/kali/Desktop]`
	`└─# tar xvf mar26.tar`
	`first.py`
	`ish.py`
	`main.py`
	`maximumnumebr.py`
	`second.py`
	`strreverse.py`
	Tar xvf extracts the files from the tar file
	Can also use the tar -zxvf <file.gz>

Create four files and move them to a gzip file	
	`┌──(root💀kali)-[/home/kali/Desktop/test]`
	`└─# ls`
	`file1   file2   file3   file4`



```
┌──(root💀kali)-[/home/kali/Desktop/test]
└─# ls -l
total 12
-rw-r--r-- 1 root root 10240 May 17 03:46 file1
-rw-r--r-- 1 root root     0 May 17 03:41 file2
-rw-r--r-- 1 root root     0 May 17 03:41 file3
-rw-r--r-- 1 root root     0 May 17 03:41 file4

┌──(root💀kali)-[/home/kali/Desktop/test]
└─# tar -cvf test.tar ./file{1..4}
./file1
./file2
./file3
./file4

┌──(root💀kali)-[/home/kali/Desktop/test]
└─# ls -l test.tar
-rw-r--r-- 1 root root 20480 May 17 03:47 test.tar
```

Part 13: Questions

1. ***What are Root Folders?***

Folders present under the "/" are the root folders

/bin – is used to store essential user binaries and system programs

It contains programs that are essential for the system to boot and run

/etc – contains the configuration files

The configuration files present in /etc are applied system wide

User specific config files are present in the user home dir

/proc – contains special files that represent system and process information.

It is need for the kernel to run different process

2. ***Explain the following terms:***

Encoding:

Encoding is used to ensure data usability

Encoding is used to transform any data into a format using a scheme that is publicly available, so that it can be easily reversed. The data can be decoded using the same algorithm that was used to encode it.

The purpose of encoding is not to keep the data secret but to ensure that it is properly consumed by a different kind of system.

It can be defined as the process of applying a specific code, such as letters, symbols, and numbers, to data for conversion into an equivalent cipher.

Hashing:

Hashing is used to ensure integrity of data. If something is changed the user can find out that it has been changed

Hashing takes arbitrary input and produces a fixed length string.

The same input wll always produce the same output

It is not possible to reverse the output to the input

Any modification in the data input, will change the hash

Hashing is used along with authentication to ensure that the data is not tampered

Symmetric Encryption:

Encryption is done to transform data to ensure secrecy and that only the person using a secret key can reverse it. Helps to protect the Confidentiality of the data.

Symmetric Encryption: The same key/string is used on both sides for encryption/decryption

Asymmetric Encryption:

Involves using a pair of keys, the private and public key.

The data encrypted with the public key can only be decrypted with the corresponding private key.

The public key is given out to the other end who wants to receive the message.

This ensures the identity of both ends

3. *What is the usage of SSH? And Is SSH encrypted*

SSH is a cryptographic Network Protocol that operates with network services like telnet. It creates a secure connection in client server architecture, ensuring confidentiality and integrity through encryption

When installing SSH , the configuration file needs to be changed, Why?

The Config files:

Ssh_config (Client Side) and sshd_config (Server Config) are under /etc/ssh

The password or key is stored in the users .ssh folder

To connect to a ssh server, the server's config file needs some changes

The port to connect to, the password rules (authentication) , the user type

4. *Do you know another configuration file and in which service?*

A similar config file is used for ftp under /etc

/etc/vsftpd.conf

5. *What is Kernel?*

Kernel is the core of the Operating System.

It is used to establish connection between the devices and manages resources

The primary responsibilities of Kernel are

- Device management
- Memory Management
- Process Management
- Handling System Calls

6. What should be performed to create a connection between two virtual machines?

The two virtual machines should be in the same network

1. NAT Network (if no connection with host but need to reach internet)
2. Bridged Network (in the same network as host)
3. Internal Network (no internet and host connectivity)

7. What is ping

Ping is ICMP based command that uses icmp echo request /reply to determine if the target is alive or not

8. The Permission over files and Folders use either numeric or UGO representation.

The numbers 4,2,1 are representing the read, write and execute permissions.

Read → 4 , defines if a user can read the contents of the speficied file or folder

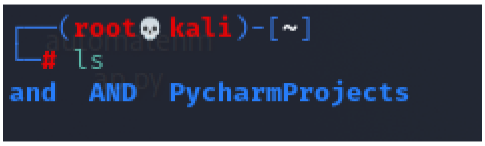
Write -> 2, defines if a user can modify a file

Execute->1 defines if a file can be executed by a user.

Also, it is necessary for a folder to have the execute permission without which it cannot be used

We specify them three times so that it is specified for the owner of the file , groups that owns and other users in the system.

9. Can we create two folders with the same name, lower and upper case?



```
┌──(root💀kali)-[~]
└─# ls
and   AND   PycharmProjects
```

Linux is case sensitive.

10.

Telnet	Application level protocol which provides CLI on a remote host.Typically used on Linux. And has security concerns
SSH	Application level protocol which provides CLI and command execution on a remote network device in a secure channel
Crontab	
FTP	A Application level, network protocol for transferring files between client and server. FTP is also not secure.
SFTP	Extension of SSH and provides secure file transfer between client and server over a network
Crontab	It is the equivalent of windows task scheduler It is a daemon suitable for servers. It allows task to be run in the background at regular intervals.
Gzip tar	Gzip is for compressing files and tar is for archiving files. They are commonly used together
bash	Born Again Shell. This is sh compatible shell and provides functional improvements over sh
Apache	Apache is a web server that process requests and serves web assets and content through HTTP