

# **Certified Ethical Hacking With Penetration Testing CEHWPT**

LABS Course

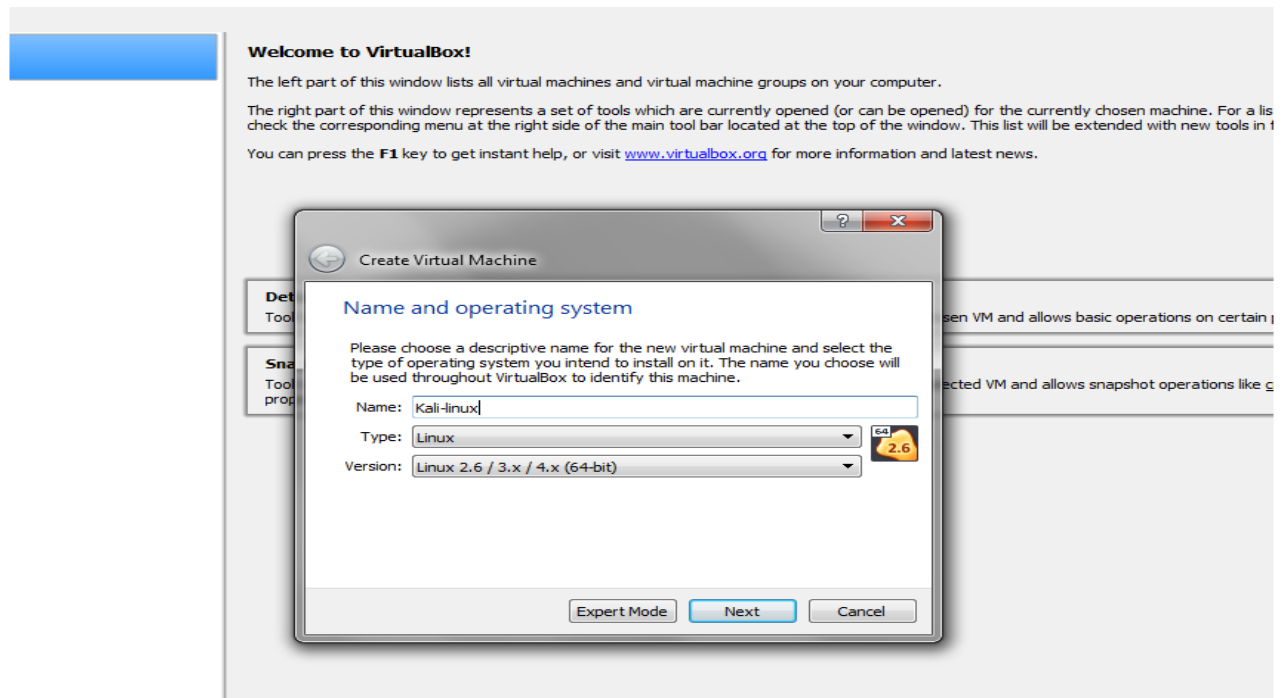
LAB1 Installing Kali Linux

Prepared by Eng. Khaled Gamo

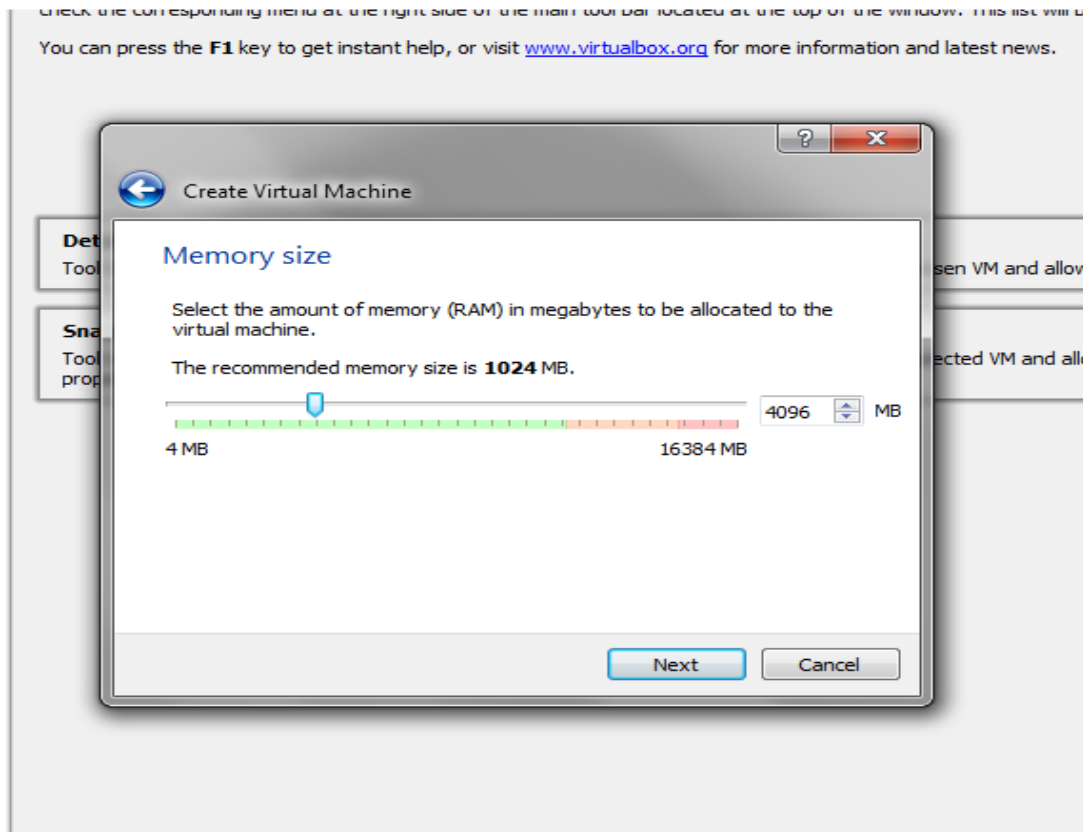
15-6-2019

## Lab 1 Installing Kali Linux

### 1- Add new VM in Virtualbox menu



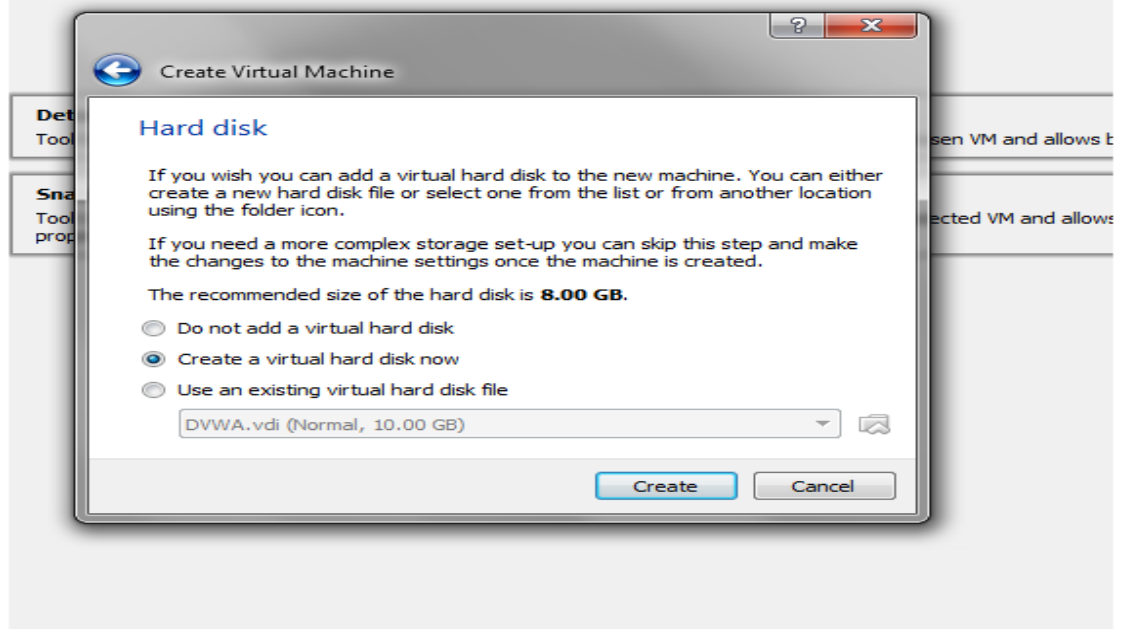
### 2- Choose memory size



### 3- Press next and create a virtual hard disk

check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be

You can press the **F1** key to get instant help, or visit [www.virtualbox.org](http://www.virtualbox.org) for more information and latest news.



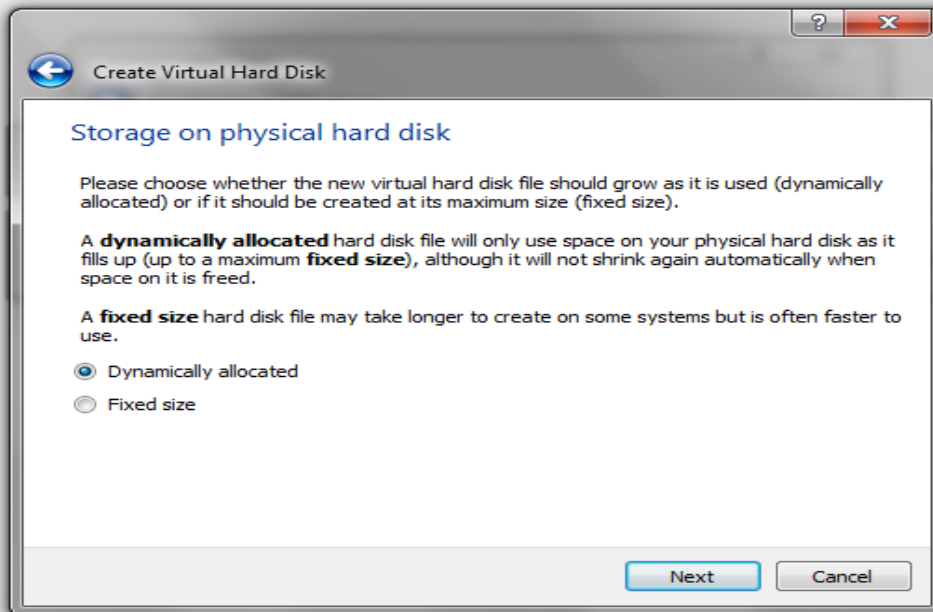
### 4- Choose dynamic allocated

**Welcome to VirtualBox!**

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently checked menu at the right side of the main tool bar located at the top of the window. This list will be extended as more tools are added.

You can press the **F1** key to get instant help, or visit [www.virtualbox.org](http://www.virtualbox.org) for more information and latest news.



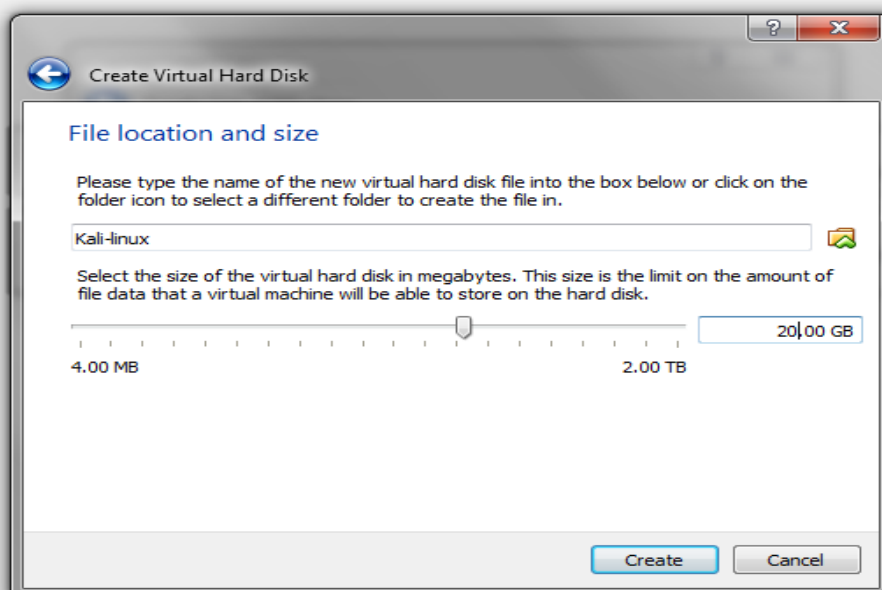
## 5- Change Disk size to 20 GB

**Welcome to VirtualBox!**

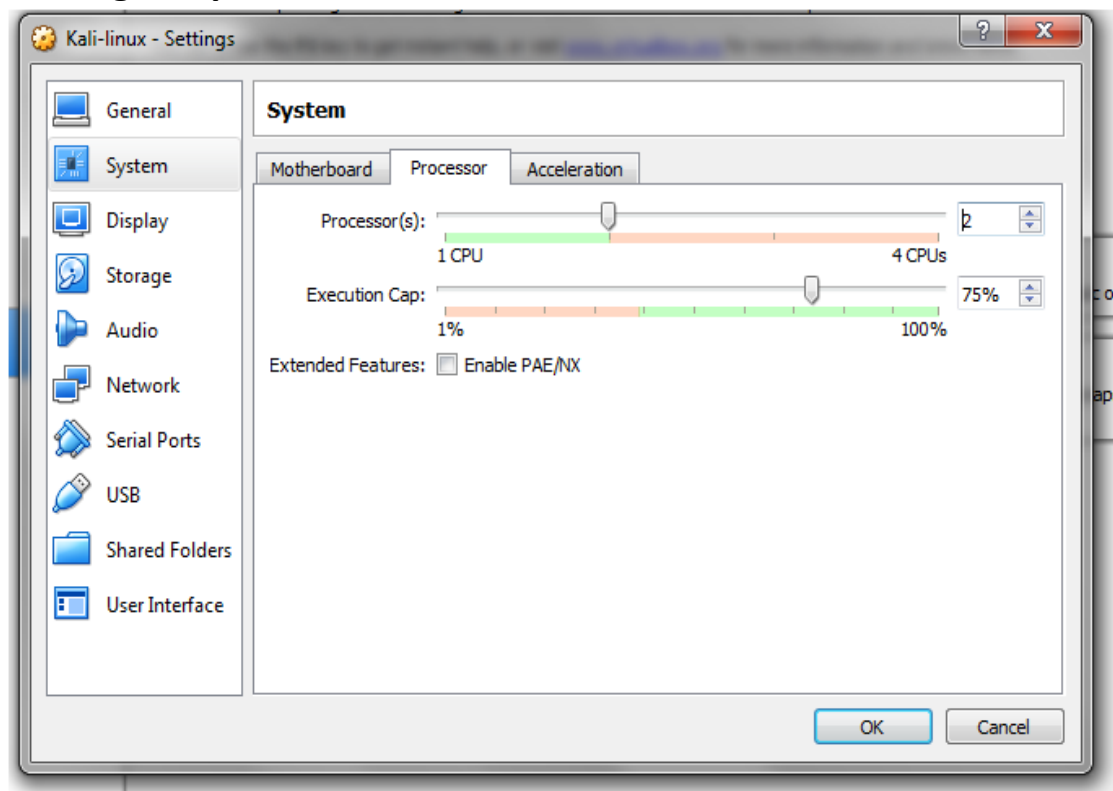
The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently checked menu at the right side of the main tool bar located at the top of the window. This list will be extended as more tools are added.

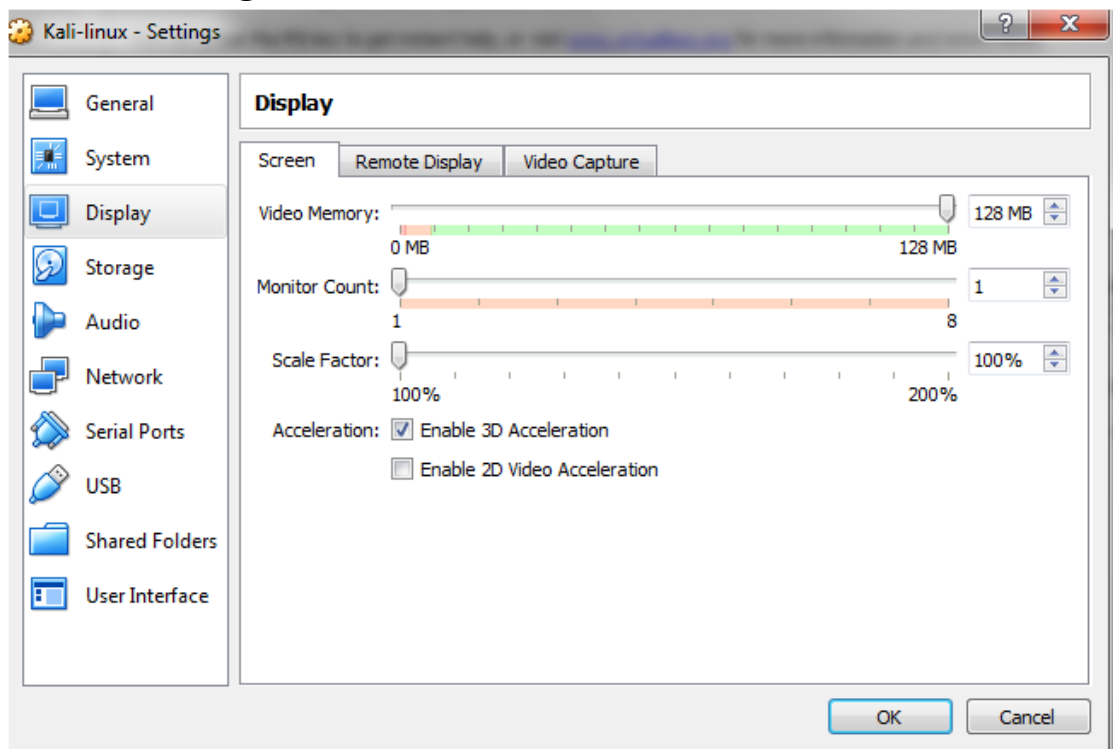
You can press the **F1** key to get instant help, or visit [www.virtualbox.org](http://www.virtualbox.org) for more information and latest news.



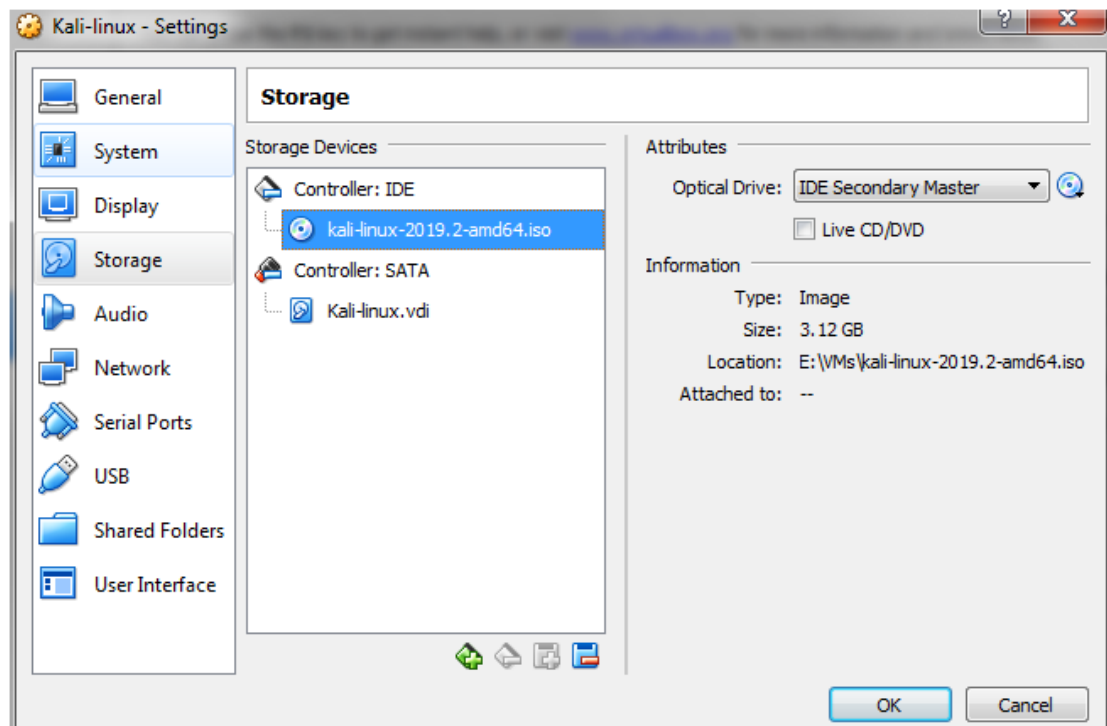
## 6- Setting the process



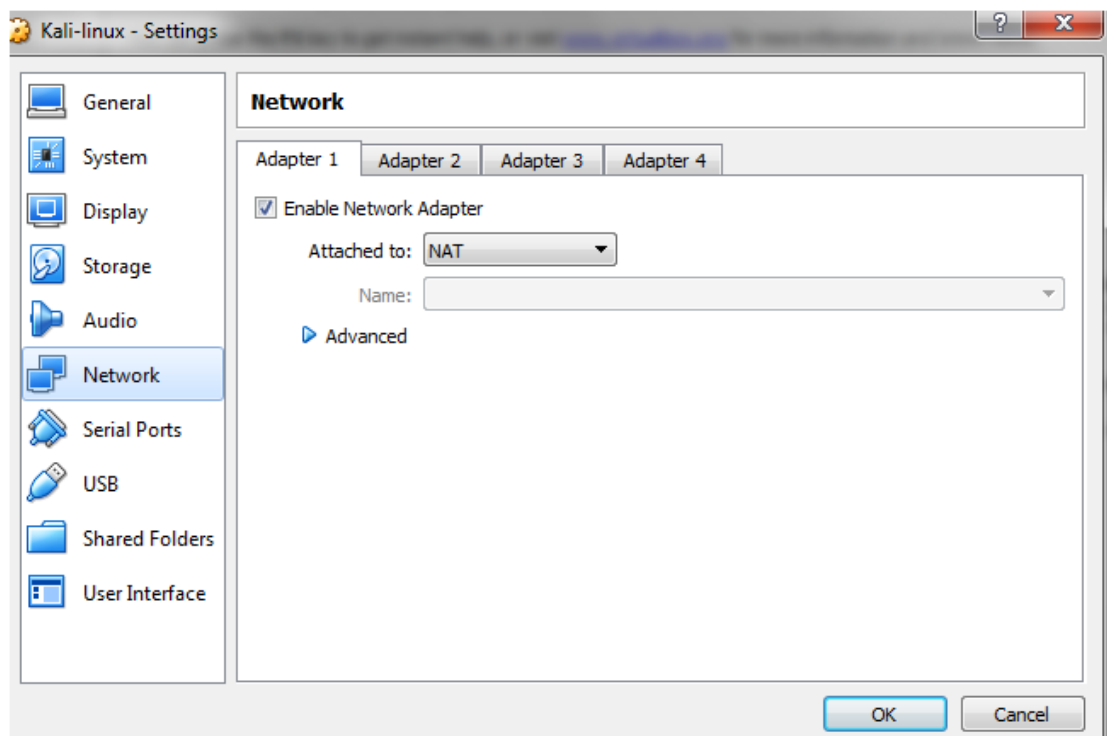
## 7- Screen setting



## 8- Storage setting Choose the ISO image



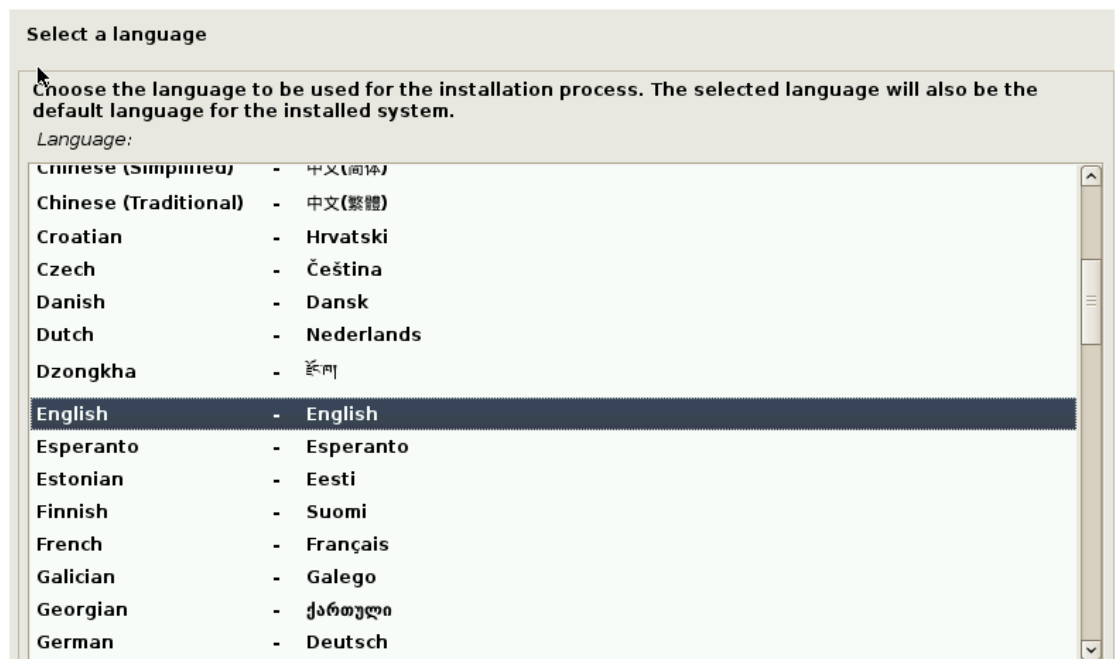
## 9- In network setting choose NAT



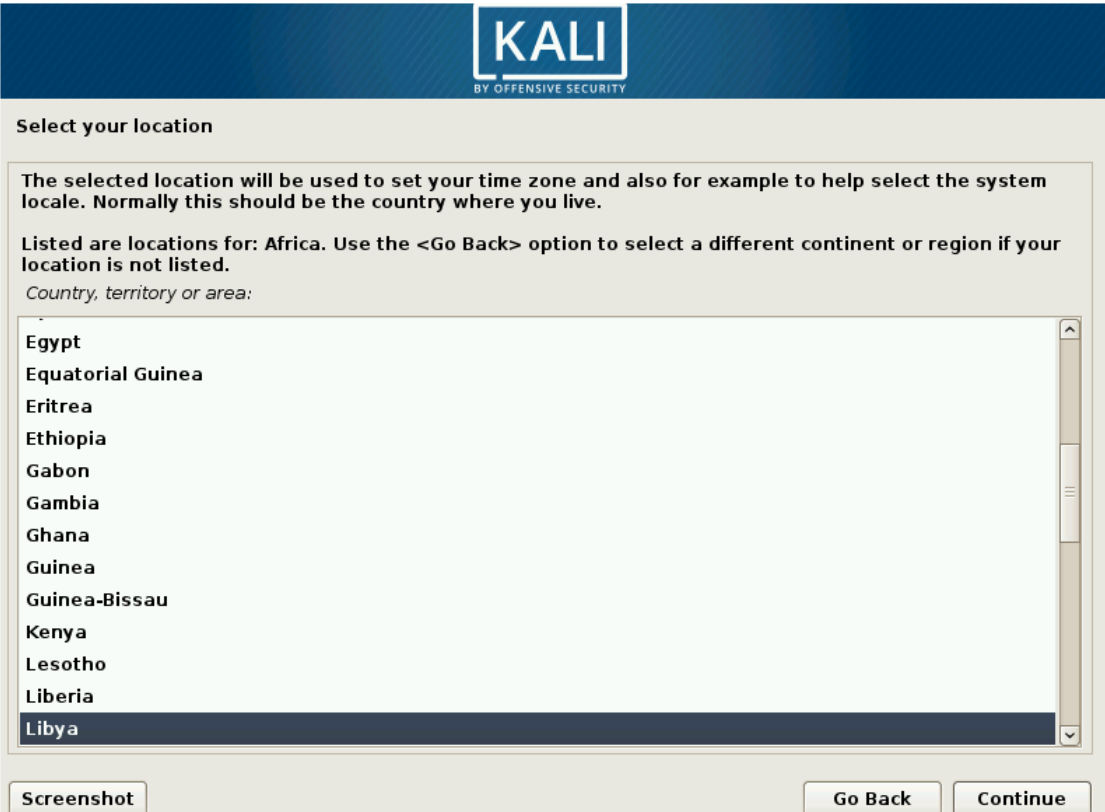
## 10- startup the VM and choose Graphical install



## 11- Select language



## 12- Select your location



The Kali Linux installation window has a dark blue header with the Kali logo and the text "BY OFFENSIVE SECURITY". Below the header, the title "Select your location" is displayed. The main content area contains instructions: "The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live." and "Listed are locations for: Africa. Use the <Go Back> option to select a different continent or region if your location is not listed." Below this, a label "Country, territory or area:" is followed by a scrollable list of countries. The list includes Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, and Libya. The "Libya" option is currently selected and highlighted in dark blue. At the bottom of the window, there are three buttons: "Screenshot", "Go Back", and "Continue".

**KALI**  
BY OFFENSIVE SECURITY

Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Listed are locations for: Africa. Use the <Go Back> option to select a different continent or region if your location is not listed.

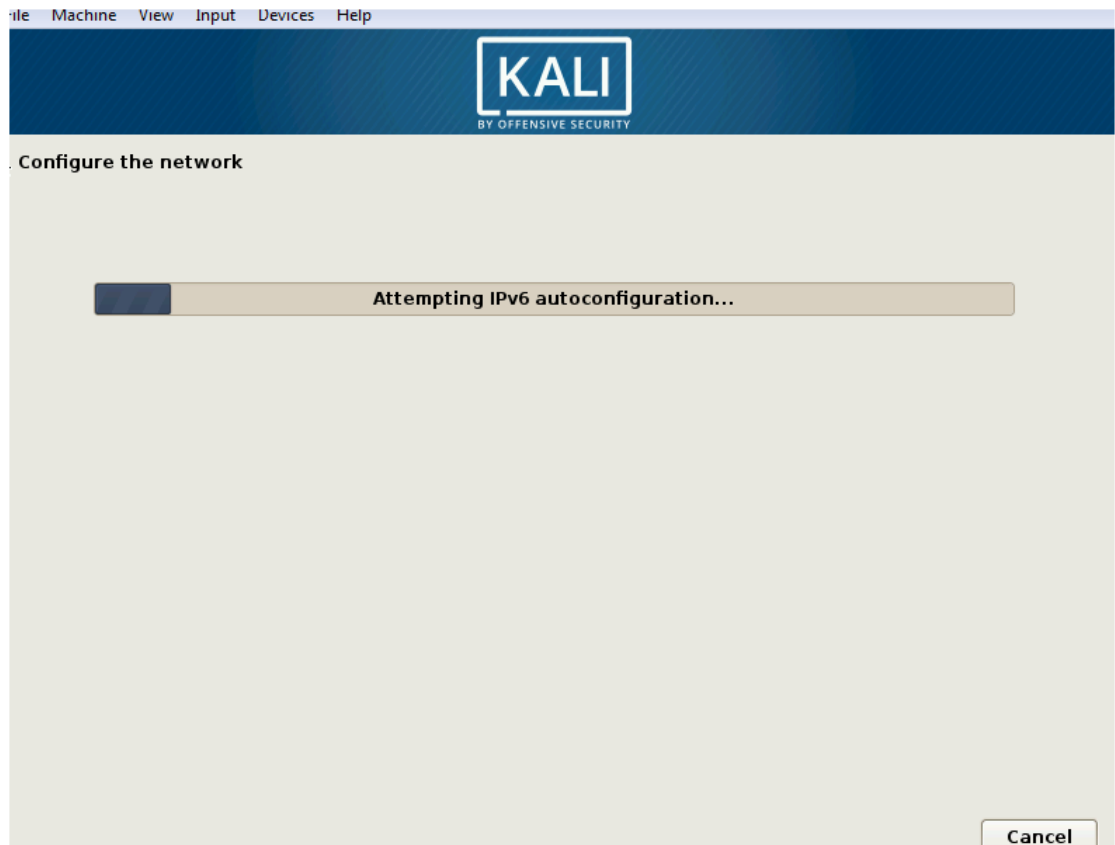
Country, territory or area:

- Egypt
- Equatorial Guinea
- Eritrea
- Ethiopia
- Gabon
- Gambia
- Ghana
- Guinea
- Guinea-Bissau
- Kenya
- Lesotho
- Liberia
- Libya

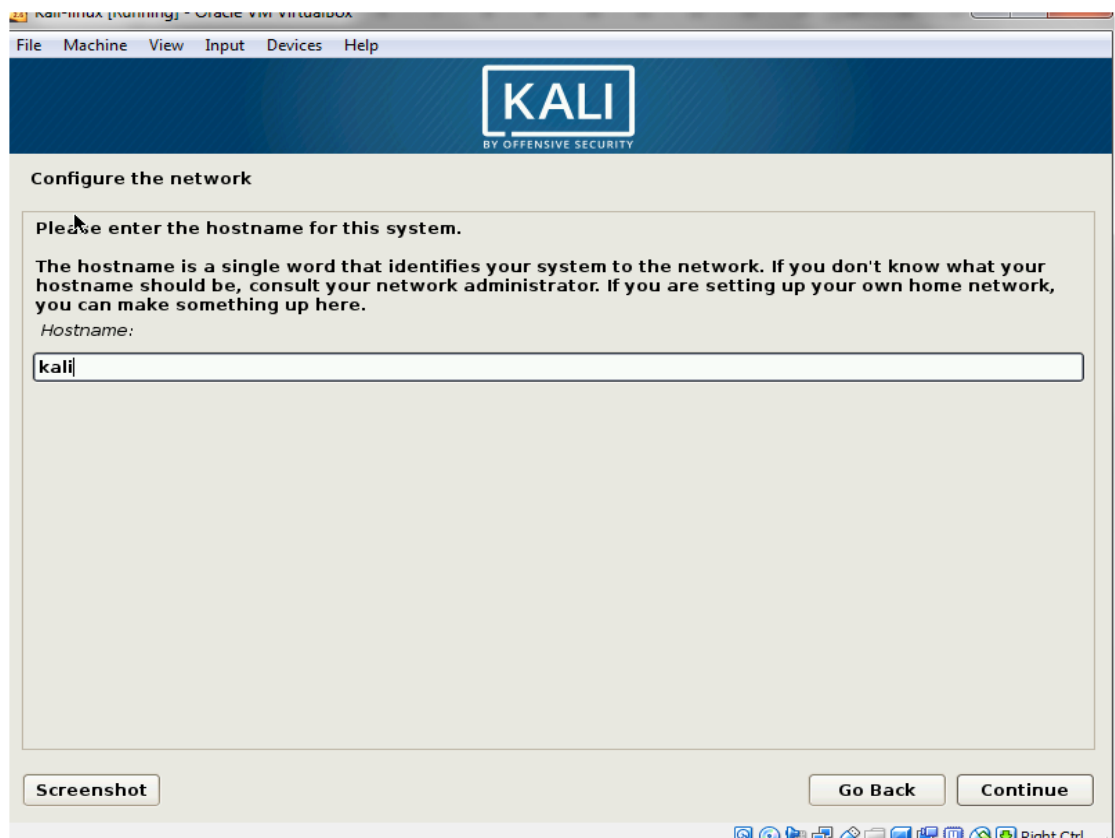
Screenshot Go Back Continue

### 13- Start copying files

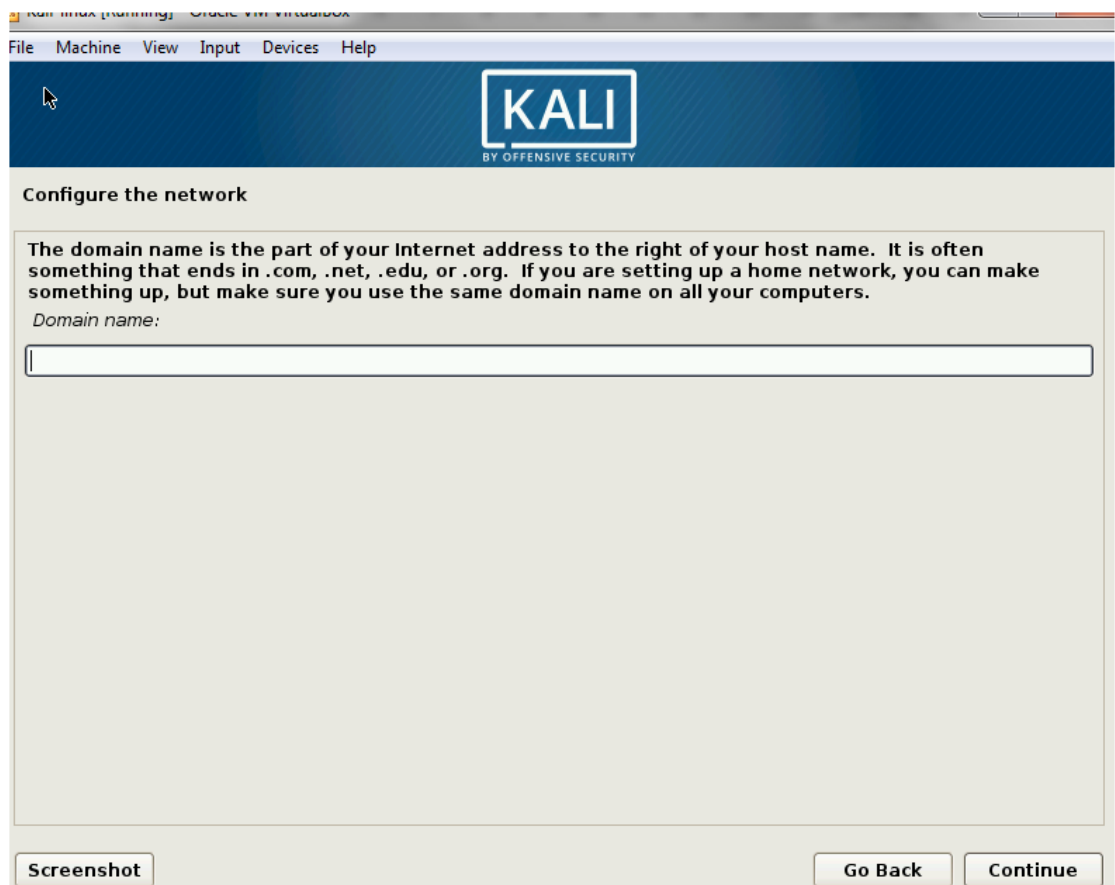




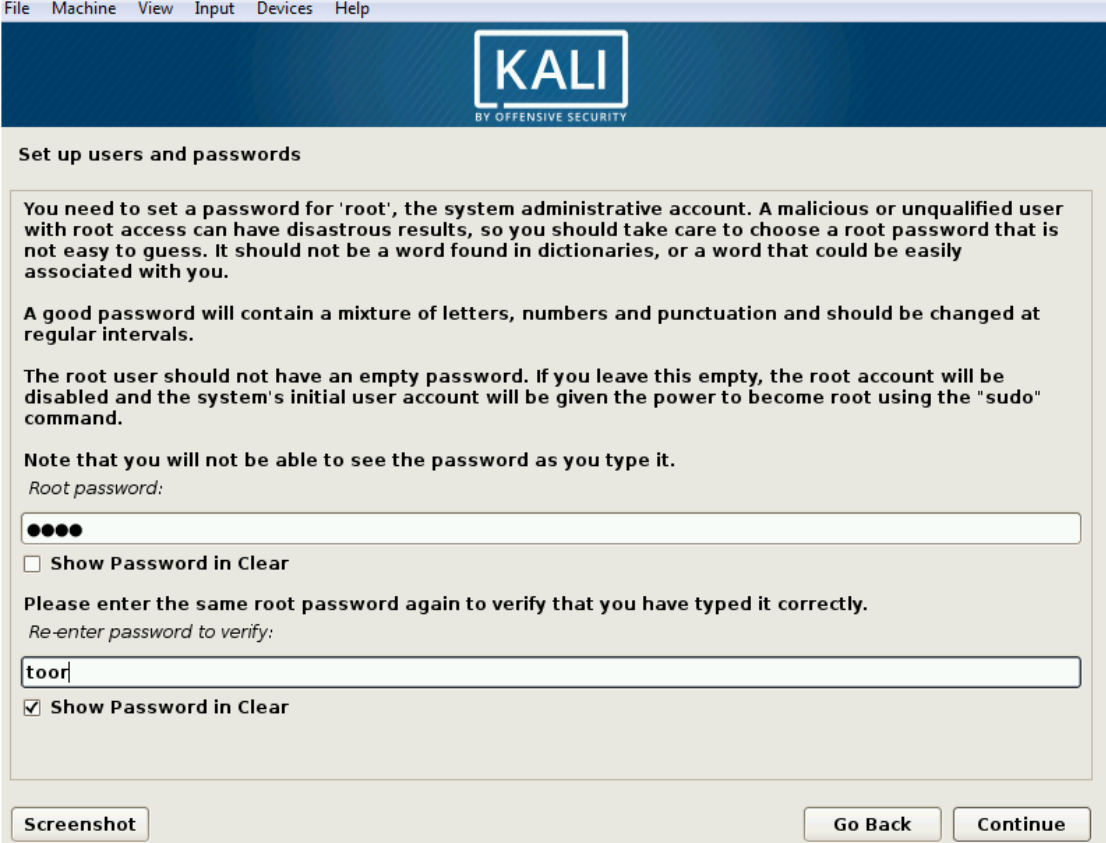
## 14- Choose the name of the kali



## 15- We will keep the domain empty



## 16- Setup the password



The image shows a Kali Linux installer window titled "Set up users and passwords". It features a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The Kali logo is at the top. The main text explains the importance of setting a root password and provides instructions on password requirements. It includes a password input field with masked characters, a checkbox for "Show Password in Clear", and a verification section with another input field and a checkbox. Navigation buttons "Screenshot", "Go Back", and "Continue" are at the bottom.

File Machine View Input Devices Help

**KALI**  
BY OFFENSIVE SECURITY

### Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

•••••

☐ Show Password in Clear

Please enter the same root password again to verify that you have typed it correctly.

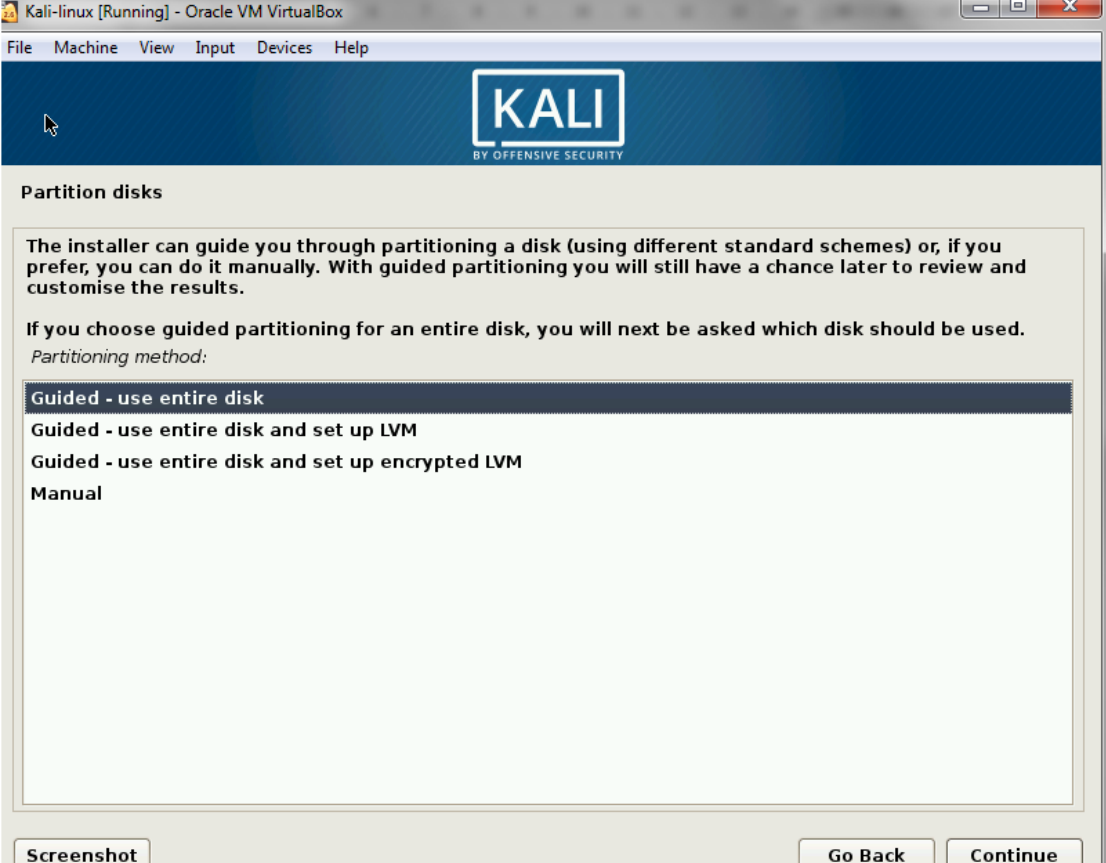
Re-enter password to verify:

toor

☒ Show Password in Clear

Screenshot Go Back Continue

## 17- for disk partition we will choose use entire disk



The image shows a Kali Linux installer window titled "Partition disks". It features a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The Kali logo is at the top. The main text explains the partitioning options: guided (entire disk, LVM, encrypted LVM) or manual. A list of options is shown with "Guided - use entire disk" selected. Navigation buttons "Screenshot", "Go Back", and "Continue" are at the bottom.

Kali-linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

**KALI**  
BY OFFENSIVE SECURITY

### Partition disks

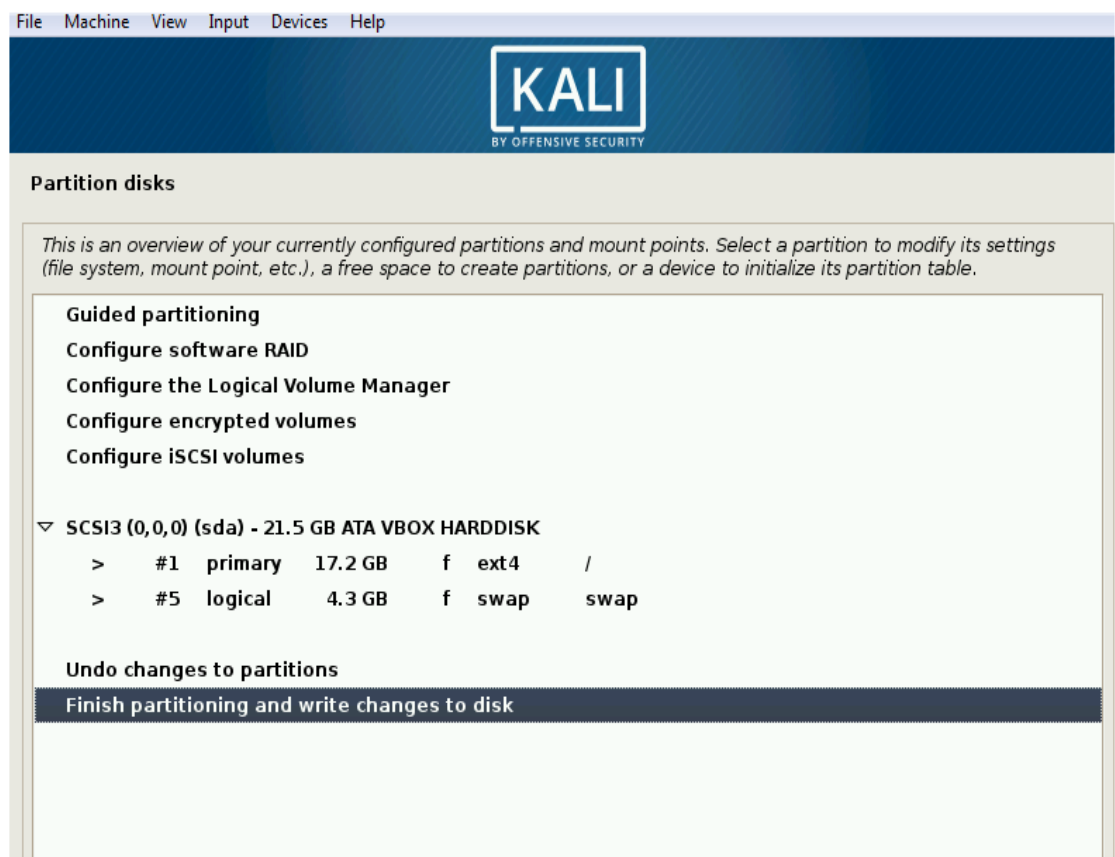
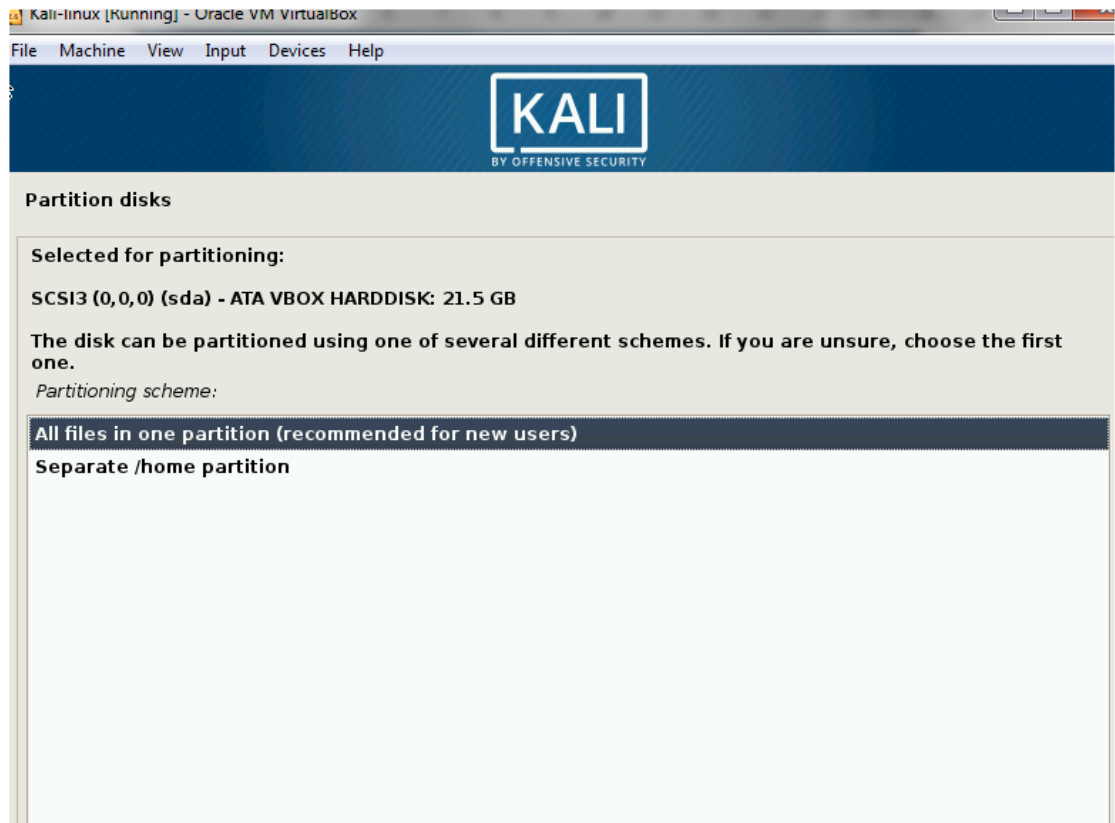
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

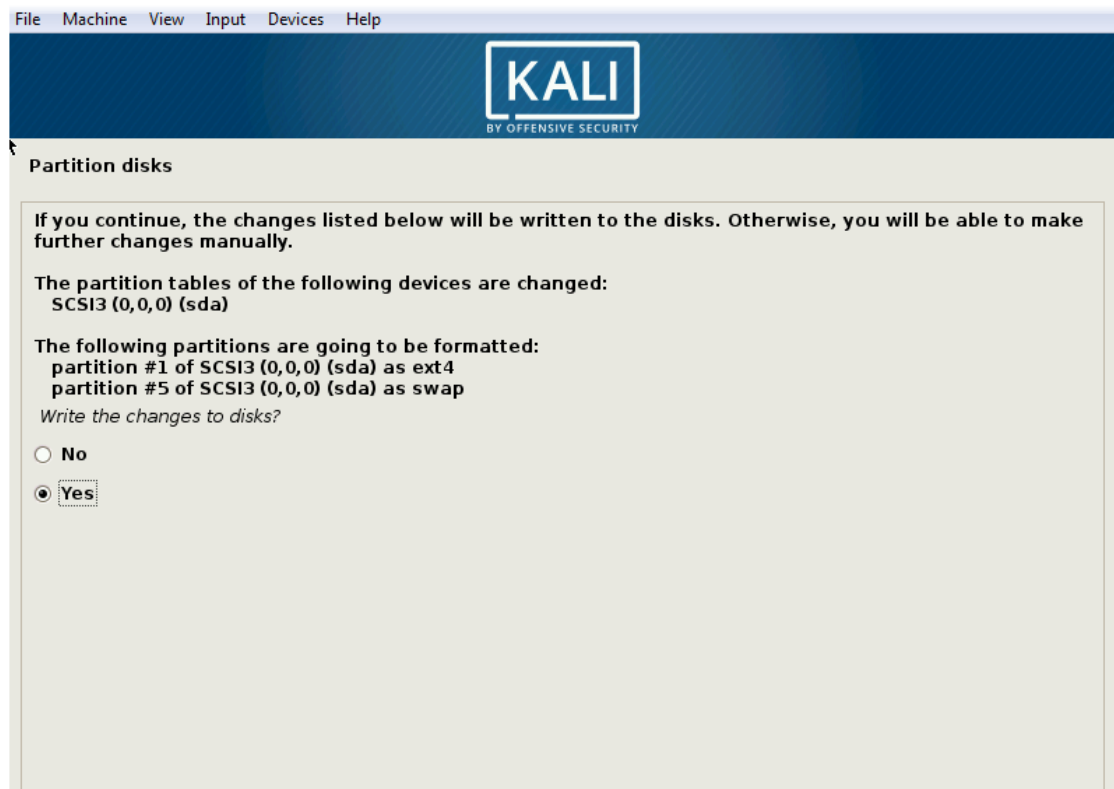
Partitioning method:

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

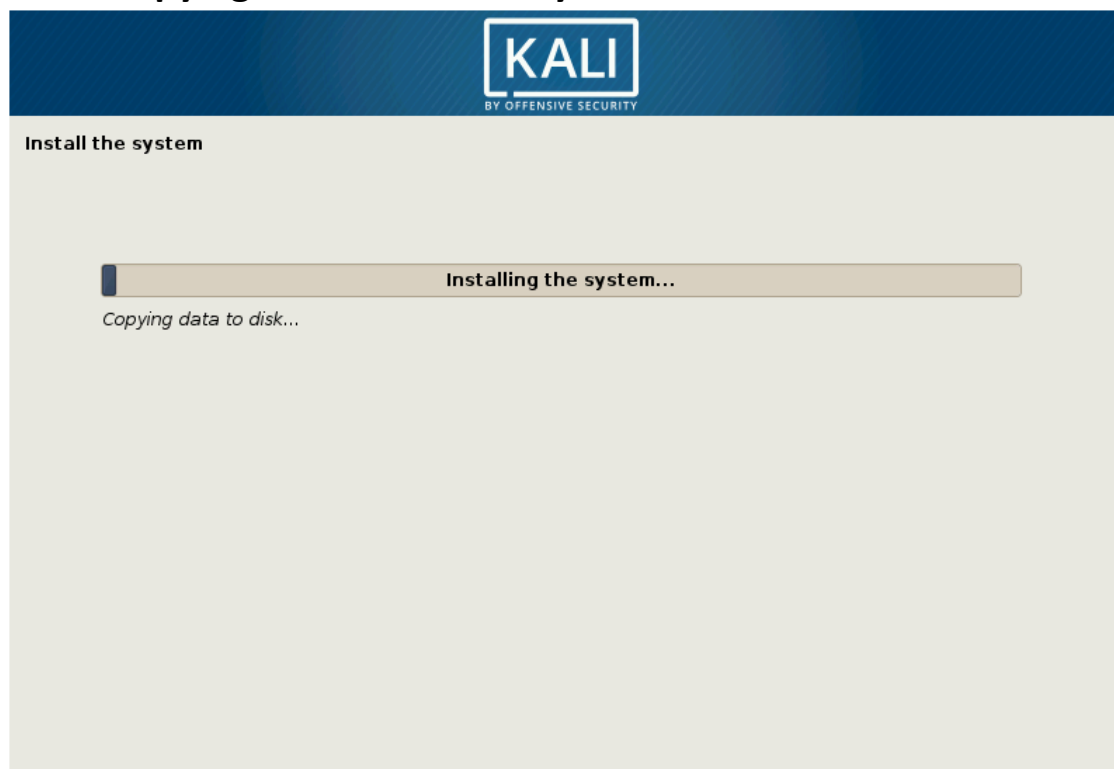
Screenshot Go Back Continue




## 18- writing to the disk



## 19- copying the data to the system



## 20- configure package manager



The image shows a Kali Linux installer window titled "Configure the package manager". The window has a dark blue header with the Kali logo and the text "BY OFFENSIVE SECURITY". Below the header, the title "Configure the package manager" is displayed. The main content area contains a paragraph: "A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available." Below this paragraph is the question "Use a network mirror?" followed by two radio button options: "No" and "Yes". The "Yes" option is selected. At the bottom of the window, there are three buttons: "Screenshot", "Go Back", and "Continue".

**KALI**  
BY OFFENSIVE SECURITY

**Configure the package manager**

A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.


Use a network mirror?

☐ No

☒ Yes

Screenshot Go Back Continue

## No proxy setting



The image shows a Kali Linux installer window titled "Configure the package manager". The window has a dark blue header with the Kali logo and the text "BY OFFENSIVE SECURITY". Below the header, the title "Configure the package manager" is displayed. The main content area contains a paragraph: "If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank." Below this paragraph is another paragraph: "The proxy information should be given in the standard form of 'http://[[user]:pass]@host[:port]/'." followed by "HTTP proxy information (blank for none):". Below this text is a text input field. At the bottom of the window, there are three buttons: "Screenshot", "Go Back", and "Continue".

**KALI**  
BY OFFENSIVE SECURITY

**Configure the package manager**


If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user]:pass]@host[:port]/".

HTTP proxy information (blank for none):

Screenshot Go Back Continue

## 21- Installing GRUB loader



Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

**Warning:** If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.


*Install the GRUB boot loader to the master boot record?*

☐ No

☒ Yes

Screenshot

Go Back Continue



Install the GRUB boot loader on a hard disk

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB on the master boot record of your first hard drive. If you prefer, you can install GRUB elsewhere on the drive, or to another drive, or even to a floppy.

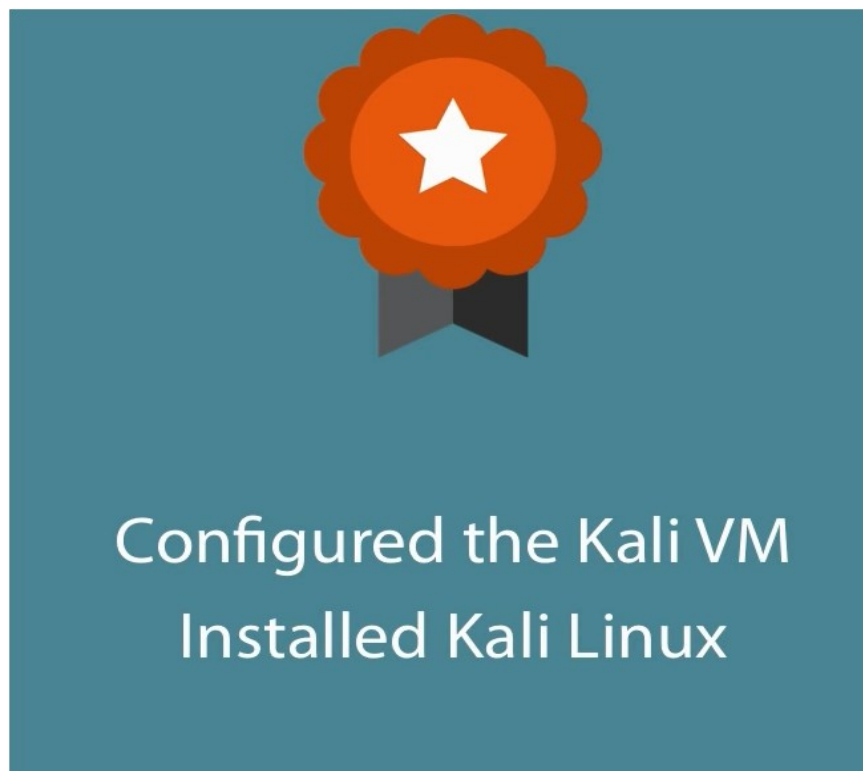
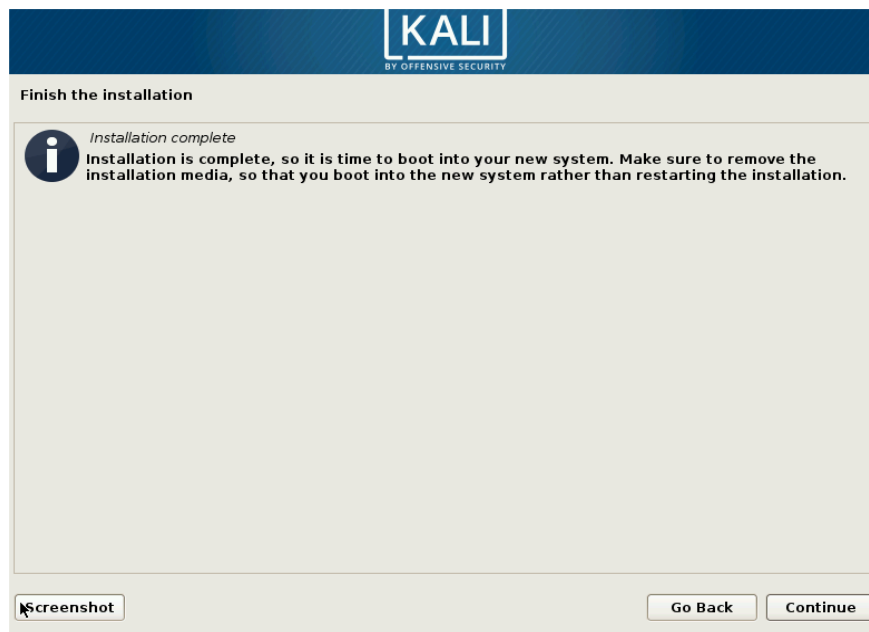
*Device for boot loader installation:*

Enter device manually

`/dev/sda (ata-VBOX_HARDDISK_VB8e04792d-0539fa47)`

Screenshot

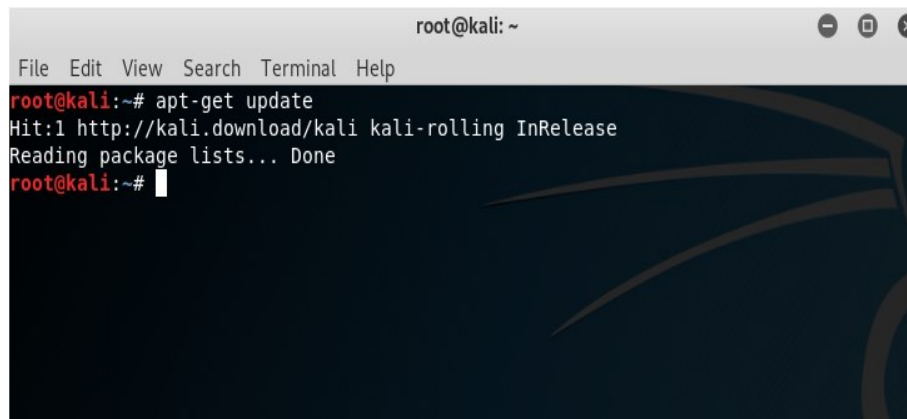
Go Back Continue





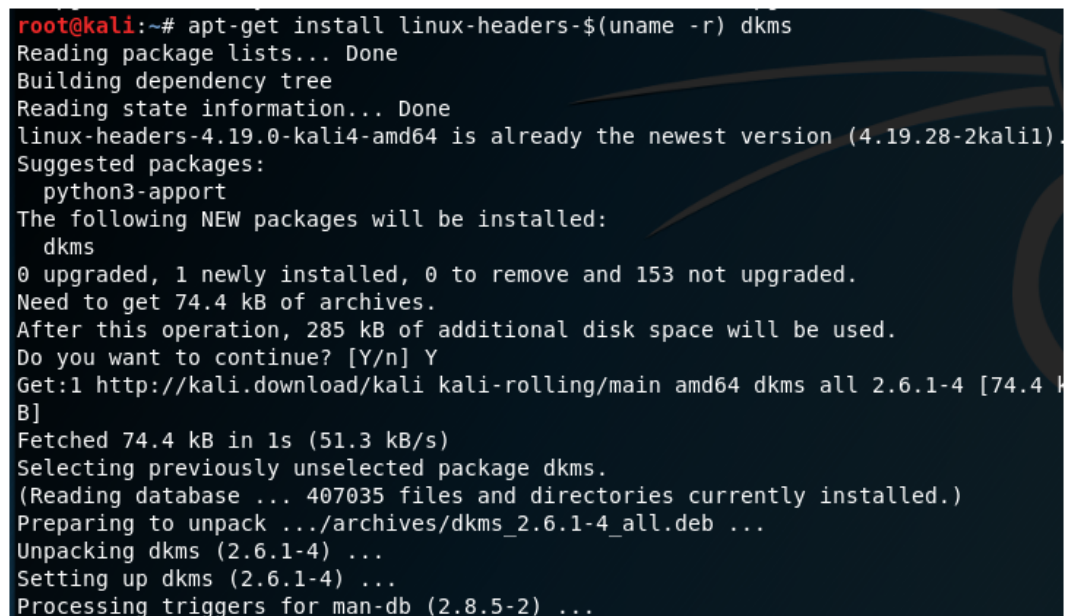
## LAB 2 Configuring Kali Linux

### 1- Update package list using command `apt-get update`

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'apt-get update' has been executed, resulting in the following output: 'Hit:1 http://kali.download/kali kali-rolling InRelease', 'Reading package lists... Done', and the prompt 'root@kali:~#'.

```
root@kali:~# apt-get update
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
root@kali:~#
```

### 2- Install Linux header using command `apt-get install linux-headers-$(uname -r) dkms`

A terminal window showing the execution of 'apt-get install linux-headers-\$(uname -r) dkms'. The output includes: 'Reading package lists... Done', 'Building dependency tree', 'Reading state information... Done', 'linux-headers-4.19.0-kali4-amd64 is already the newest version (4.19.28-2kali1)', 'Suggested packages: python3-apport', 'The following NEW packages will be installed: dkms', '0 upgraded, 1 newly installed, 0 to remove and 153 not upgraded.', 'Need to get 74.4 kB of archives.', 'After this operation, 285 kB of additional disk space will be used.', 'Do you want to continue? [Y/n] Y', 'Get:1 http://kali.download/kali kali-rolling/main amd64 dkms all 2.6.1-4 [74.4 kB]', 'Fetched 74.4 kB in 1s (51.3 kB/s)', 'Selecting previously unselected package dkms.', '(Reading database ... 407035 files and directories currently installed.)', 'Preparing to unpack .../archives/dkms\_2.6.1-4\_all.deb ...', 'Unpacking dkms (2.6.1-4) ...', 'Setting up dkms (2.6.1-4) ...', and 'Processing triggers for man-db (2.8.5-2) ...'.

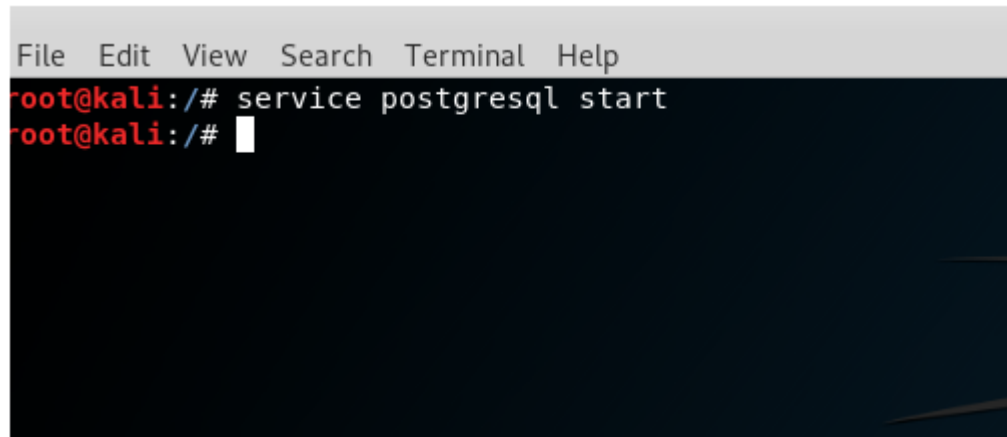
```
root@kali:~# apt-get install linux-headers-$(uname -r) dkms
Reading package lists... Done
Building dependency tree
Reading state information... Done
linux-headers-4.19.0-kali4-amd64 is already the newest version (4.19.28-2kali1).
Suggested packages:
  python3-apport
The following NEW packages will be installed:
  dkms
0 upgraded, 1 newly installed, 0 to remove and 153 not upgraded.
Need to get 74.4 kB of archives.
After this operation, 285 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 dkms all 2.6.1-4 [74.4 kB]
Fetched 74.4 kB in 1s (51.3 kB/s)
Selecting previously unselected package dkms.
(Reading database ... 407035 files and directories currently installed.)
Preparing to unpack .../archives/dkms_2.6.1-4_all.deb ...
Unpacking dkms (2.6.1-4) ...
Setting up dkms (2.6.1-4) ...
Processing triggers for man-db (2.8.5-2) ...
```

### 3- Copying VBoxLinuxAdditions.run to tmp folder `Cp /media/cdrom/VBoxLinuxAdditions.run /tmp` Run it from tmp directory

/tmp/VBoxLinuxAdditions.run

#### 4- Starting postgresql

Service postgresql start



```
File Edit View Search Terminal Help
root@kali:/# service postgresql start
root@kali:/#
```

#### 5- Init metasploit database

Msfdb init



```
root@kali:/# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:/#
```

#### 6- Starting metasploit using

Msfconsole

```

root@kali:/# msfconsole

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccc.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffff.....
ffffffff.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aieee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!

```

## 7- Check database status

### db\_status

```

msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 >

```