

## Lab 1 – Practice commands in Linux

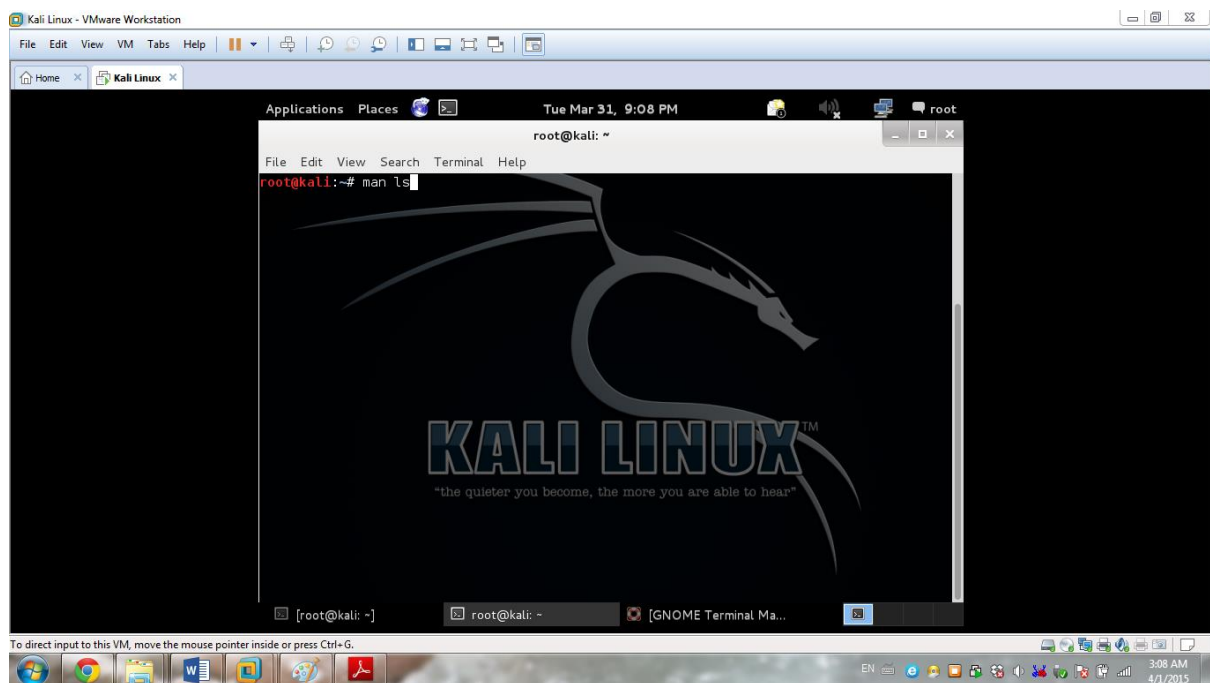
In this lab we will take a closer look at some basic commands in Linux. Please read and follow the instructions on your Kali machine.

### Kali Linux commands

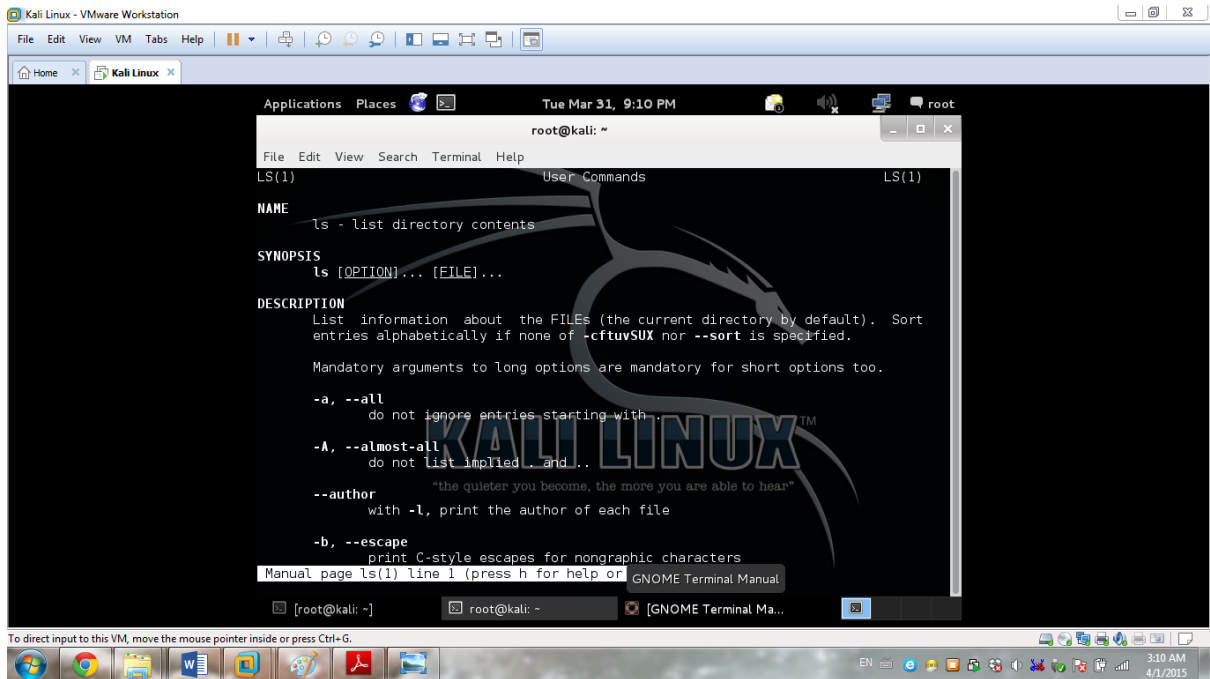
So let's start with some basic commands first. For better understanding we will divide the command on different categories, based on their field of usage. It is not expected to know all the commands by heart, that is why there is always manuals (included in Kali) –help commands, or if you have any troubles there are thousands of articles on the web that you can read about almost every issue that you might have.

Please note: all commands should be issued in small letters, capital letters will not be recognized.

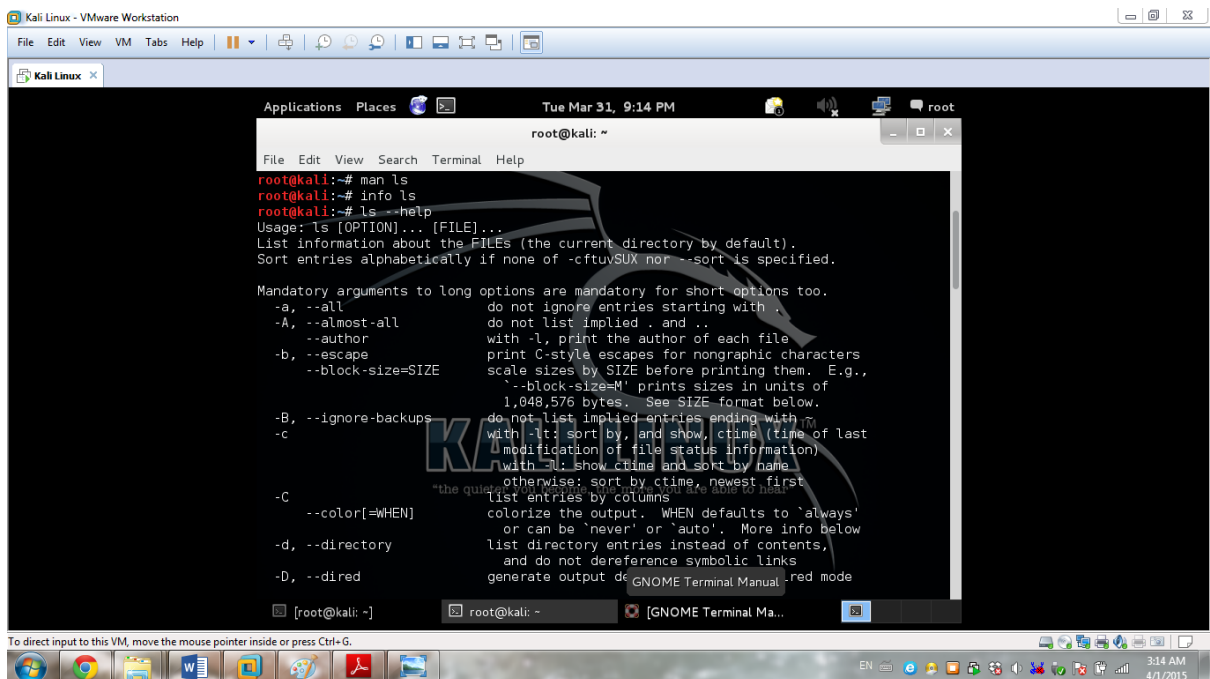
- Manual command – if you need help about a certain command type : man ,followed by the command ( man ls )



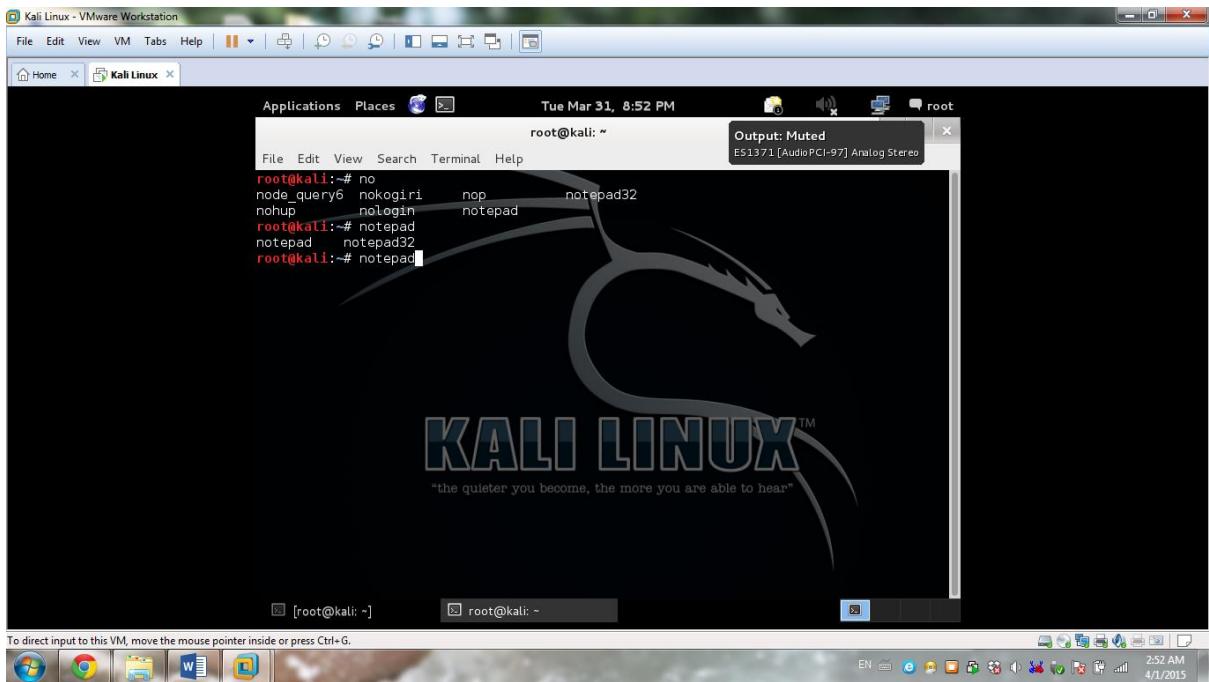
You will be presented with explanation of what this command is doing:



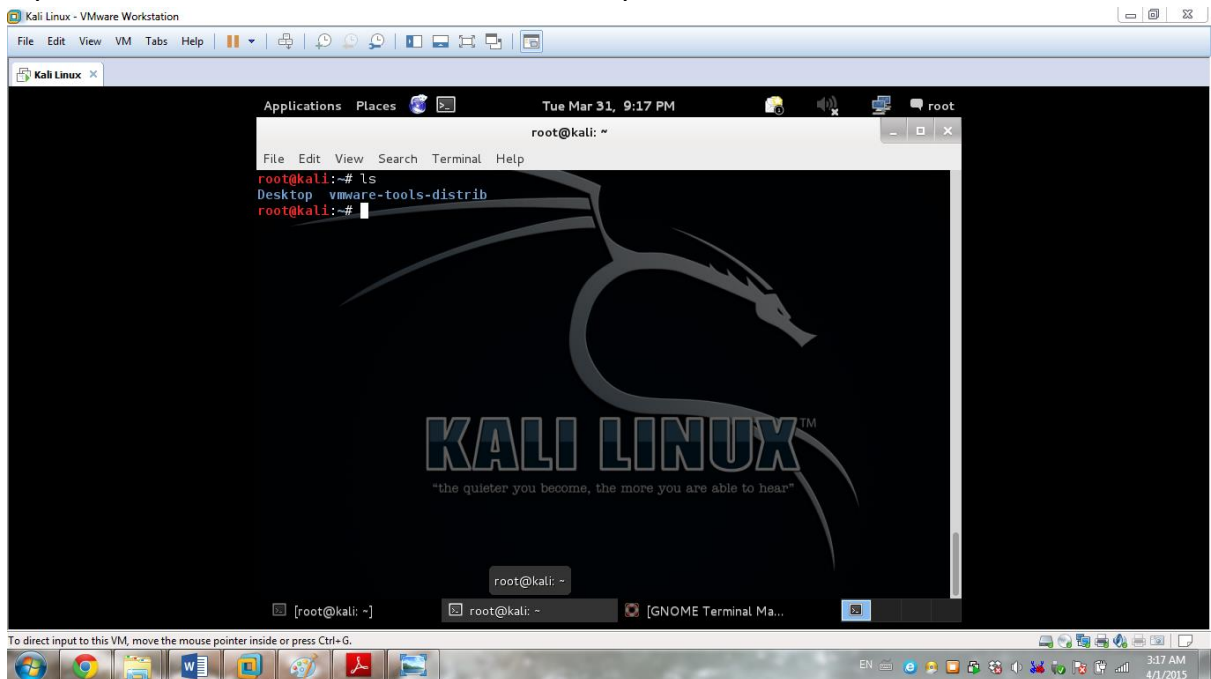
- Info command – more extended version of the Man command. Type in : “info ls”
- Help command – just type in : “ls—help”



- Command / filename completion – you don't have to type the full name of a file, just part of it, then press TAB. The filename completion will finish it for you. If I type in just : no “ and press TAB ,Kali will present me with a list of commands I can use:

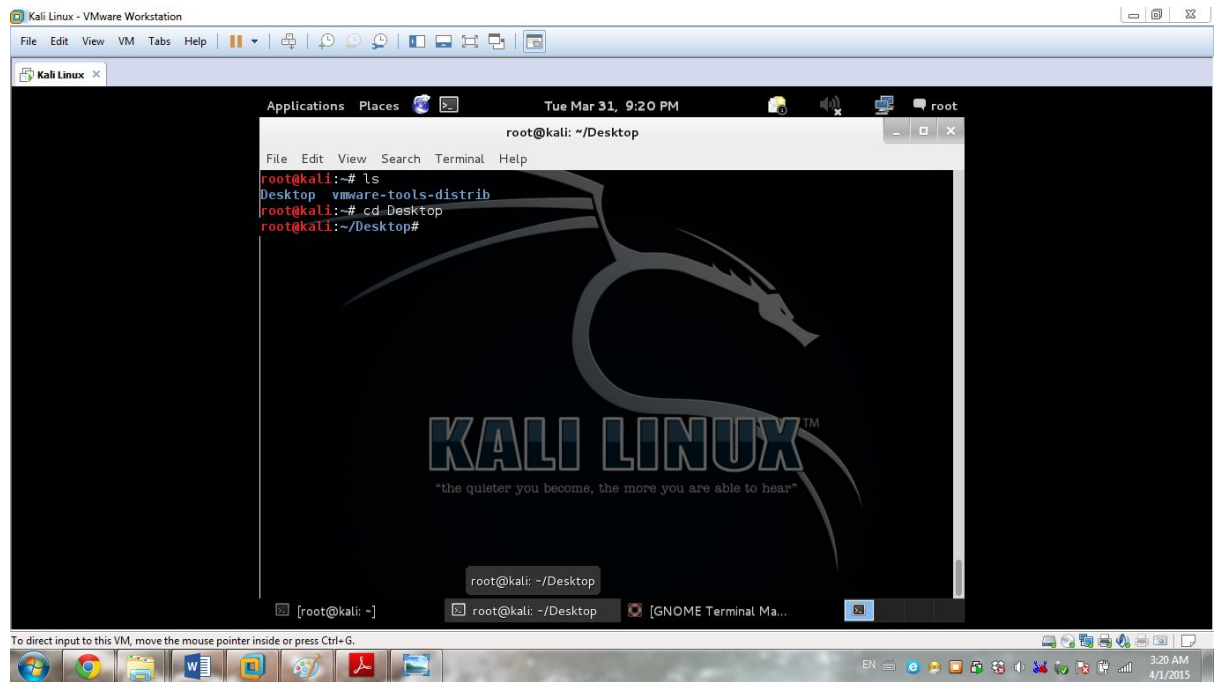


- Command History – recalls all the commands you type, usually the last 2000 commands. How to use it: Just press the UP ARROW KEY.
- Linux is case sensitive. Unlike DOS or Windows, commands like Password and password are considered to be different.
- If you would like to see all the files in a directory the command is : ls

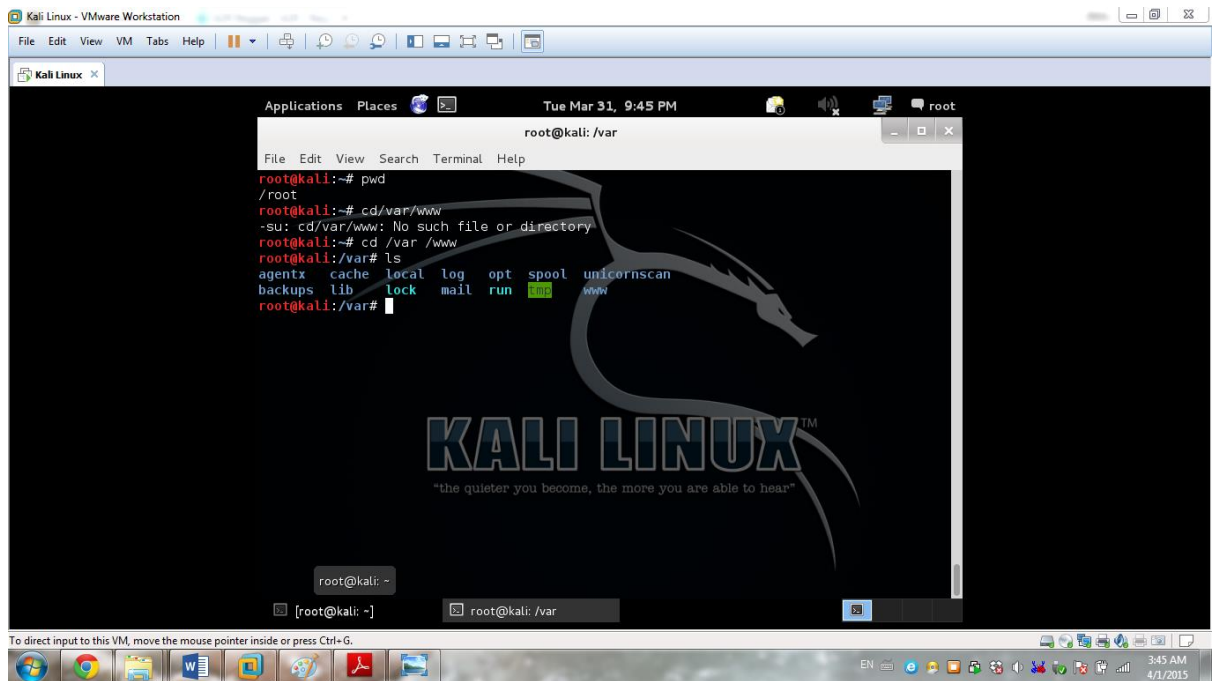


- Directories are in red color ,files are in white

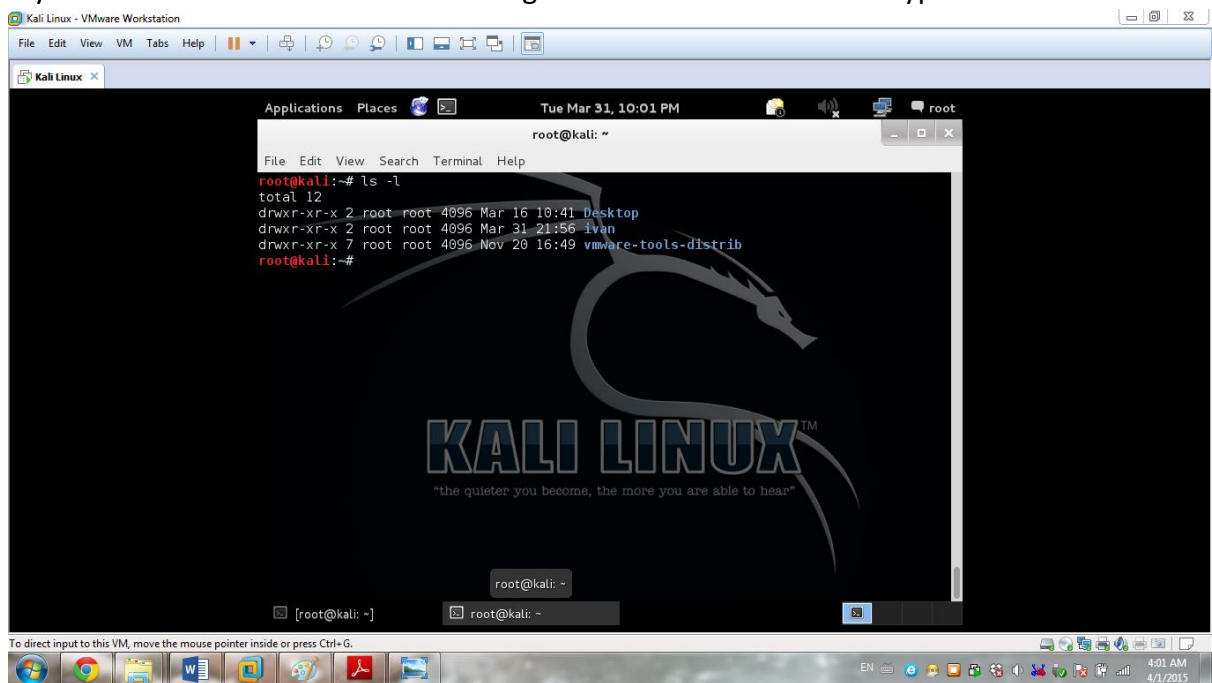
- If you would like to change the directory the command is : `cd` , followed by directory name:



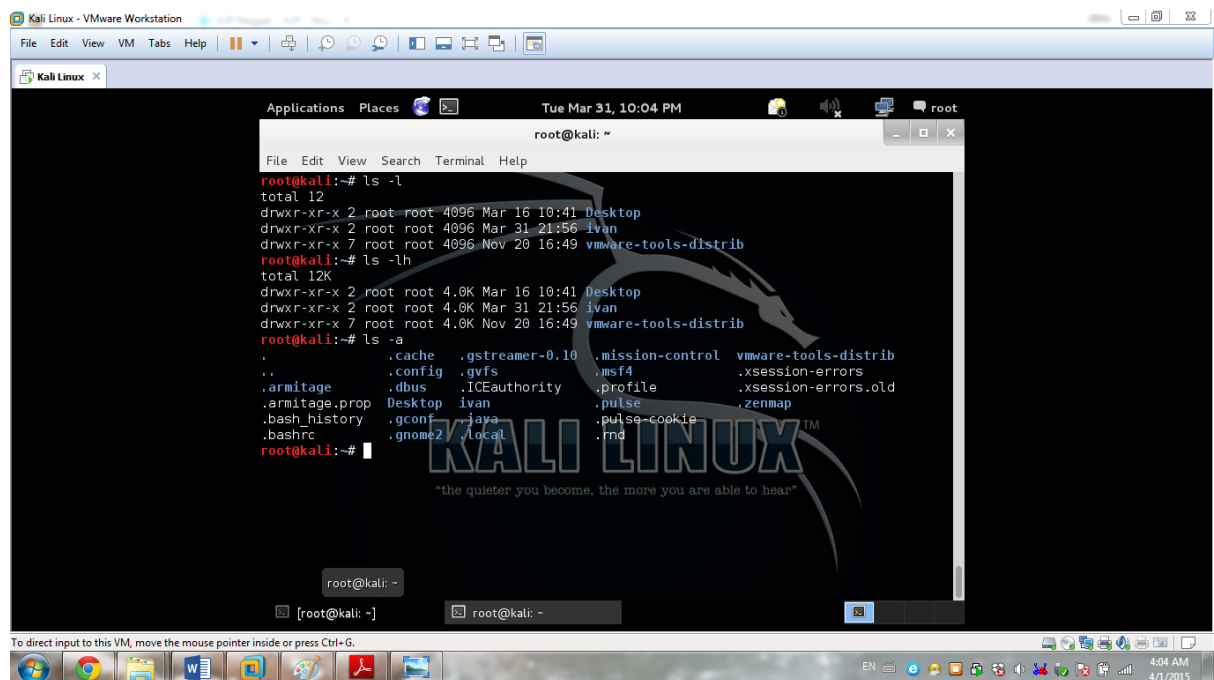
- There are users and super users. Normal users on Kali can run programs, but superuser called : `root` can do anything to the system. To become a superuser just type in : `su -l` , and the console will present you with a password prompt.
- All files are stored in directories and directories can be put inside another directories .They become subdirectories. On top of the tree is the root directory .Every other directory is actually a subdirectory of the root directory.
- If you want to see in which directory are you now type in : `pwd` (print working directory) If you want to change your working directory you need the command : `cd` . Please note, in order to change your working directory, `cd` command should be followed by space and then the directory you want to go in. You can always go back with : `"cd .."` . No matter where are you, you can always go back to your home directory with: `"cd~"` "



- You can create directories with: mkdir command. If you want to remove it : rmdir
- If you want to see a more detailed listing of the files and directories type in : ls -l



Using “ls -a” will list all files, even the hidden ones:



- Another commands are : cp (copy) , mv (move) , rm (remove) .
- If you would like to change your user account password type : passwd
- uname -a = gives you OS system info
- free = gives you memory space info
- history = all commands previously used
- w = who is online
- whoami = info about which user are you
- date = current date
- cal = calendar

In Linux (just like in every other operational system) there are users and groups of users. Usually every user has got his own space on the system, his own folder, he has different permissions to modify, read files or folders and so on. Most of the Linux distributions will have 2 default groups, already created – the users group and the admin group, which contains the root account and /or others. As we said before the root user account has the right to do everything he wants on the machine: deleting accounts, creating groups and so on and so on.

## 7. Users, groups and permissions

In Linux, unlike Windows users and groups are kept much simpler.

To add an user simply type in: adduser “name of the user”

The command: userdel “name of the user” deletes the user

If you want to change the password for a user : passwd “name of the user”

If you want to see all the users on the system type in :vim /etc/passwd , if you want to modify the file – type “a” , to escape – wq

Groups

To create group type in : groupadd “name of the group”

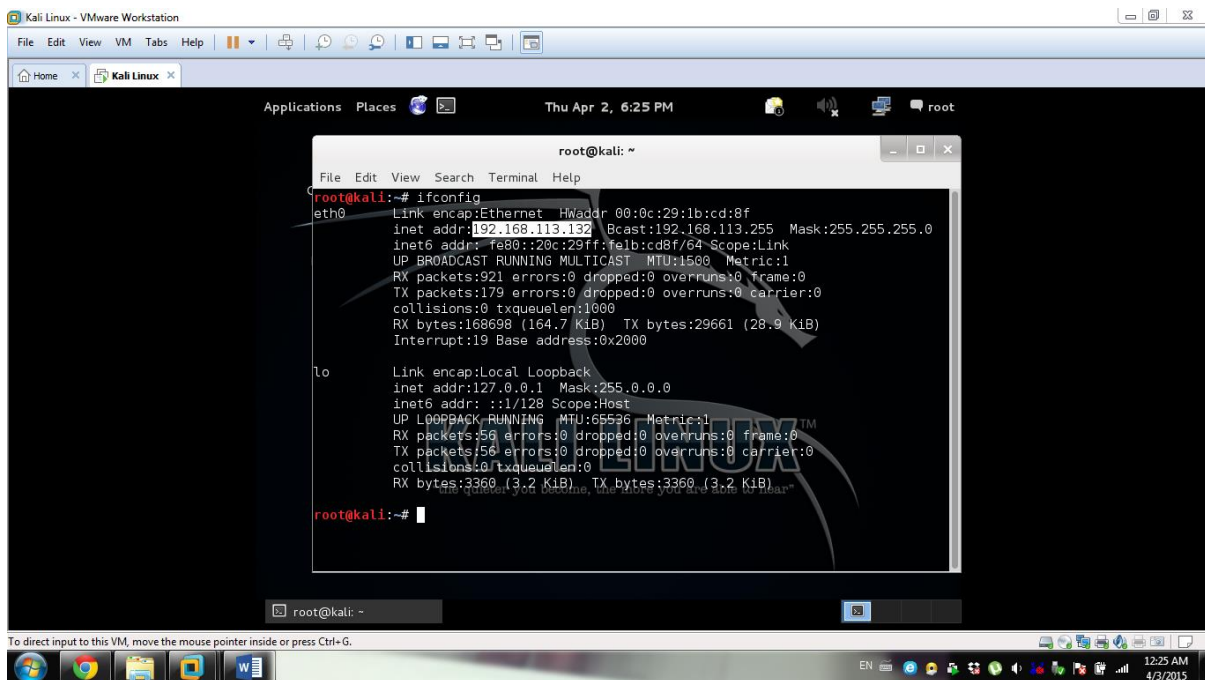
To add an user to a specific group : adduser “name of the user” “name of the group”

## 6. Networking commands in Kali Linux

In order to do some penetration testing, we should be aware of some networking commands which work with Kali. We assume that the reader already has a very good understanding of IP addresses , TCP/IP protocol , subnet masks , NAT , DNS and DHCP protocols. Let’s begin then.

- If you would like to see what is your IP address on your Kali Linux machine , simply type : [Ifconfig](#)

It is important to notice that by default Kali is not announcing itself on the network, requiring an IP address from the DHCP server. In this way, it comes to the network in a stealthy way, without letting other hosts on the network to notice its presence.



```
root@kali:~# ifconfig
eth0:
Link encap:Ethernet  HWaddr 00:0c:29:1b:cd:8f
inet addr:192.168.113.132  Bcast:192.168.113.255  Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe1b:cd8f/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:921 errors:0 dropped:0 overruns:0 frame:0
TX packets:179 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:168698 (164.7 KiB)  TX bytes:29661 (28.9 KiB)
Interrupt:19 Base address:0x2000

lo:
Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:65536  Metric:1
RX packets:56 errors:0 dropped:0 overruns:0 frame:0
TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3360 (3.2 KiB)  TX bytes:3360 (3.2 KiB)

root@kali:~#
```

You can see many details after typing this command, including your IP address, the subnet mask, and the MAC address of your network card also.



- If you want to see what is your default gateway type :

`ip route`

```

root@kali: ~
File Edit View Search Terminal Help
RX packets:921 errors:0 dropped:0 overruns:0 frame:0
TX packets:179 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:168698 (164.7 KiB) TX bytes:29661 (28.9 KiB)
Interrupt:19 Base address:0x2000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:56 errors:0 dropped:0 overruns:0 frame:0
TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3360 (3.2 KiB) TX bytes:3360 (3.2 KiB)

root@kali:~# ifconfig | grep inet
inet addr:192.168.113.132 Bcast:192.168.113.255 Mask:255.255.255.0
inet6 addr: fe80::20d:29ff:fe1b:c08f/64 Scope:Link
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host

root@kali:~# ip route
default via 192.168.113.2 dev eth0
192.168.113.0/24 dev eth0 proto kernel scope link src 192.168.113.132
root@kali:~#

```

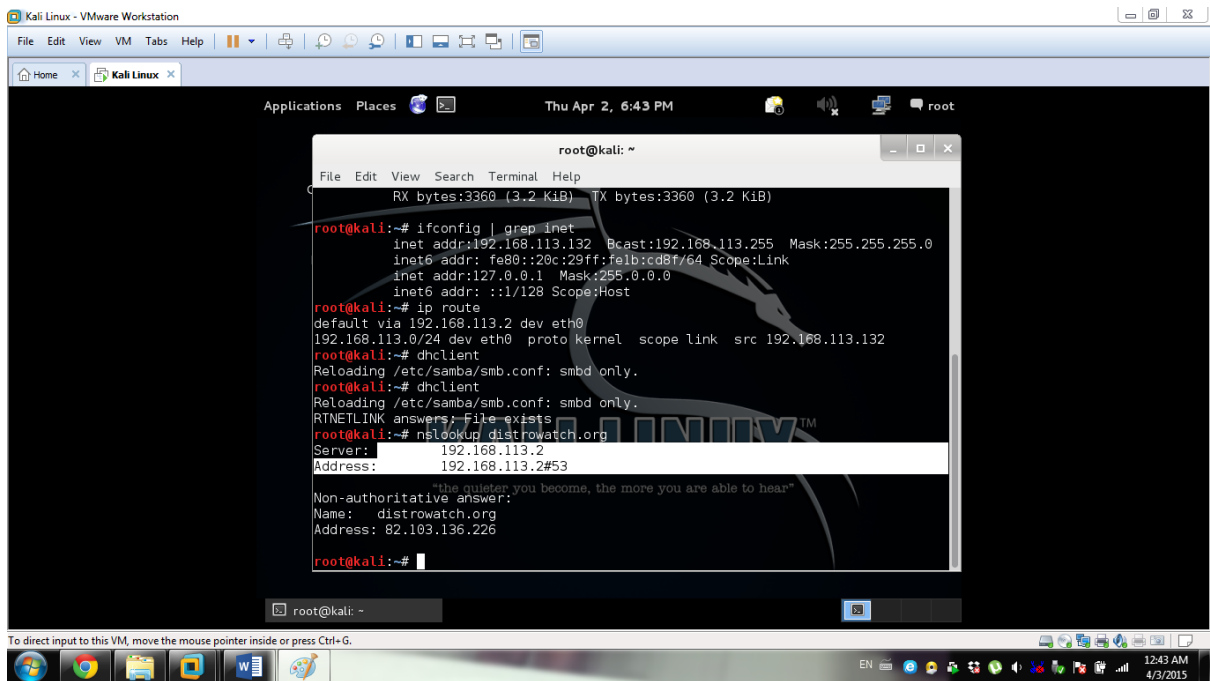
- If you don't have an IP address assigned to you automatically , you can ask the DHCP server to give you one with this command:

`dhclient`

- If you want to check if your DNS server is functioning correctly just type in the following command:

`nslookup distrowatch.org`

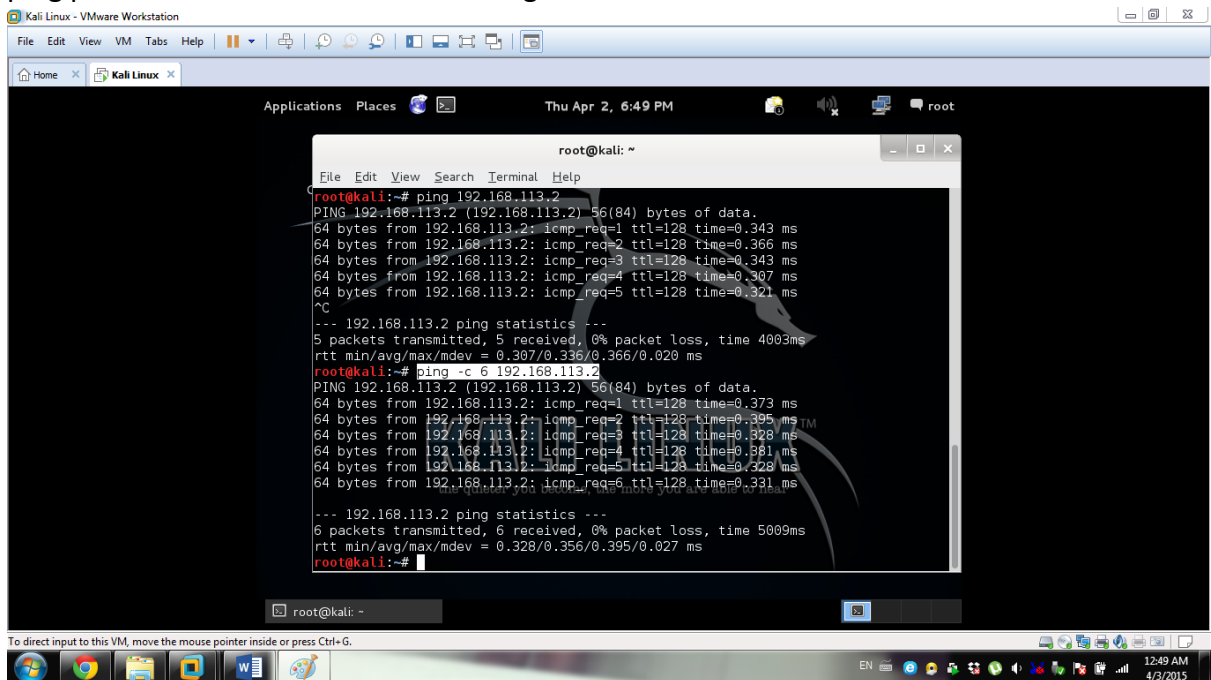




```
root@kali: ~  
File Edit View Search Terminal Help  
RX bytes:3360 (3.2 KiB) TX bytes:3360 (3.2 KiB)  
root@kali:~# ifconfig | grep inet  
inet addr:192.168.113.132 Bcast:192.168.113.255 Mask:255.255.255.0  
inet6 addr: fe80::20c:29ff:fe1b:cd8f/64 Scope:Link  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
root@kali:~# ip route  
default via 192.168.113.2 dev eth0  
192.168.113.0/24 dev eth0 proto kernel scope link src 192.168.113.132  
root@kali:~# dhclient  
Reloading /etc/samba/smb.conf: smbd only.  
root@kali:~# dhclient  
Reloading /etc/samba/smb.conf: smbd only.  
RTNETLINK answers: File exists  
root@kali:~# nslookup distrowatch.org  
Server: 192.168.113.2  
Address: 192.168.113.2#53  
Non-authoritative answer:  
Name: distrowatch.org  
Address: 82.103.136.226  
root@kali:~#
```

If you get an answer similar to this one, it means that your DNS server is operating correctly.

- If you would like to check if another host is active on the network, you just use the ping command, followed by the IP address of the host. If you would like to send just 6 ICMP ping packets to the host do the following:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ping 192.168.113.2  
PING 192.168.113.2 (192.168.113.2) 56(84) bytes of data:  
64 bytes from 192.168.113.2: icmp_req=1 ttl=128 time=0.343 ms  
64 bytes from 192.168.113.2: icmp_req=2 ttl=128 time=0.366 ms  
64 bytes from 192.168.113.2: icmp_req=3 ttl=128 time=0.343 ms  
64 bytes from 192.168.113.2: icmp_req=4 ttl=128 time=0.307 ms  
64 bytes from 192.168.113.2: icmp_req=5 ttl=128 time=0.321 ms  
^C  
--- 192.168.113.2 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 0.307/0.336/0.366/0.020 ms  
root@kali:~# ping -c 6 192.168.113.2  
PING 192.168.113.2 (192.168.113.2) 56(84) bytes of data:  
64 bytes from 192.168.113.2: icmp_req=1 ttl=128 time=0.373 ms  
64 bytes from 192.168.113.2: icmp_req=2 ttl=128 time=0.395 ms  
64 bytes from 192.168.113.2: icmp_req=3 ttl=128 time=0.328 ms  
64 bytes from 192.168.113.2: icmp_req=4 ttl=128 time=0.381 ms  
64 bytes from 192.168.113.2: icmp_req=5 ttl=128 time=0.328 ms  
64 bytes from 192.168.113.2: icmp_req=6 ttl=128 time=0.331 ms  
--- 192.168.113.2 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5009ms  
rtt min/avg/max/mdev = 0.328/0.356/0.395/0.027 ms  
root@kali:~#
```

- Sometimes the host you would like to ping is active, but you cannot reach him. You can trace the path from your computer to this host and see where the problem is. Type:

tracert (IP address)

## Connecting to remote machines

If you want to connect to a remote machine you can use the telnet command.

You can try that with: `telnet scn.org`, which will connect you to an open server.

Login as “visitor” to scroll down.

You can transfer files over a network with ftp. The command is `ftp`, then `open`, then the name of the server you want to reach.

## Additional commands

### Controlling processes

To see all running processes on your system type in: `ps`

Each process has a PID ( Process identity number)

Add `ps -e` to see more details. If you want to kill a process type in : `kill "PID"`

## Conclusion

There are thousands of commands in the command line in Kali Linux. In this lab we have discussed only a few of them. You are highly encouraged to dig in and find the commands you need about a particular case. The more commands you know, the better you become, when it comes to using the CLI in Linux distributions.