Pentetsting Lab with host only network configuration

As per organization IT Security policies, IT team won't allow users to create a bridge connection among the host and guest (virtual machine). To overcome this problem we can use host only network configuration in virtual box, which won't affect critical internal IT infrastructure and useful to do penetration testing.

Virtual Box network description [1]

Each of the eight networking adapters can be separately configured to operate in one of the following modes:

Not attached

> In this mode, Virtual Box reports to the guest that a network card is present, but that there is no connection -- as if no Ethernet cable was plugged into the card. This way it is possible to "pull" the virtual Ethernet cable and disrupt the connection, which can be useful to inform a guest operating system that no network connection is available and enforce a reconfiguration.

Network Address Translation (NAT)

> If all you want is to browse the Web, download files and view e-mail inside the guest, then this default mode should be sufficient for you, and you can safely skip the rest of this section. Please note that there are certain limitations when using Windows file sharing

NAT Network

> The NAT network is a new NAT flavor introduced in Virtual Box 4.3.

Bridged networking

> This is for more advanced networking needs such as network simulations and running servers in a guest. When enabled, Virtual Box connects to one of your installed network cards and exchanges network packets directly, circumventing your host operating system's network stack.

Internal networking

> This can be used to create a different kind of software-based network which is visible to selected virtual machines, but not to applications running on the host or to the outside world.

Host-only networking

> This can be used to create a network containing the host and a set of virtual machines, without the need for the host's physical network interface. Instead, a virtual network interface (similar to a loopback interface) is created on the host, providing connectivity among virtual machines and the host.

Generic networking

> Rarely used modes share the same generic network interface, by allowing the user to select a driver which can be included with Virtual Box or be distributed in an extension pack.
>
> At the moment there are potentially two available sub-modes:

UDP Tunnel

This can be used to interconnect virtual machines running on different hosts directly, easily and transparently, over existing network infrastructure.

VDE (Virtual Distributed Ethernet) networking

This option can be used to connect to a Virtual Distributed Ethernet switch on a Linux or a FreeBSD host. At the moment this needs compiling VirtualBox from sources, as the Oracle packages do not include it.

Step 1: Install Virtual box

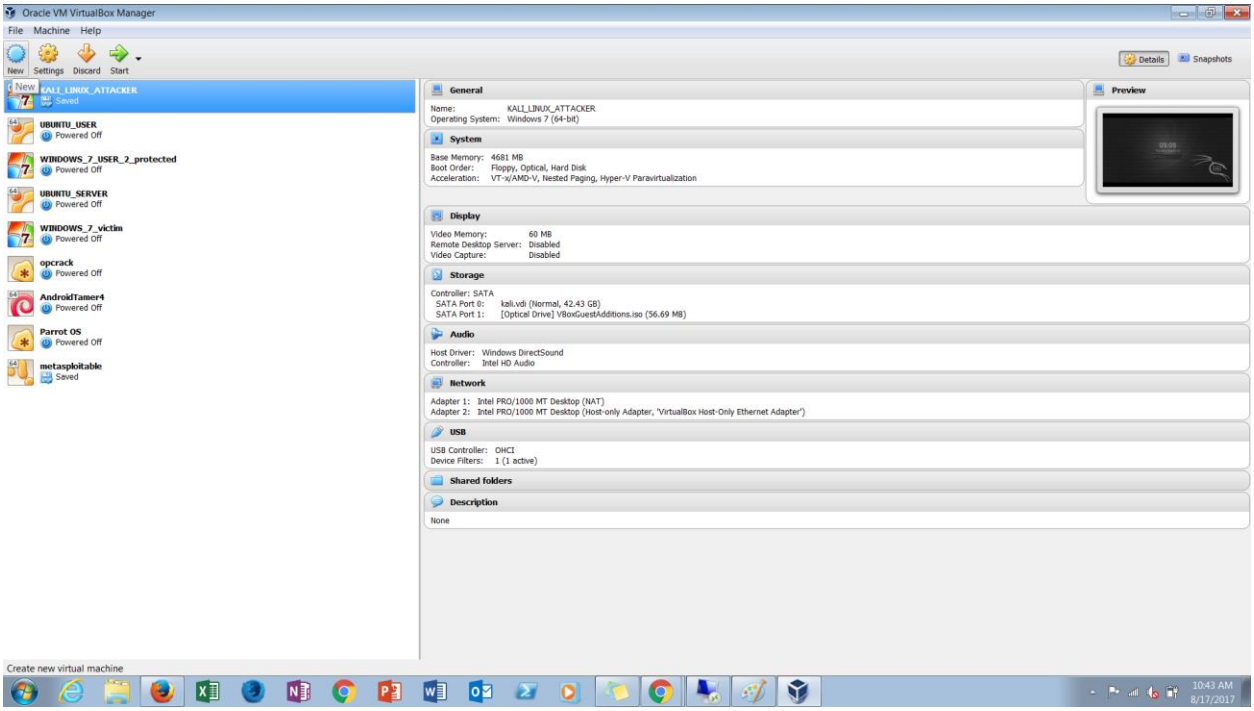
url: https://www.virtualbox.org/wiki/Downloads

Step 2: Installing Operating system which you prefer to in penetration test lab

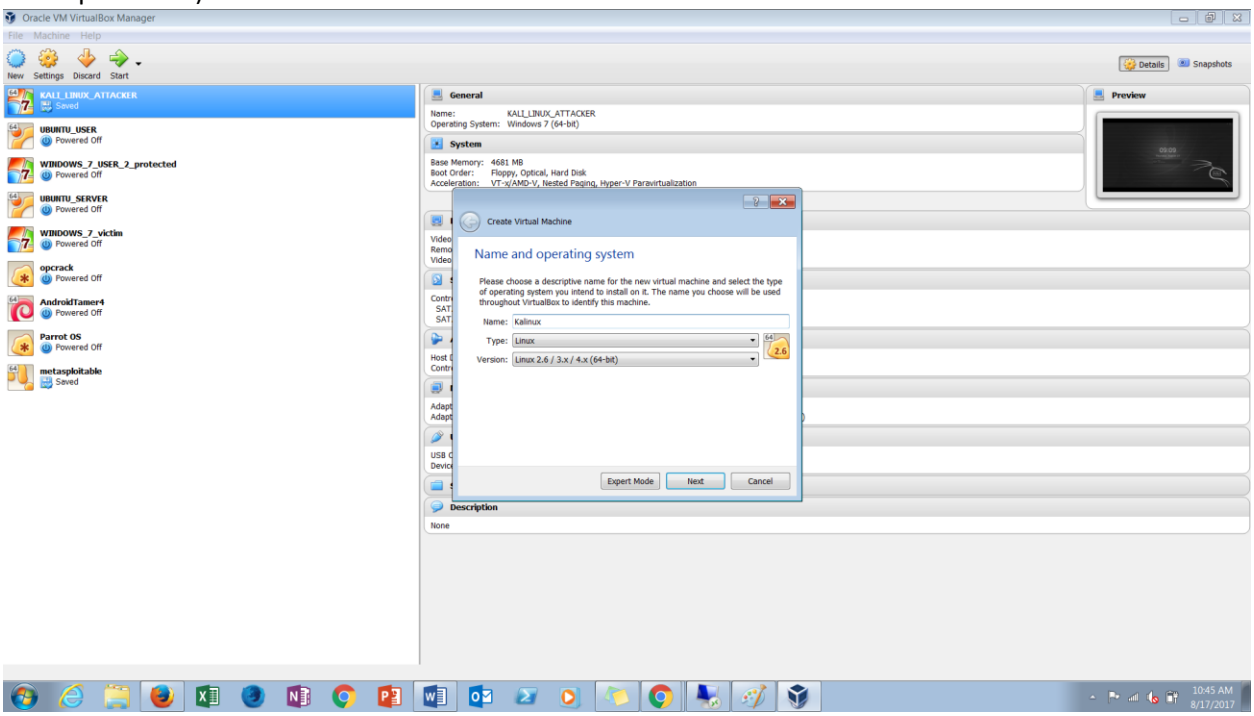
In our lab,we have Kali linux, Parrot os, Ubuntu desktop and server, windows 7, ophcrack (for password cracking), android tamer (for mobile application penetration test) and metasploitable (os with lot of vulnerabilities)

Installing Kali Linux in virtual box

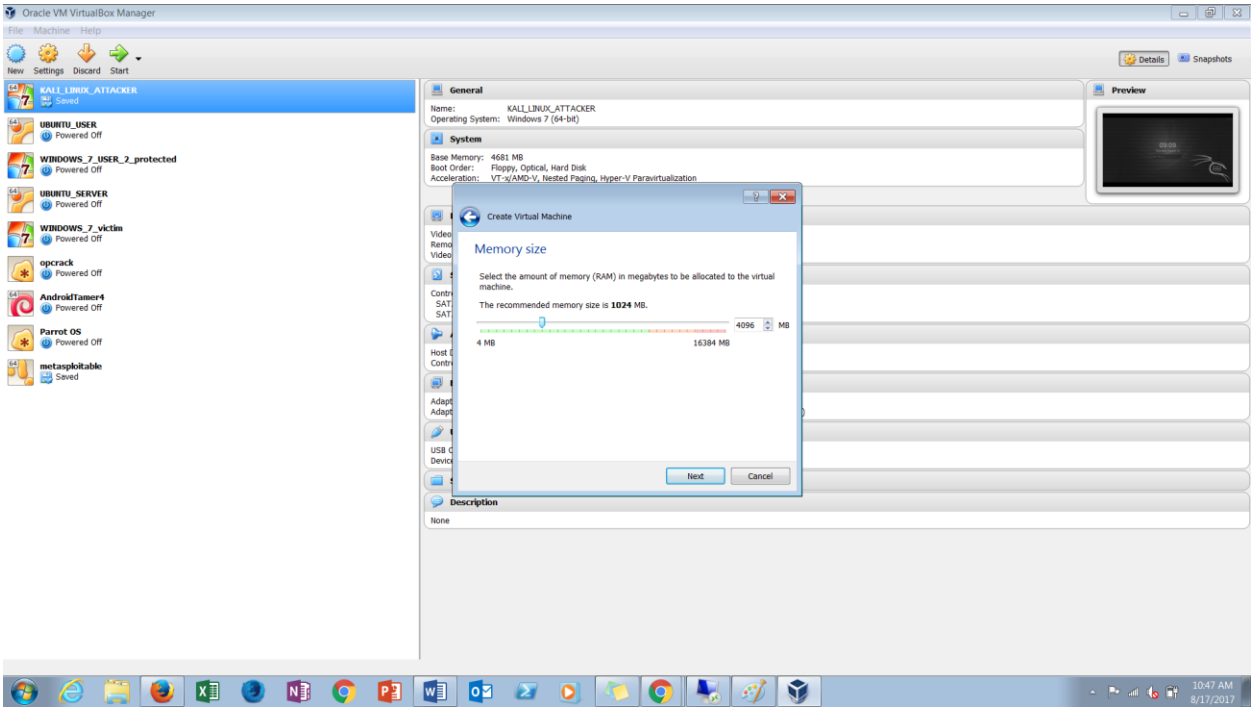
1. Download iso from url: https://www.kali.org/downloads/
2. Open virtual box => click on new



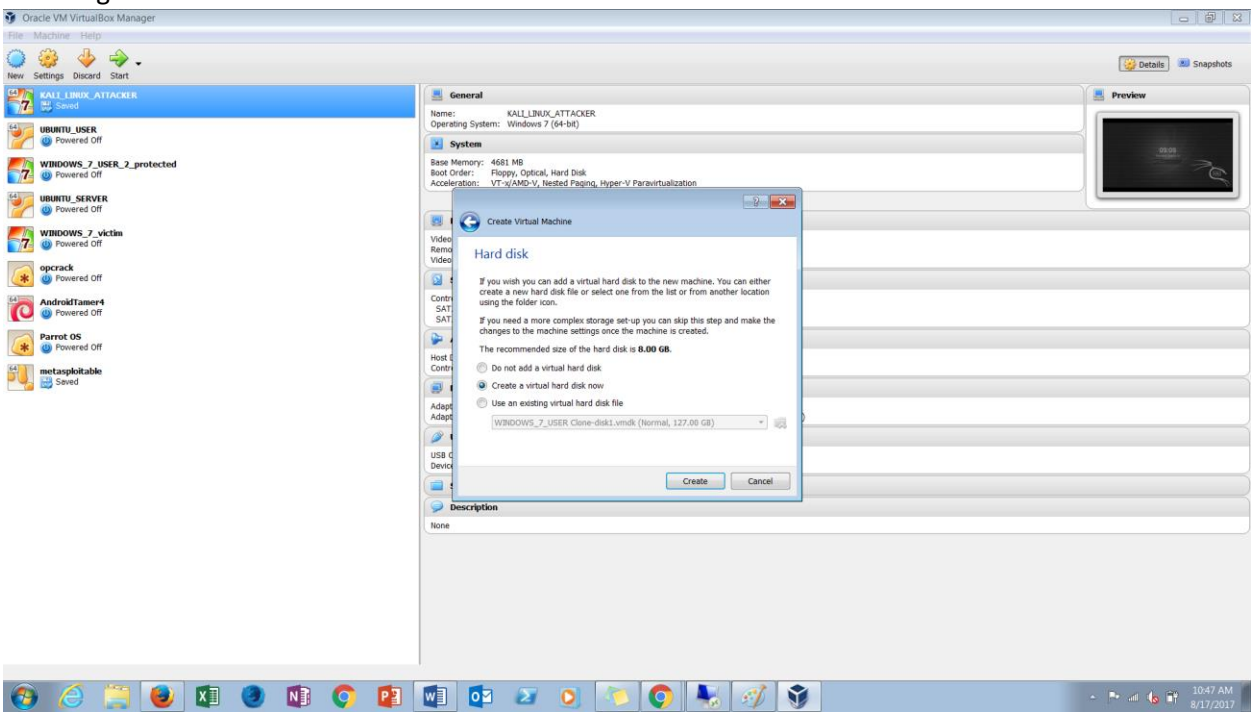
3. Give name to installing operating system, choose options according your hardware (32 bit and 64 bit processor)



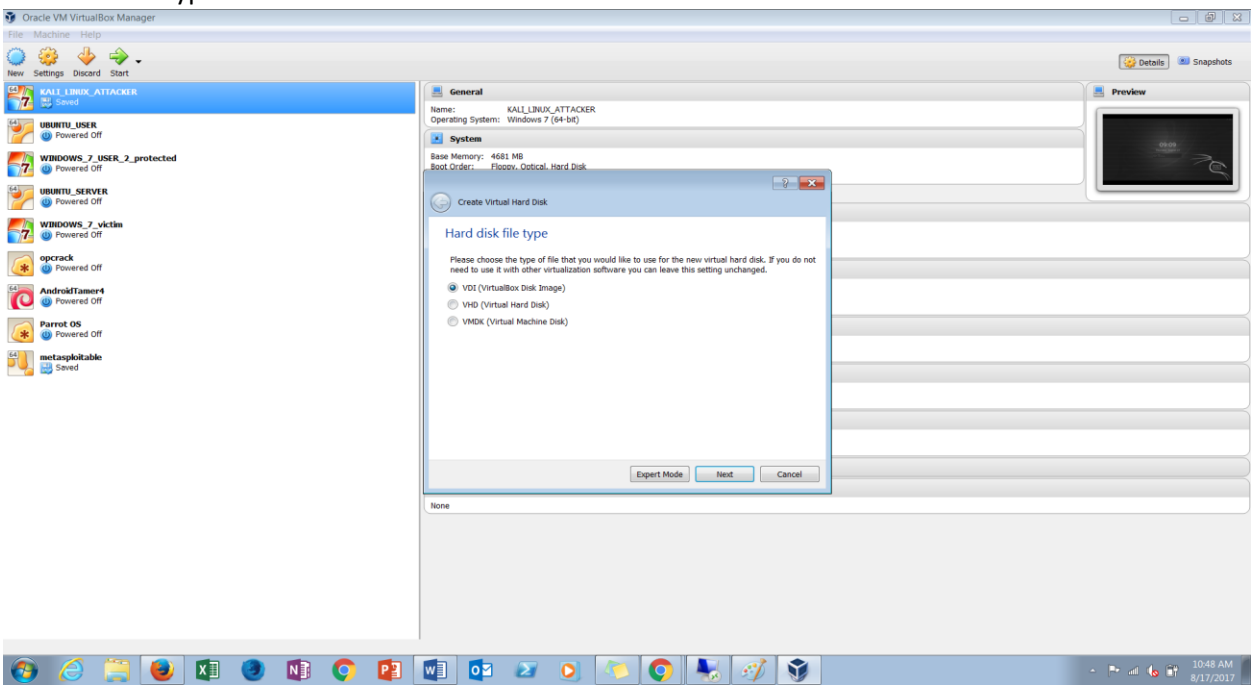
4. Select physical memory (RAM)



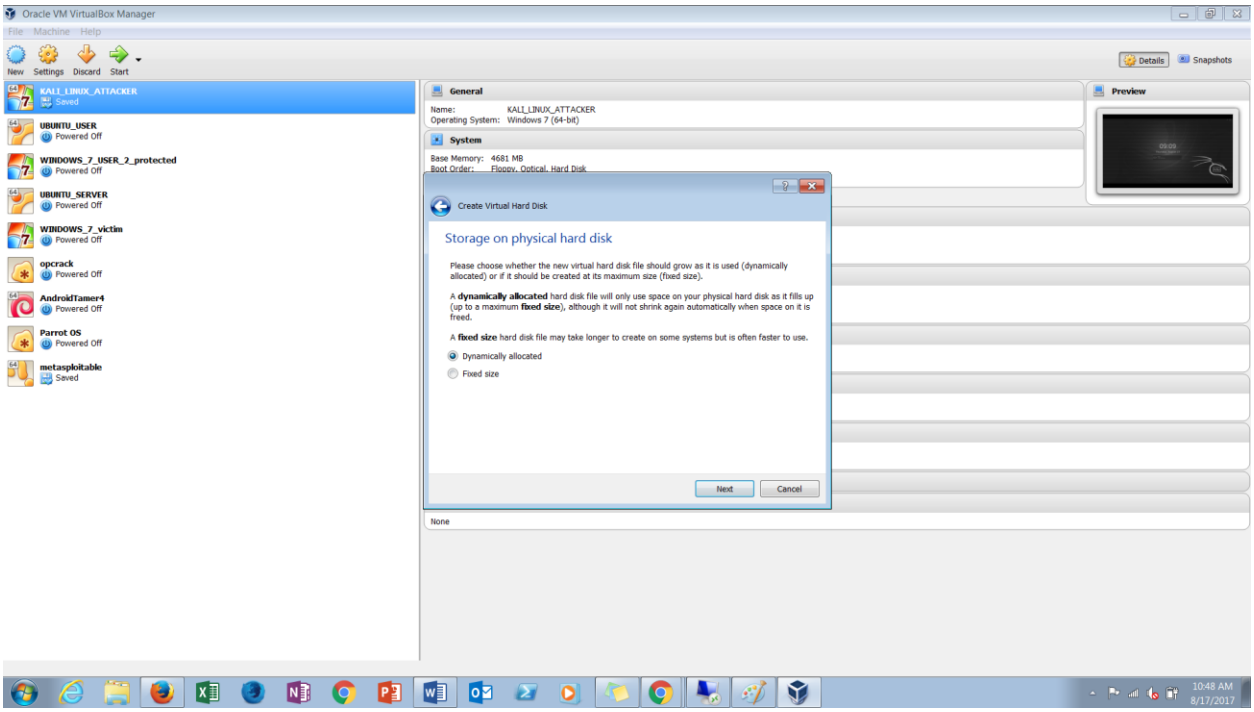
5. Creating virtual hard disk



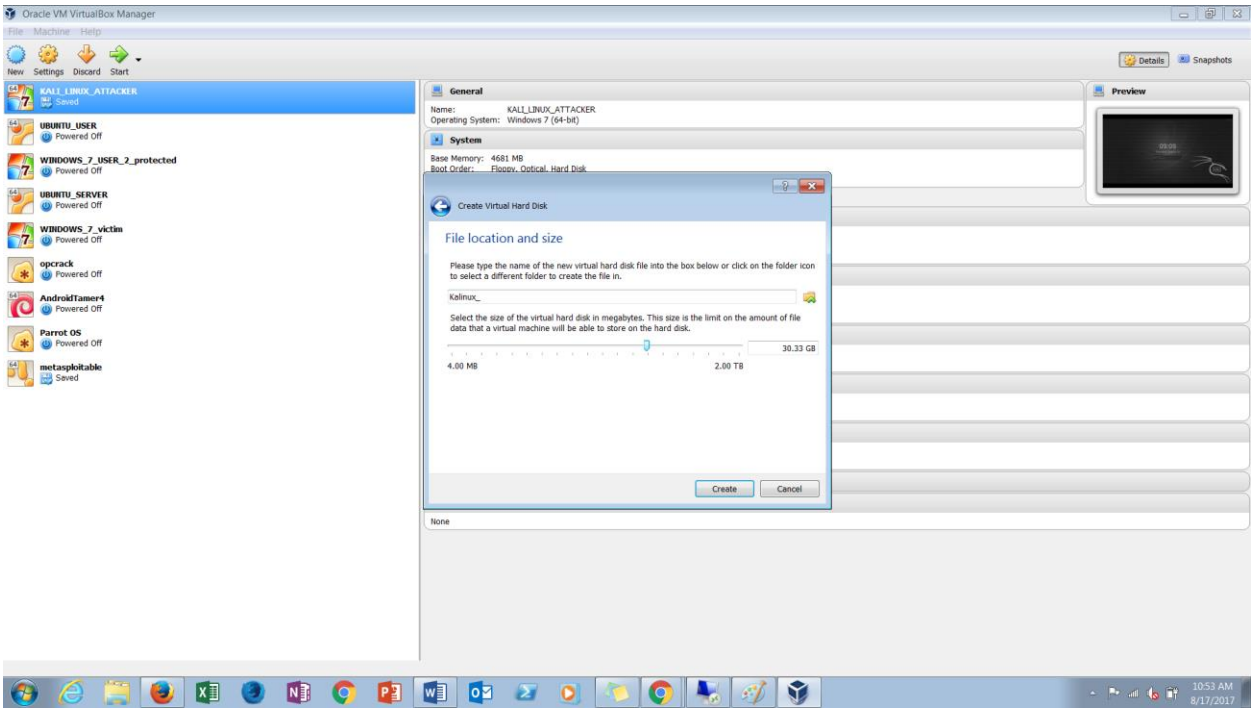
6. Hard disk file type VDI

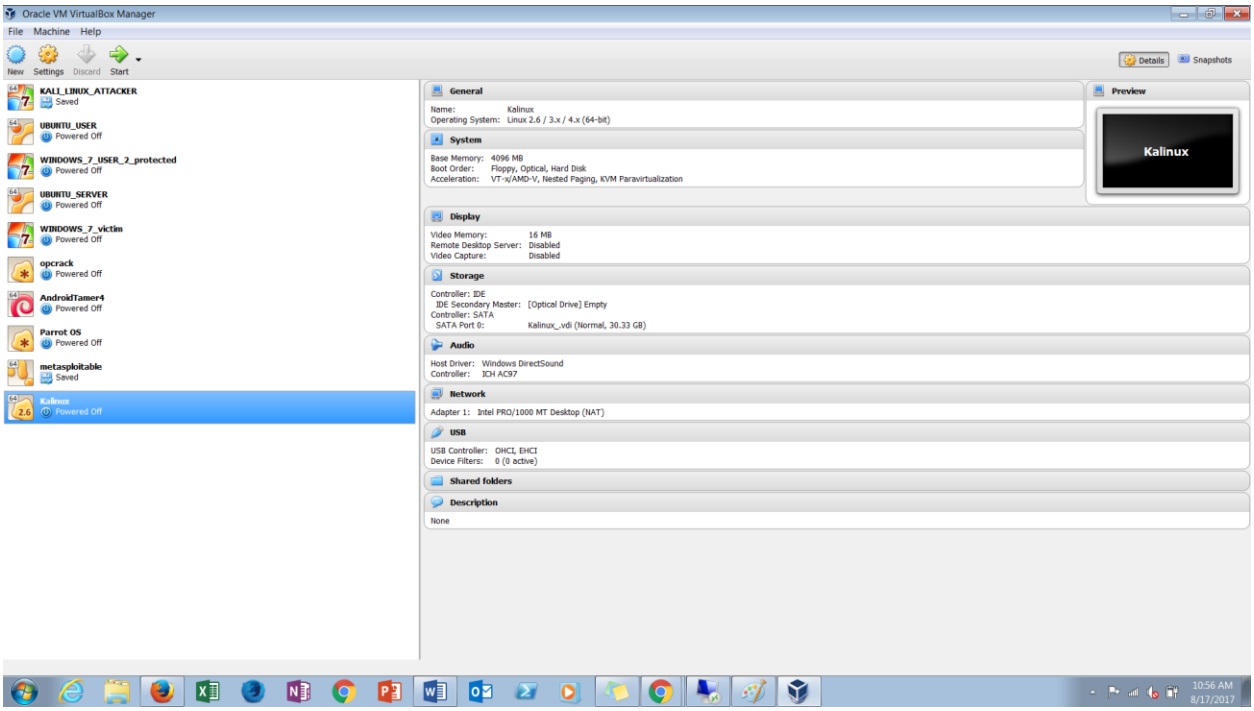


7. storage type dynamically allocated

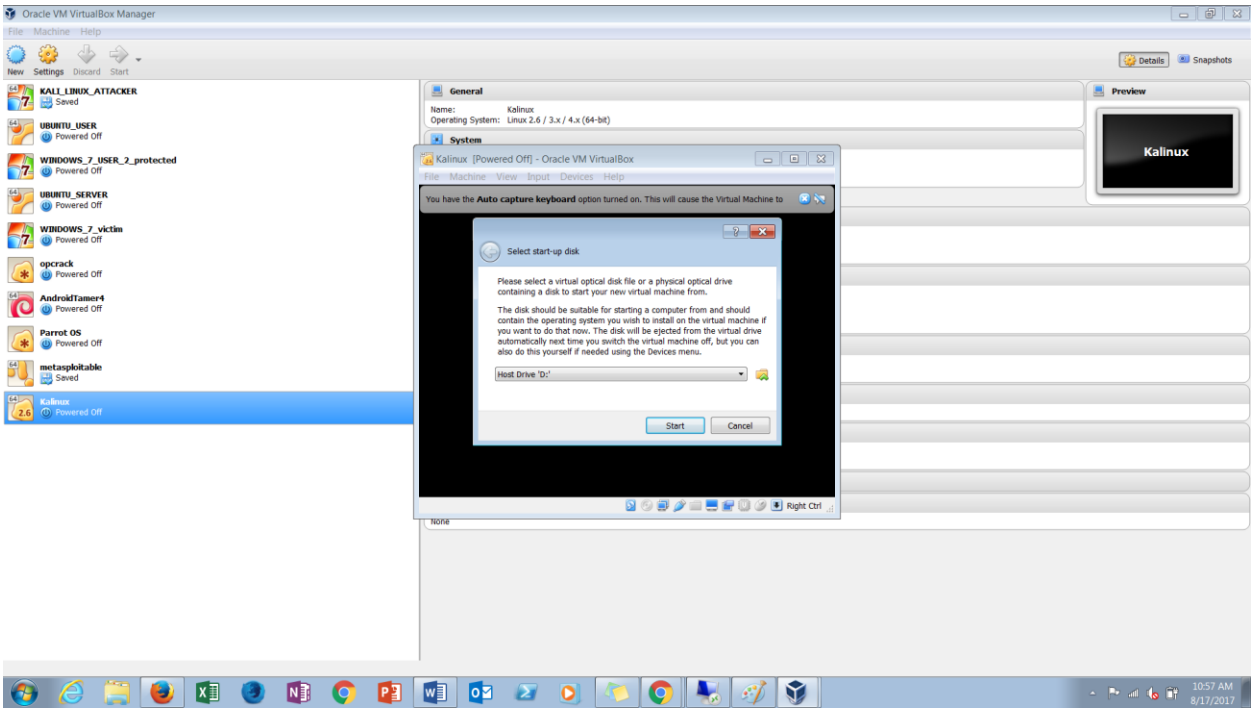


8. File location and size (choose more than 30 GB), click on create. Now we successfully created kali instance in Virtual Box

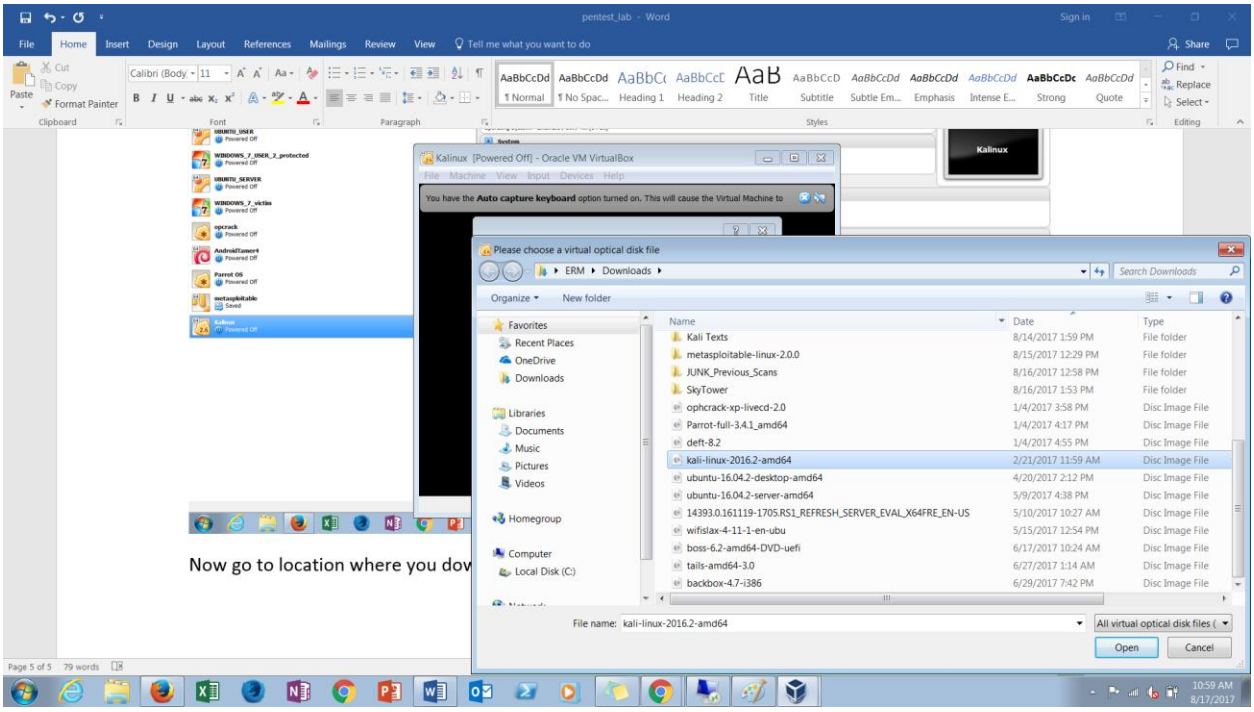




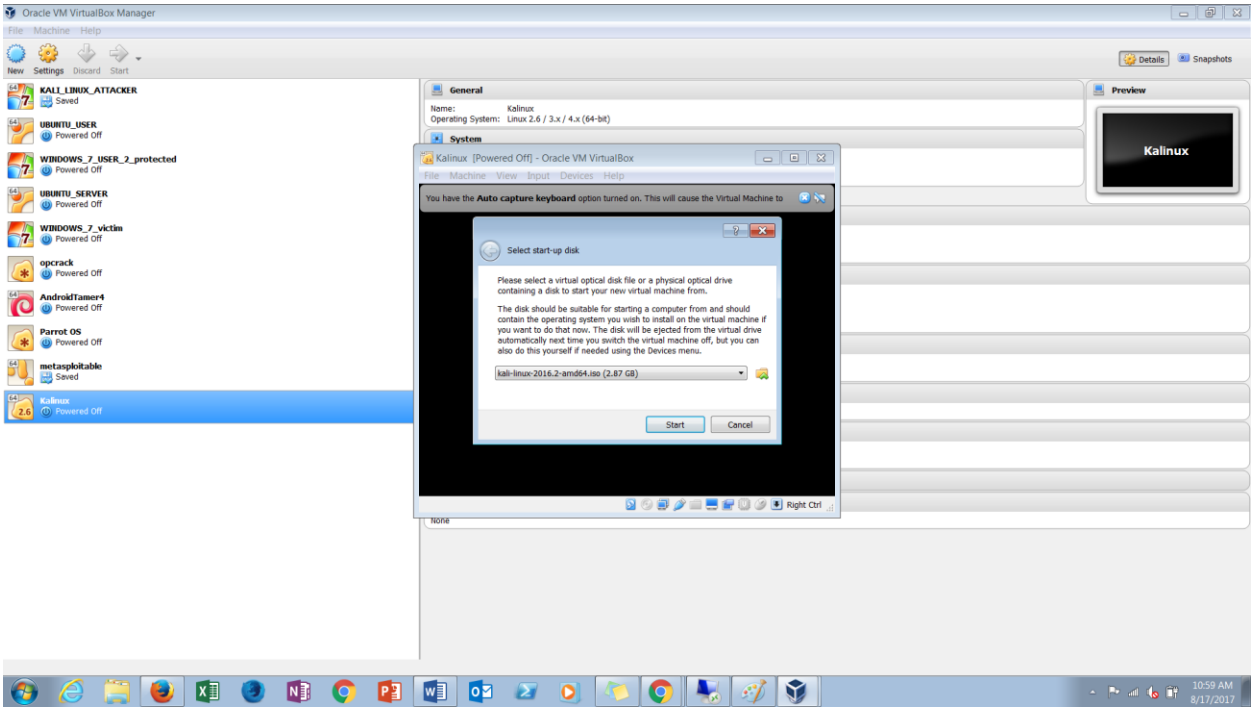
9. Click on created instance, press start button



10. Now go to location where you downloaded kali Linux iso

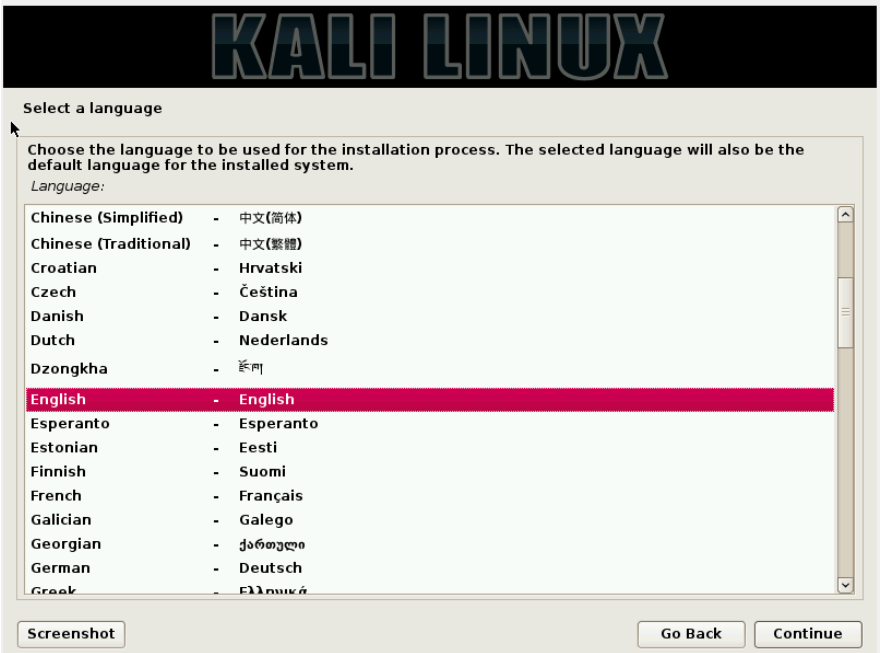


And select it

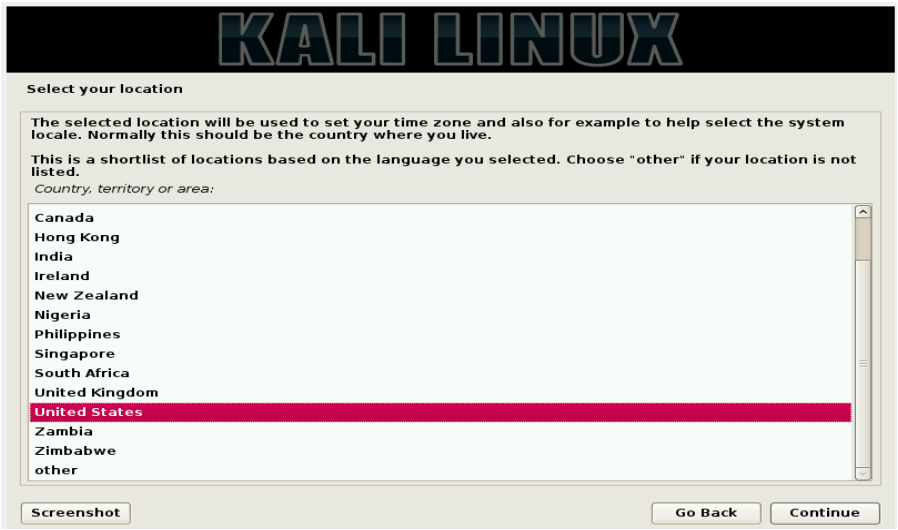


11. And click on start and choose graphical installation

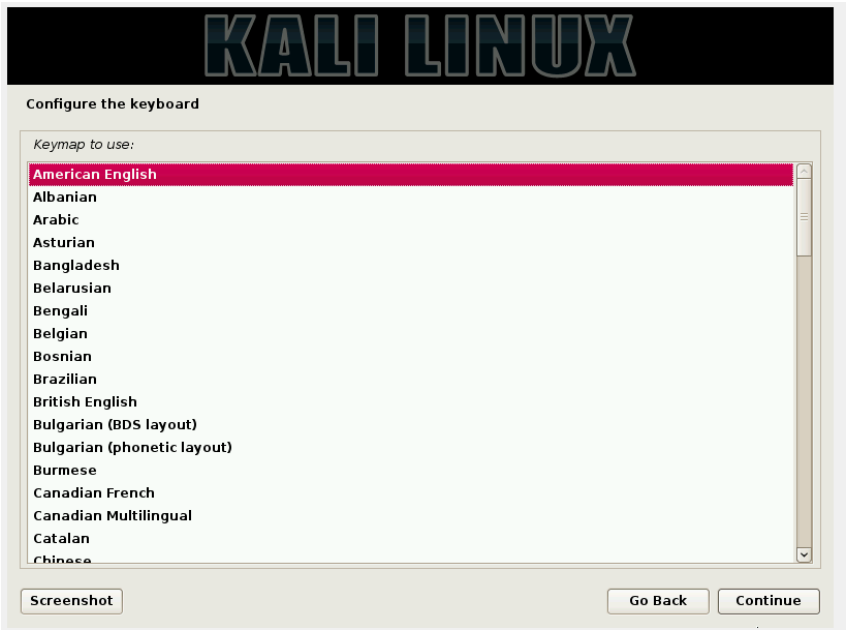
12. Select language



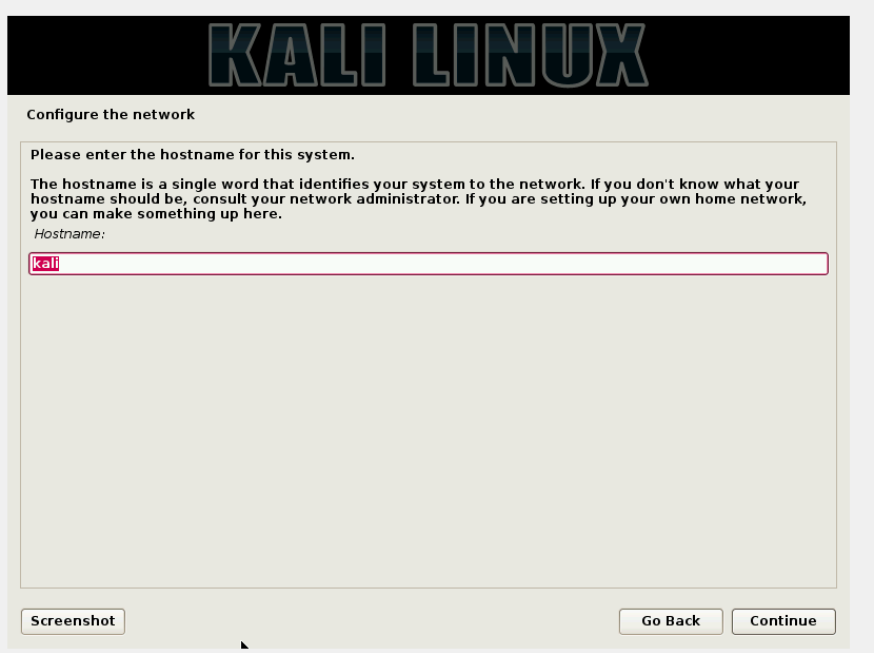
13. Location



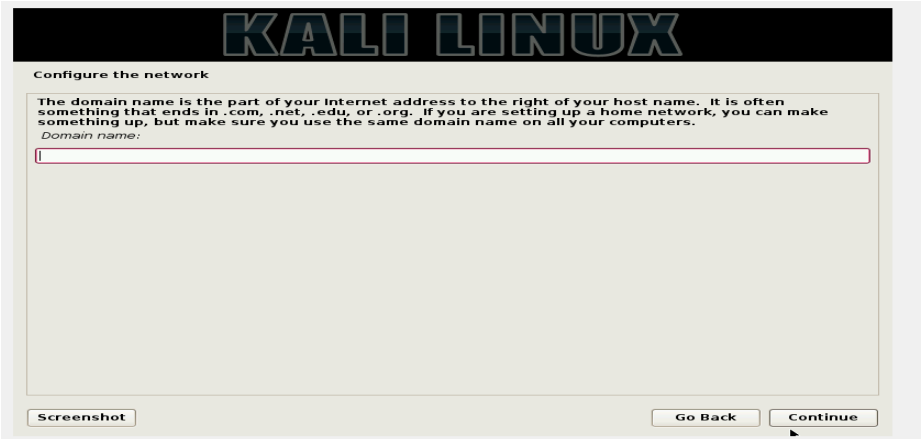
14. Keyboard configuration



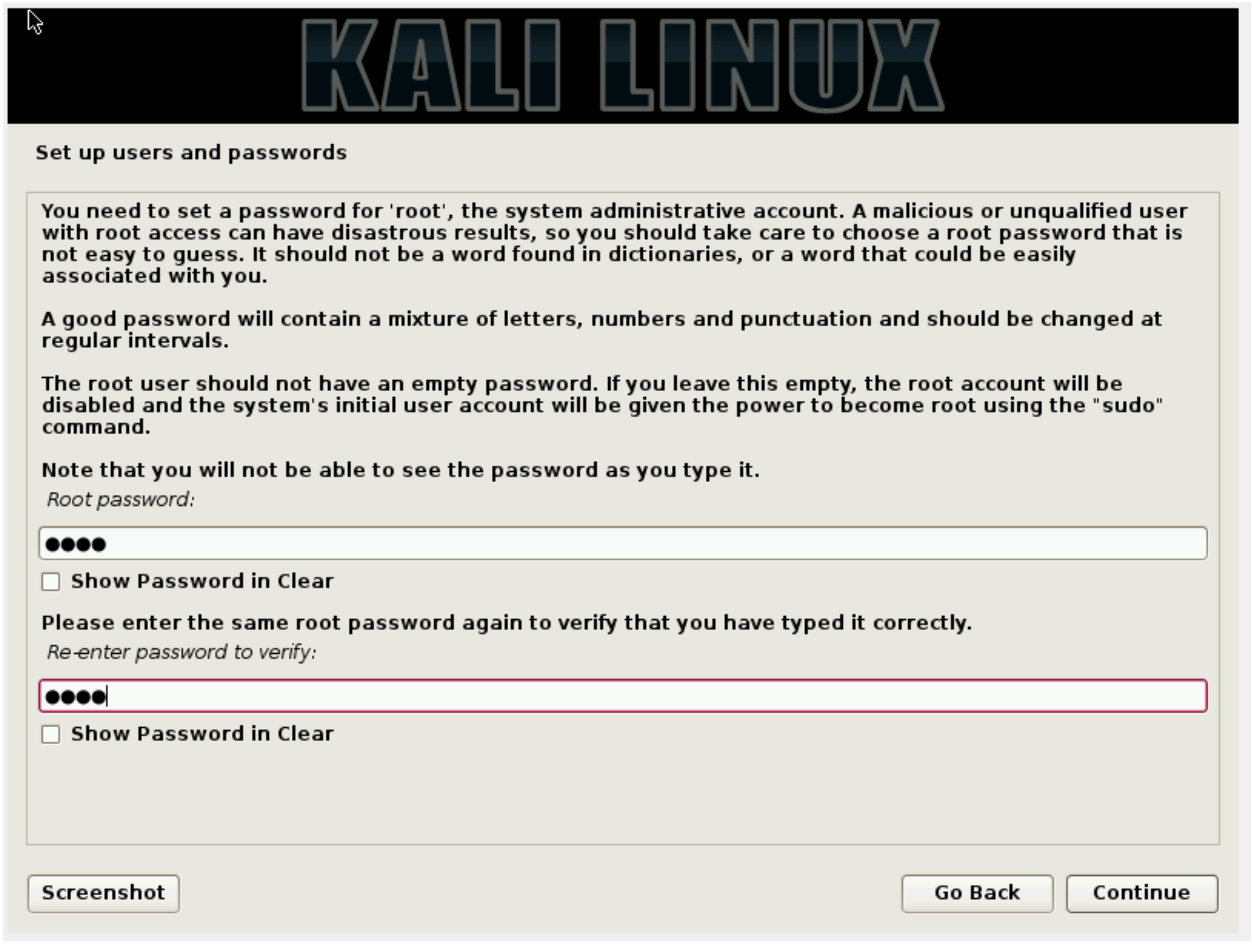
15. Choose Host Name:



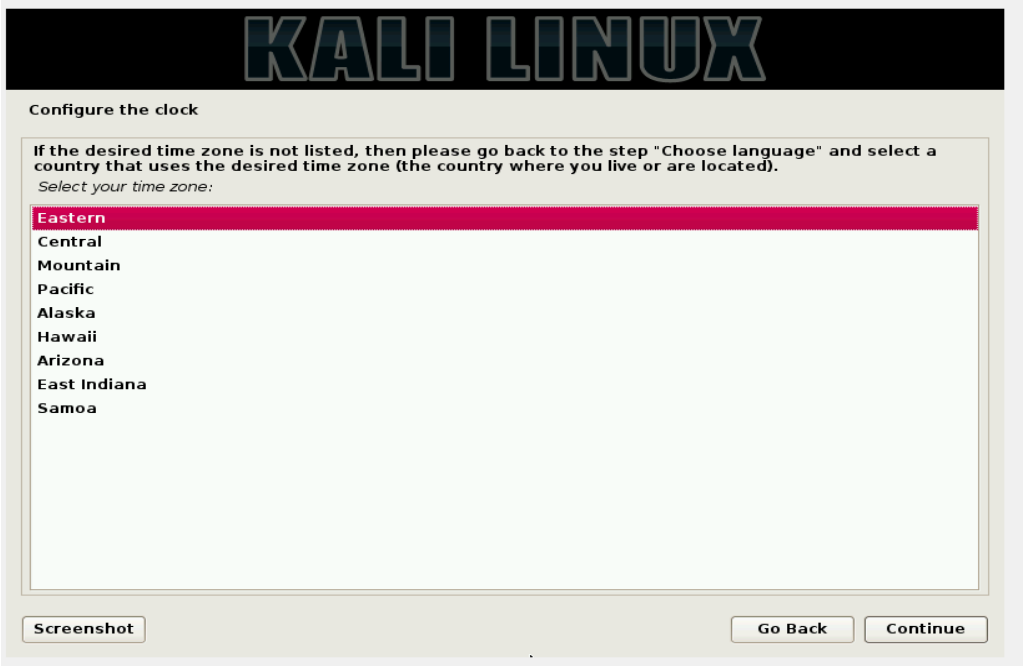
16. You can leave domain name, click next



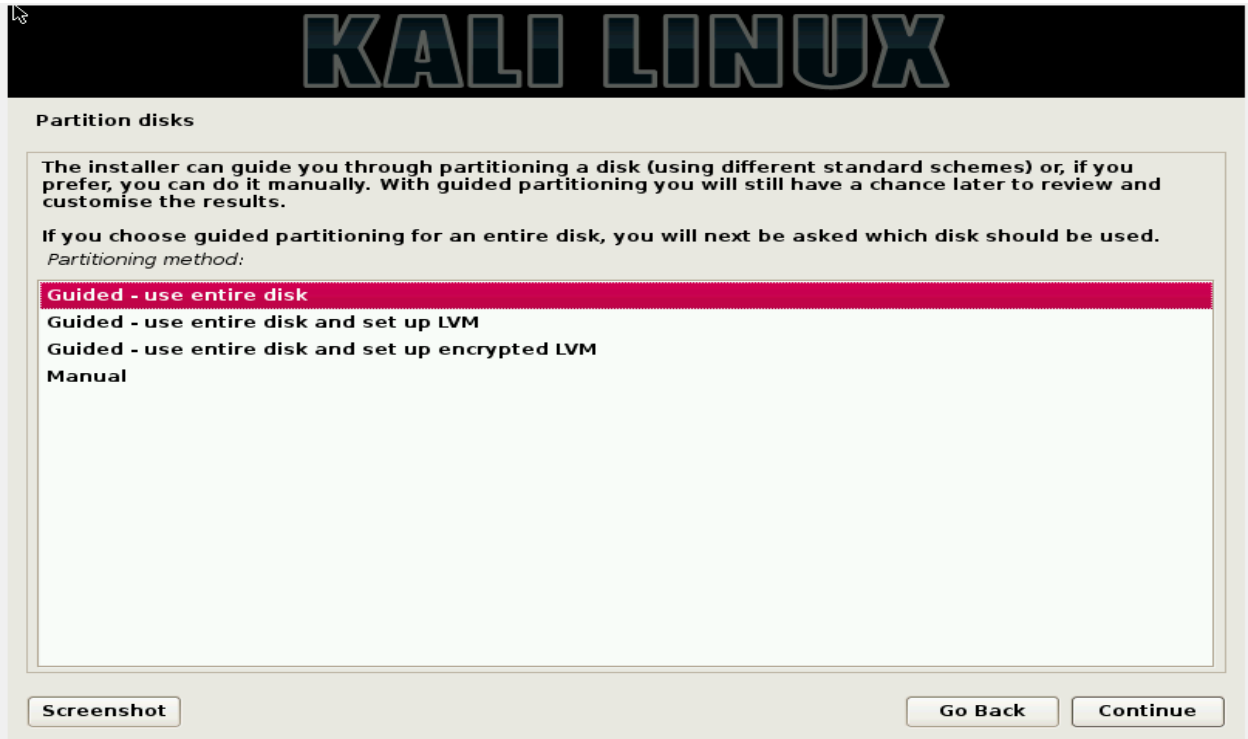
17. User password (by default you are root user)

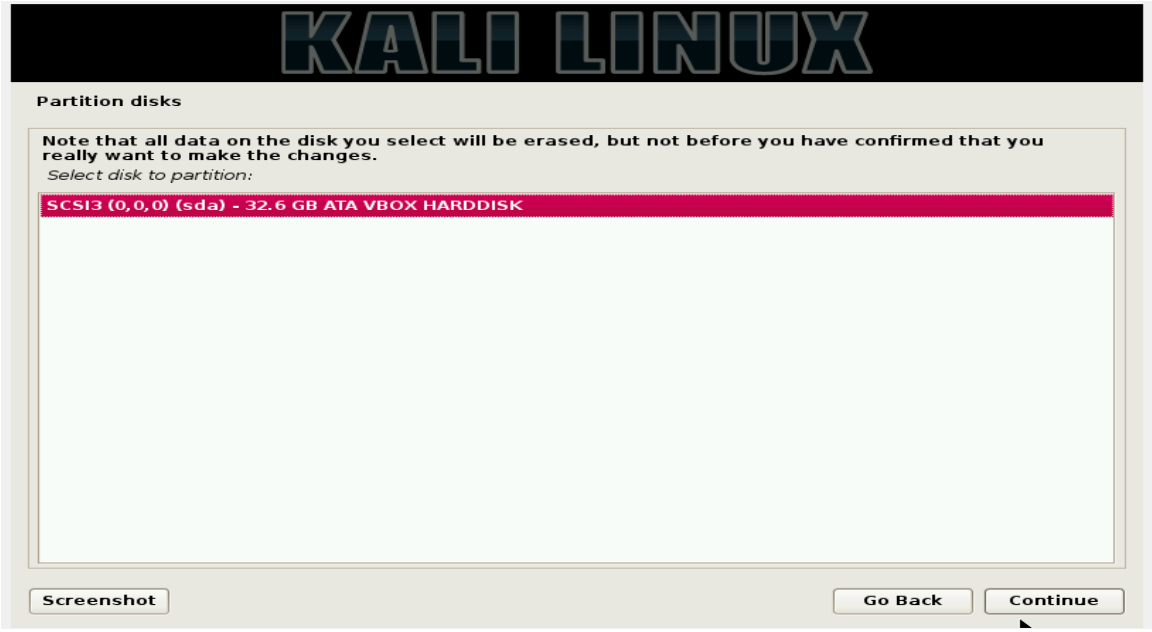


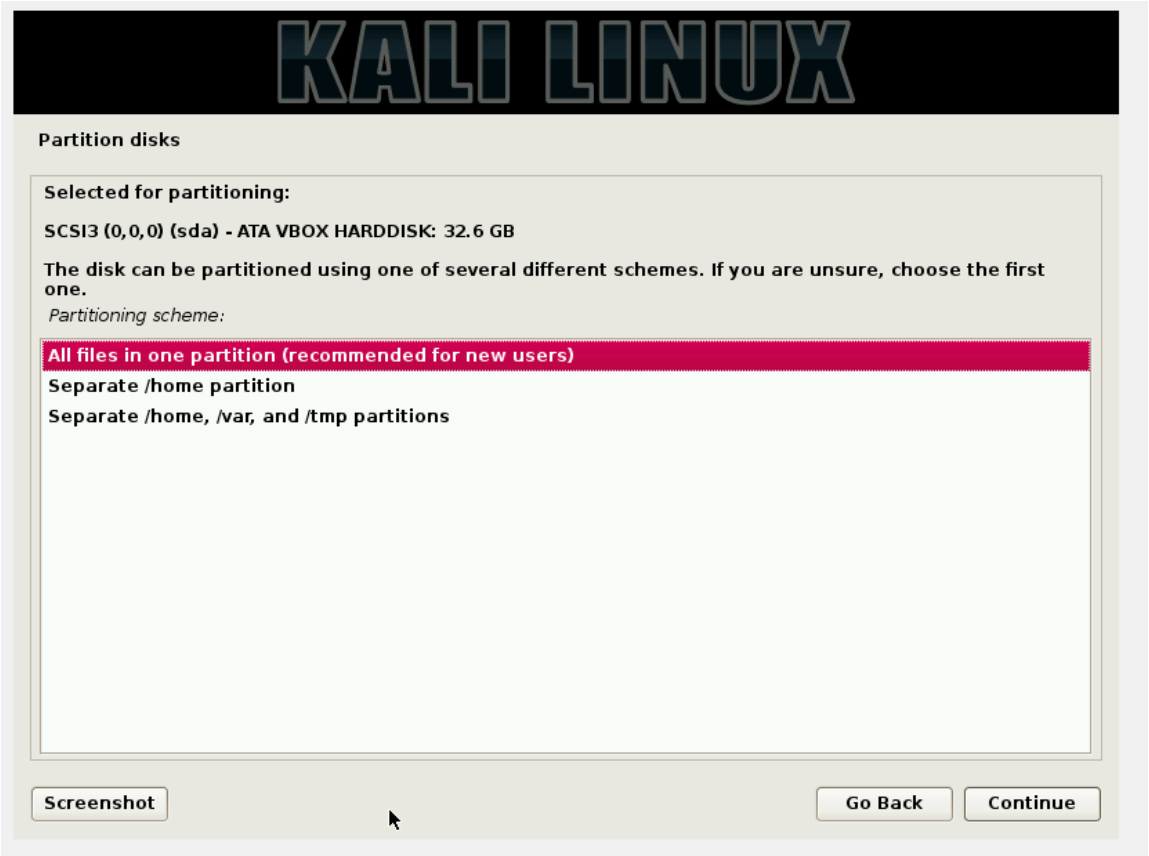
18. Clock

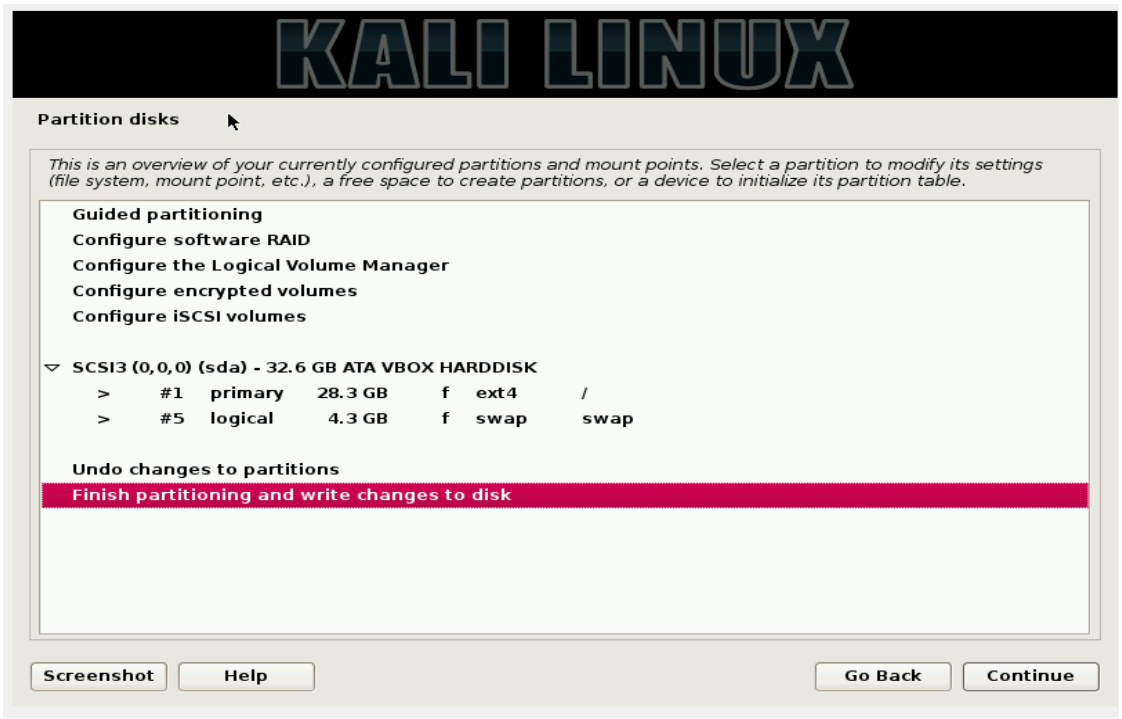


19. Disk Partition

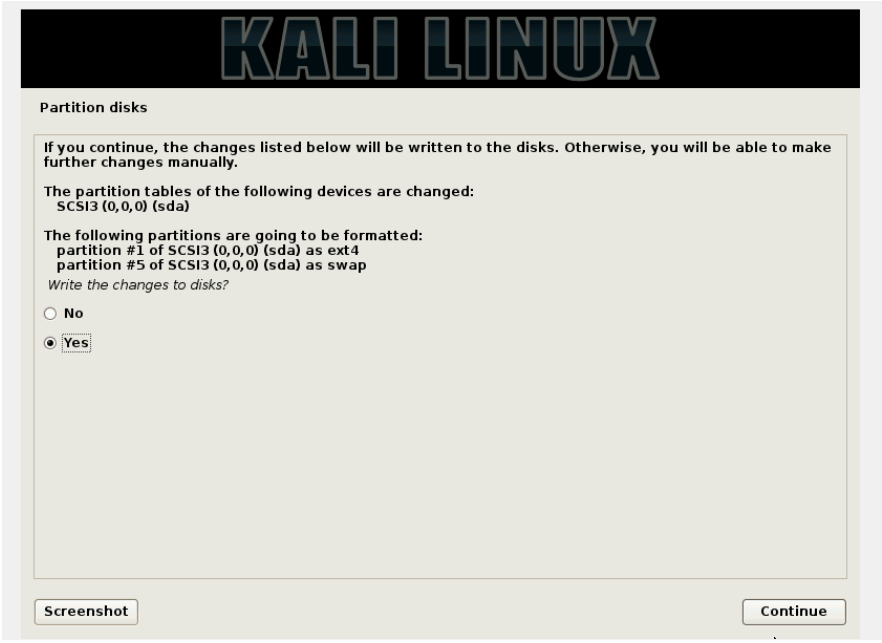


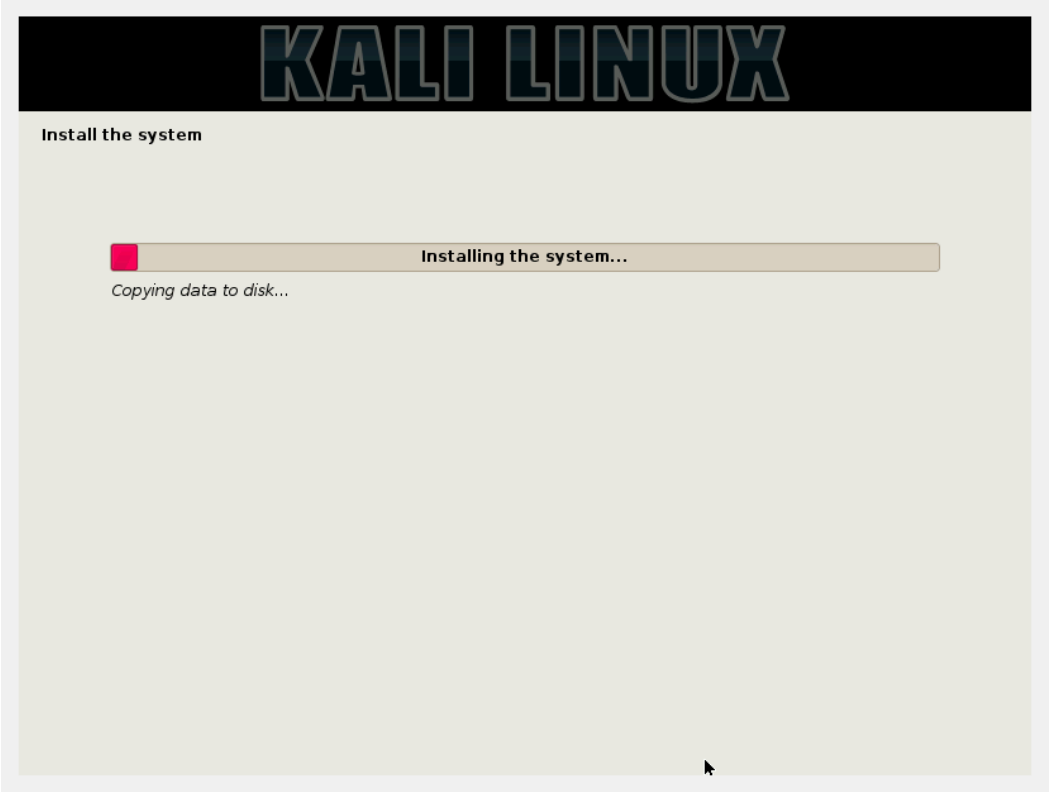

KALI LINUX
Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI3 (0,0,0) (sda) - 32.6 GB ATA VBOX HARDDISK
Screenshot
Go Back
Continue


KALI LINUX
Partition disks
Selected for partitioning:
SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 32.6 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
Screenshot
Go Back
Continue

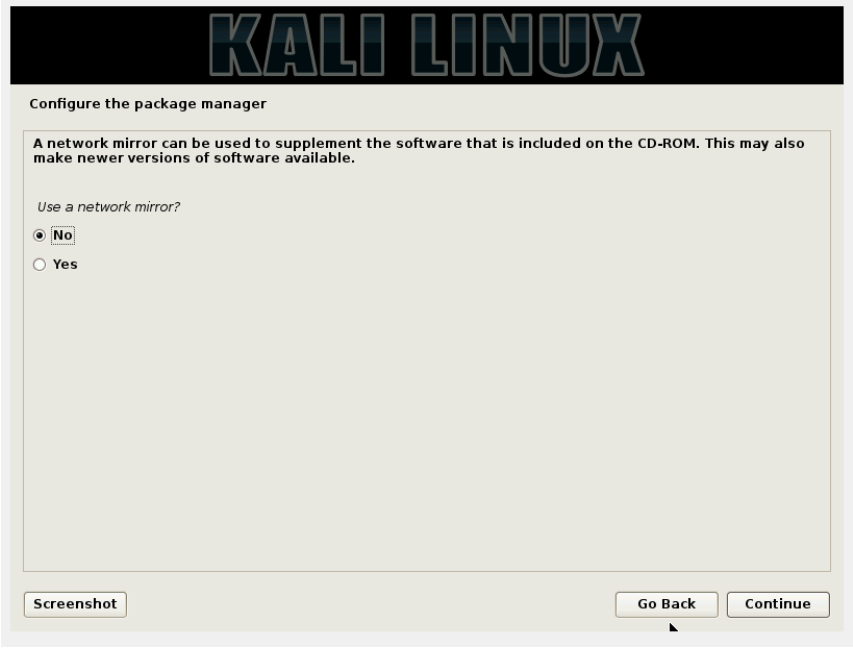


20. Select ‘yes’, to keep changes

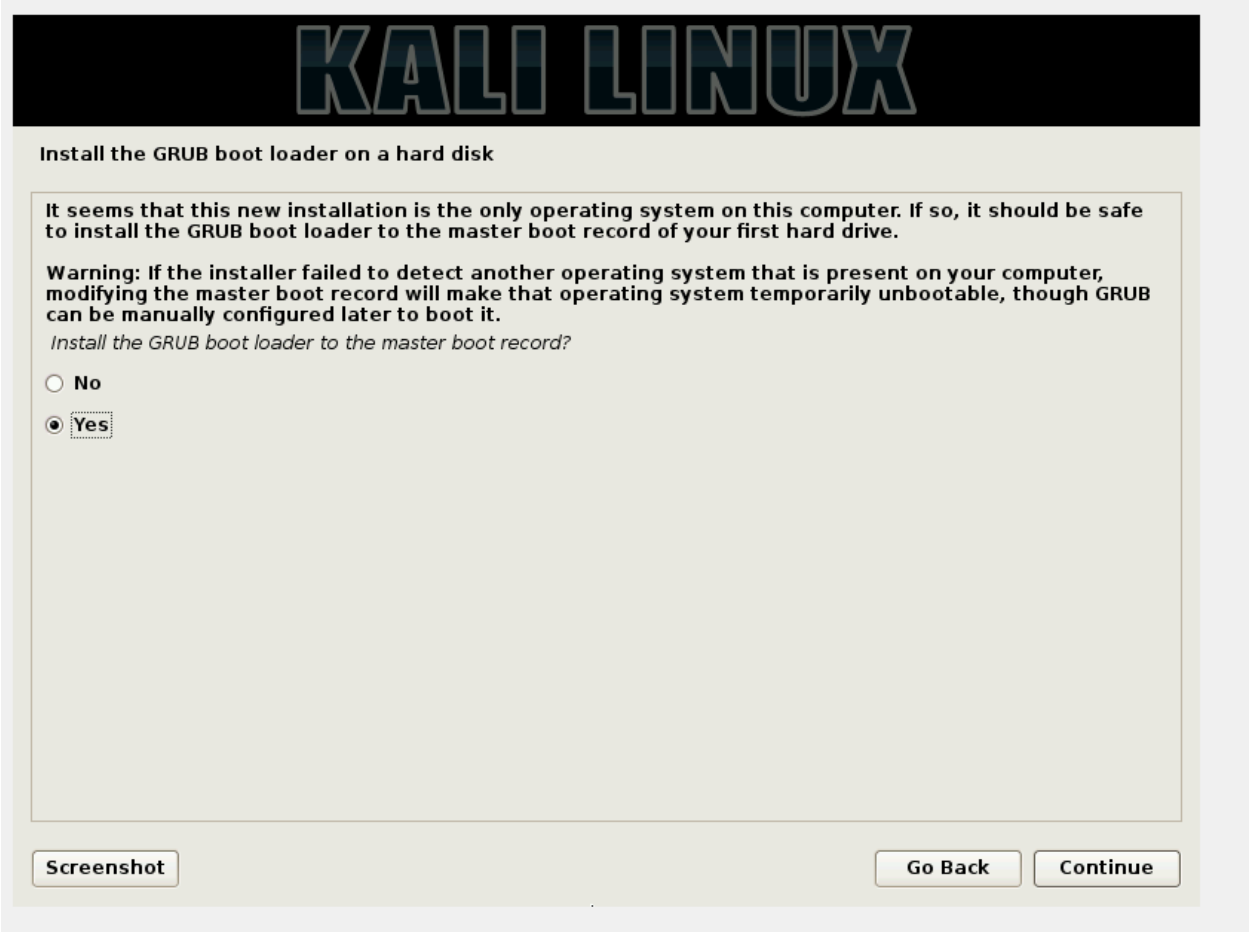




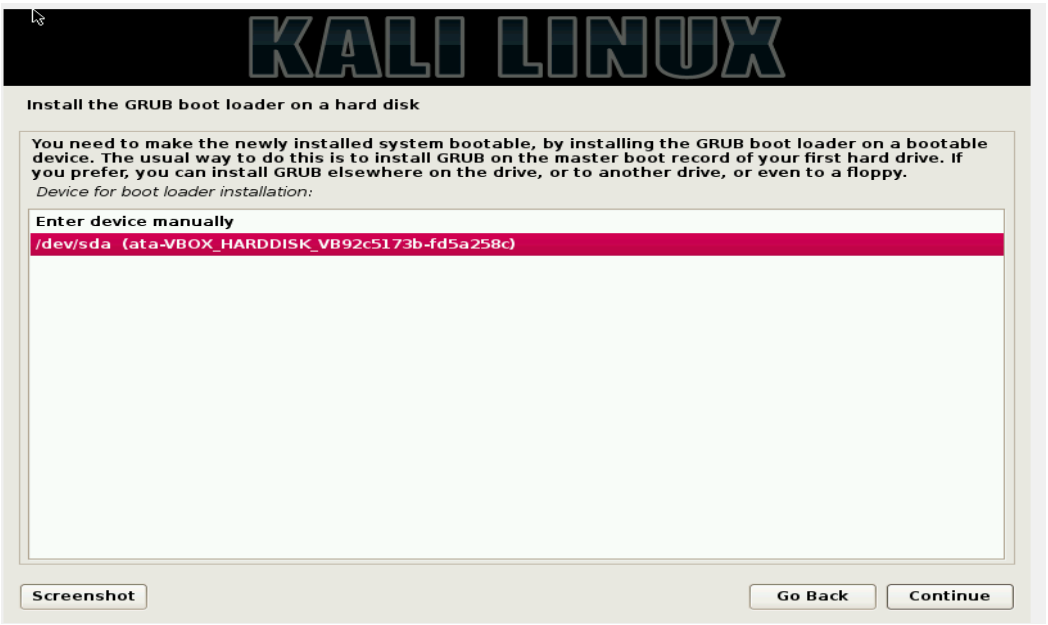
21. Select ‘no’ for network mirror



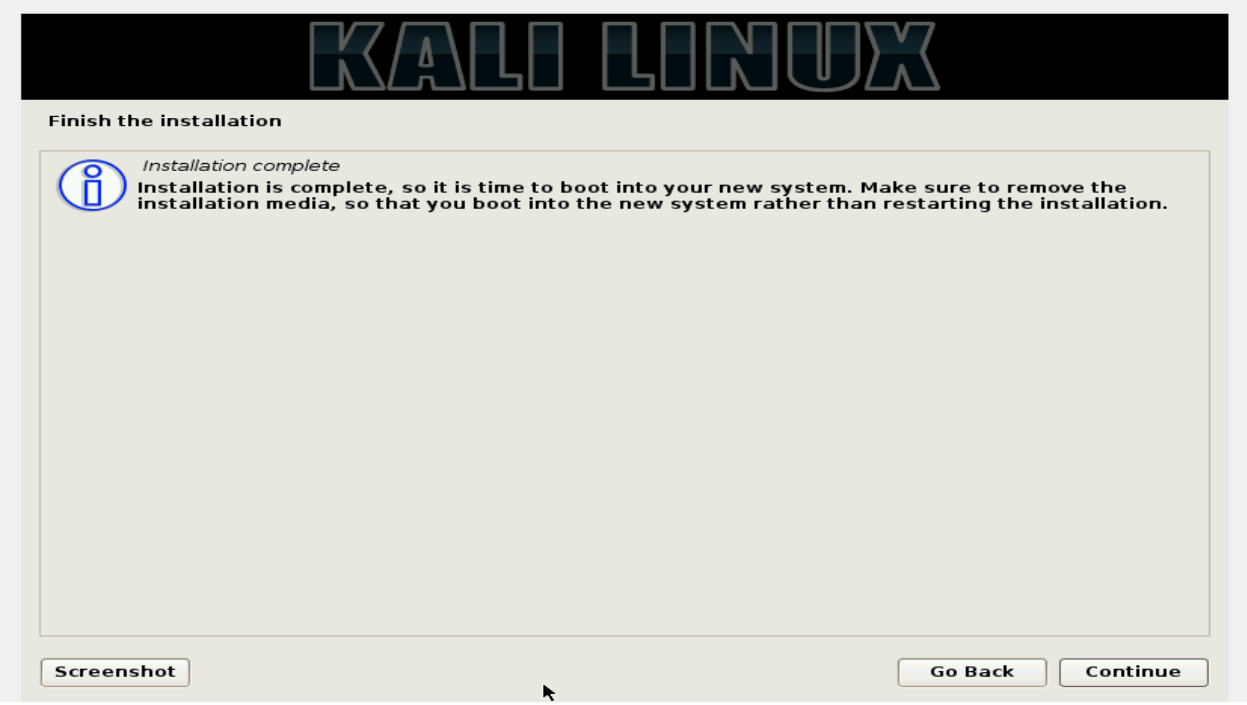
22. Press ‘yes’

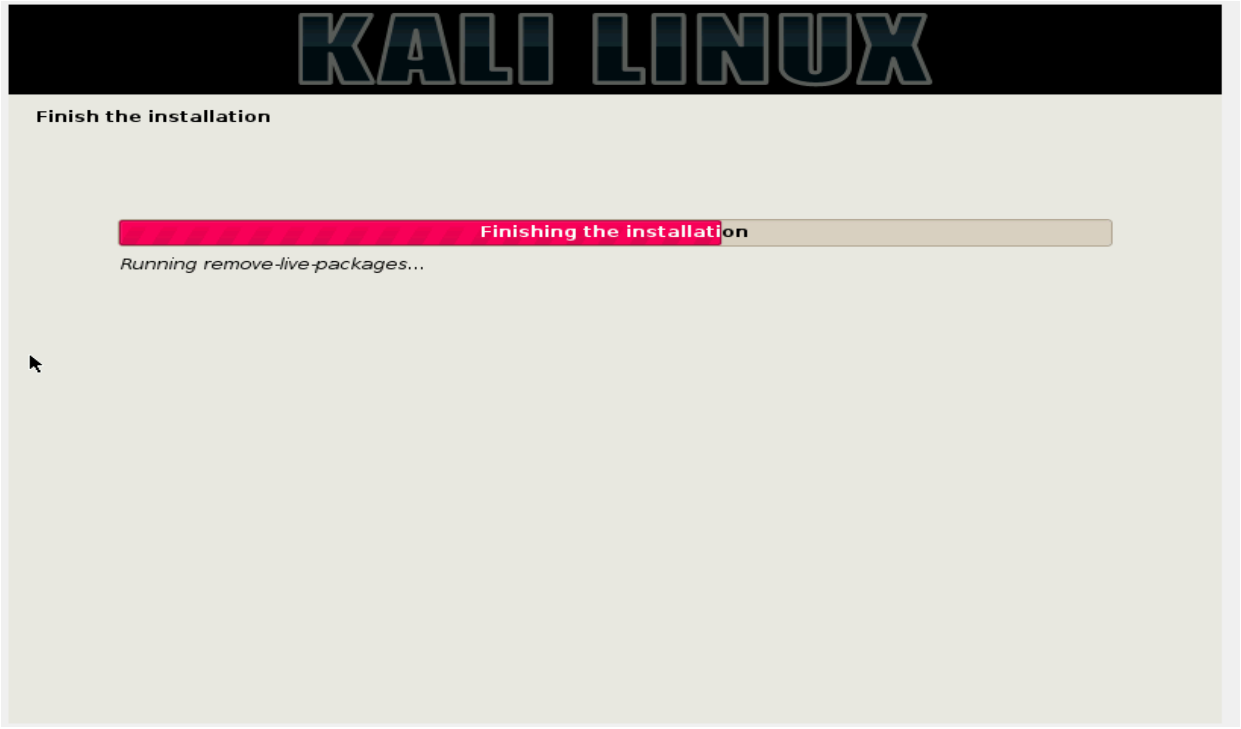


24. Select /dev/sda



25. Finally, installation completed

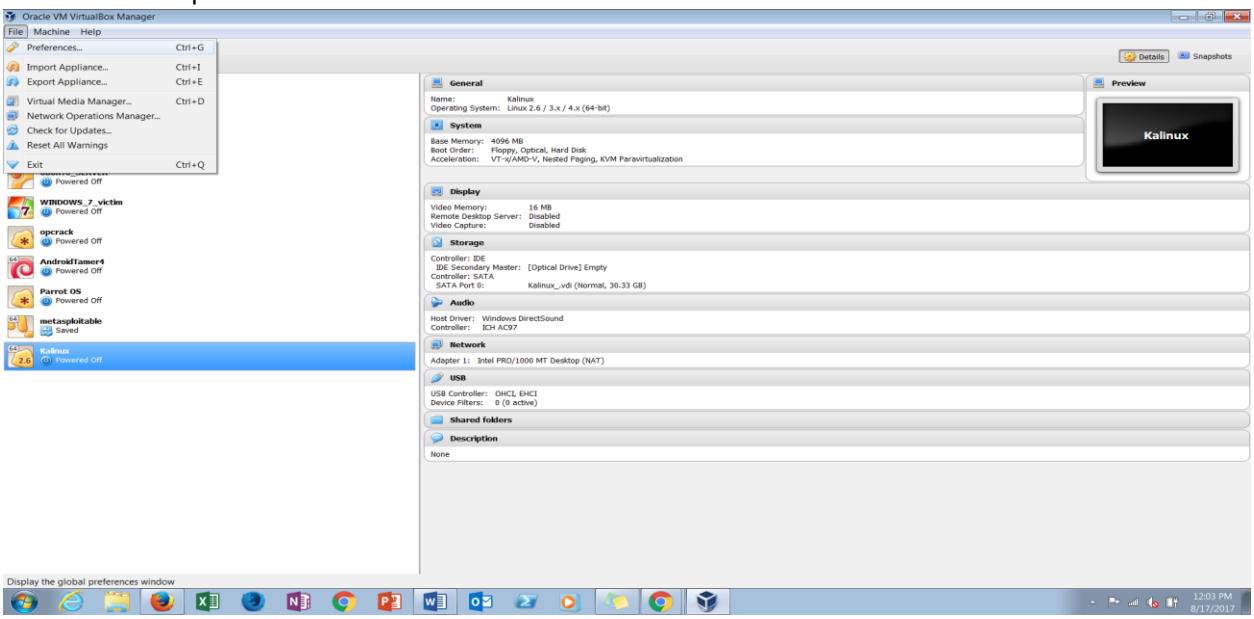




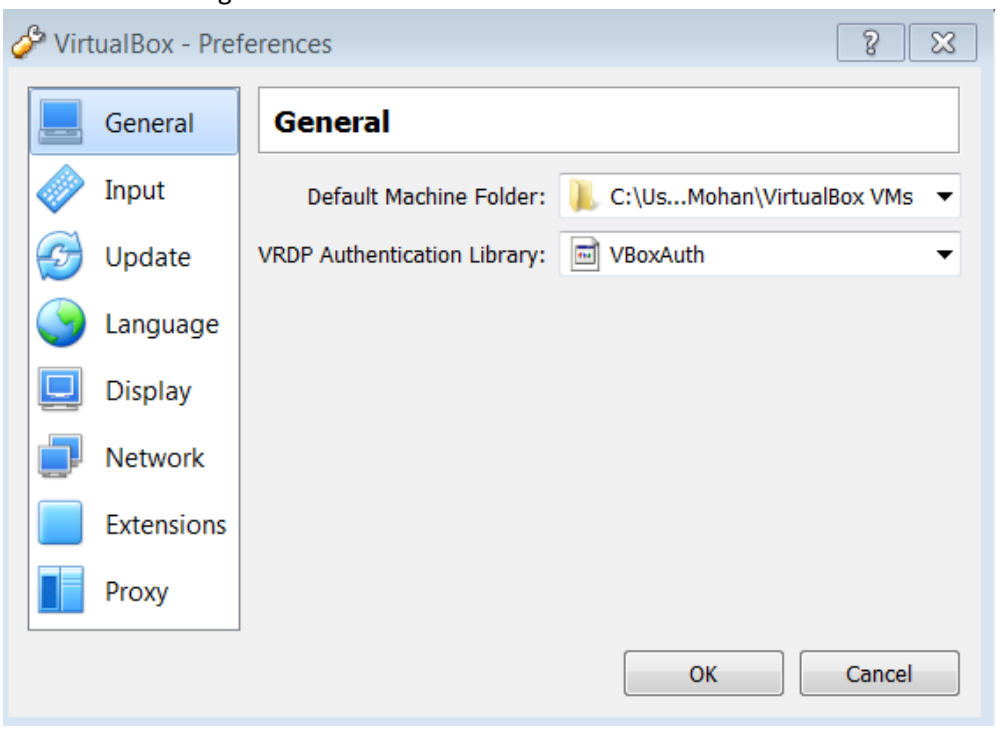
Step 3: Network settings

Now, we are configuring host only settings,

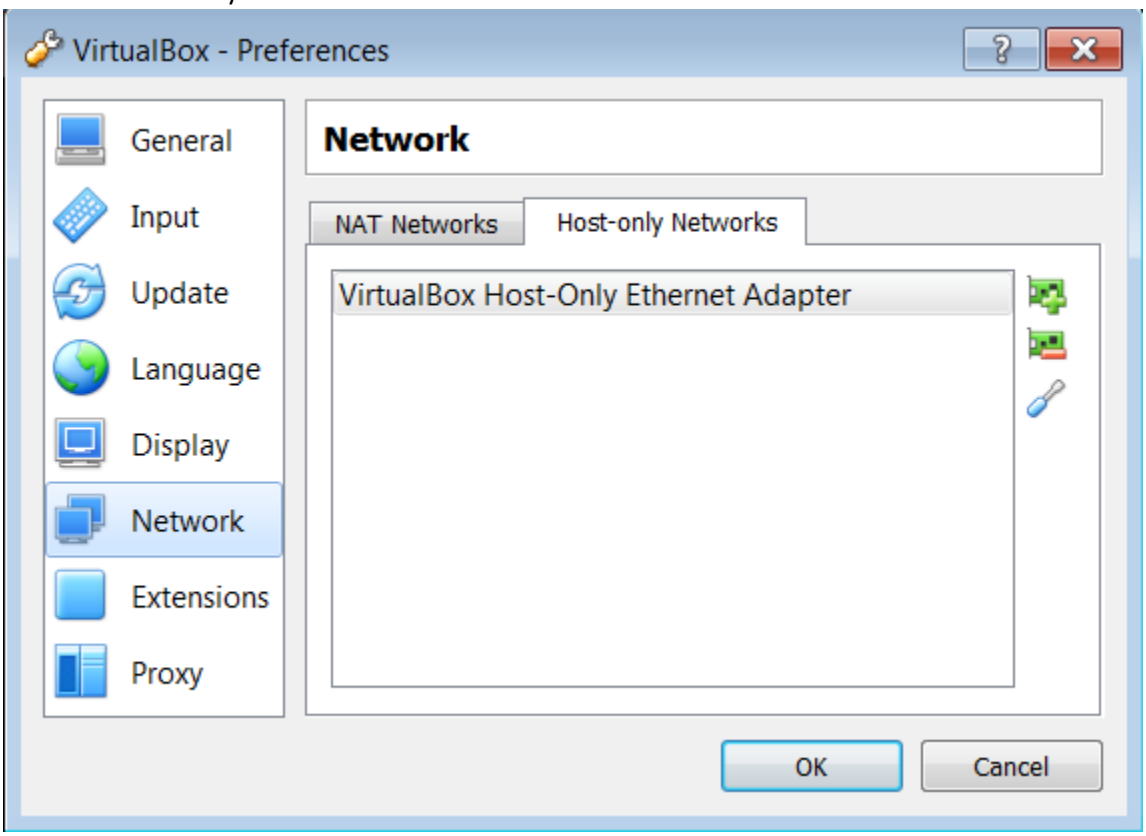
1. Goto file -> preferences



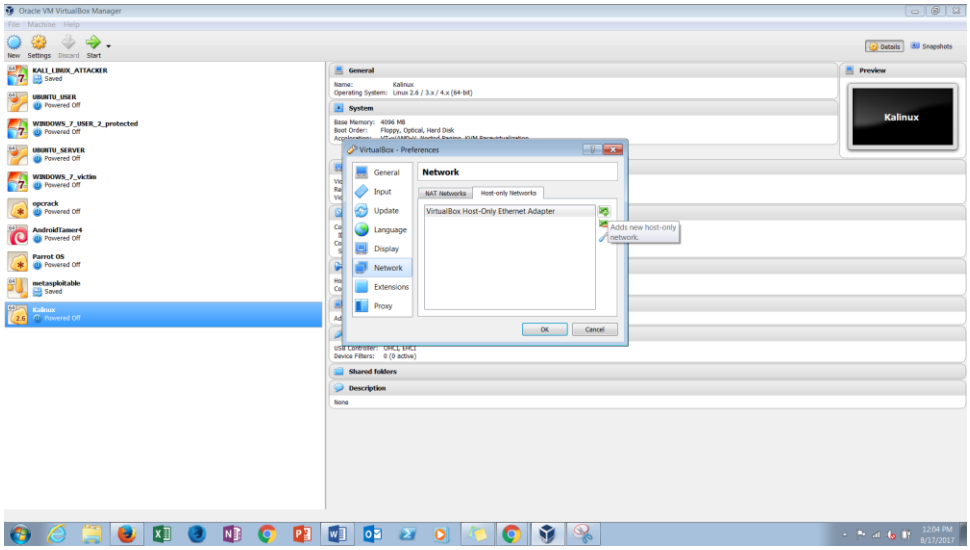
2. Click on settings

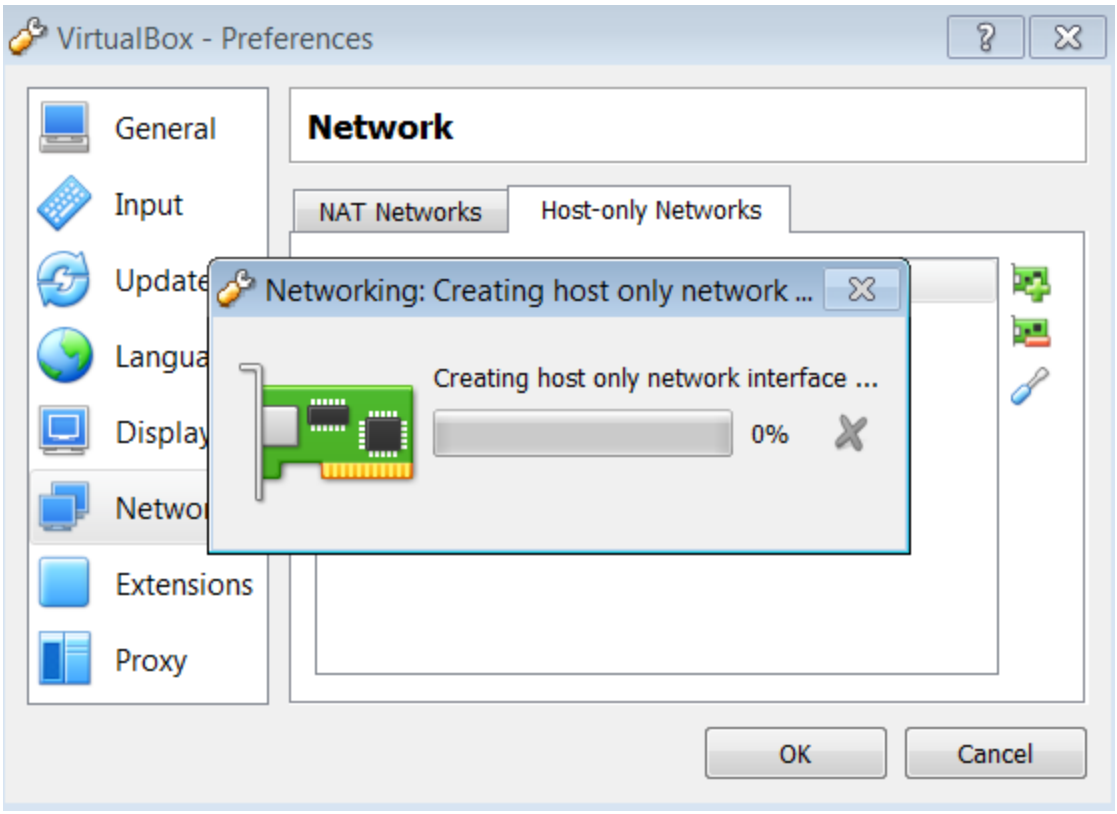


3. Select host only network

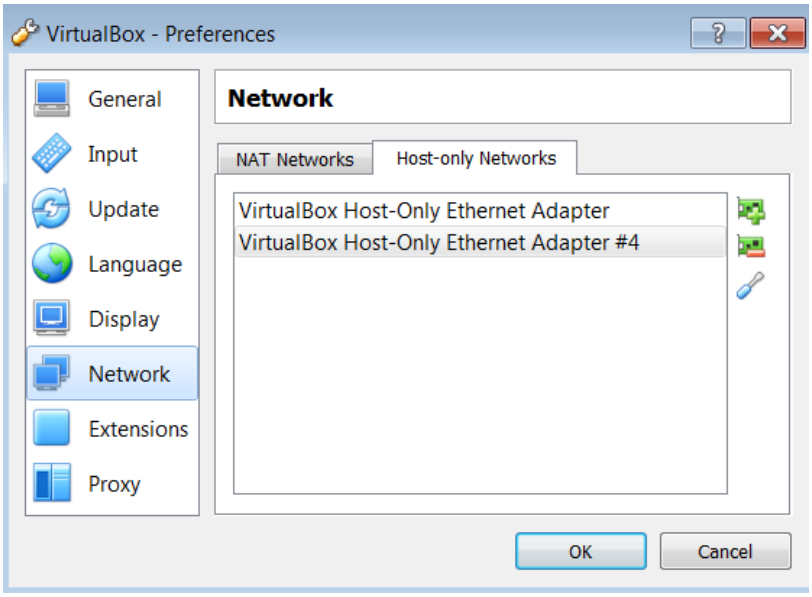


4. Select add new only host network

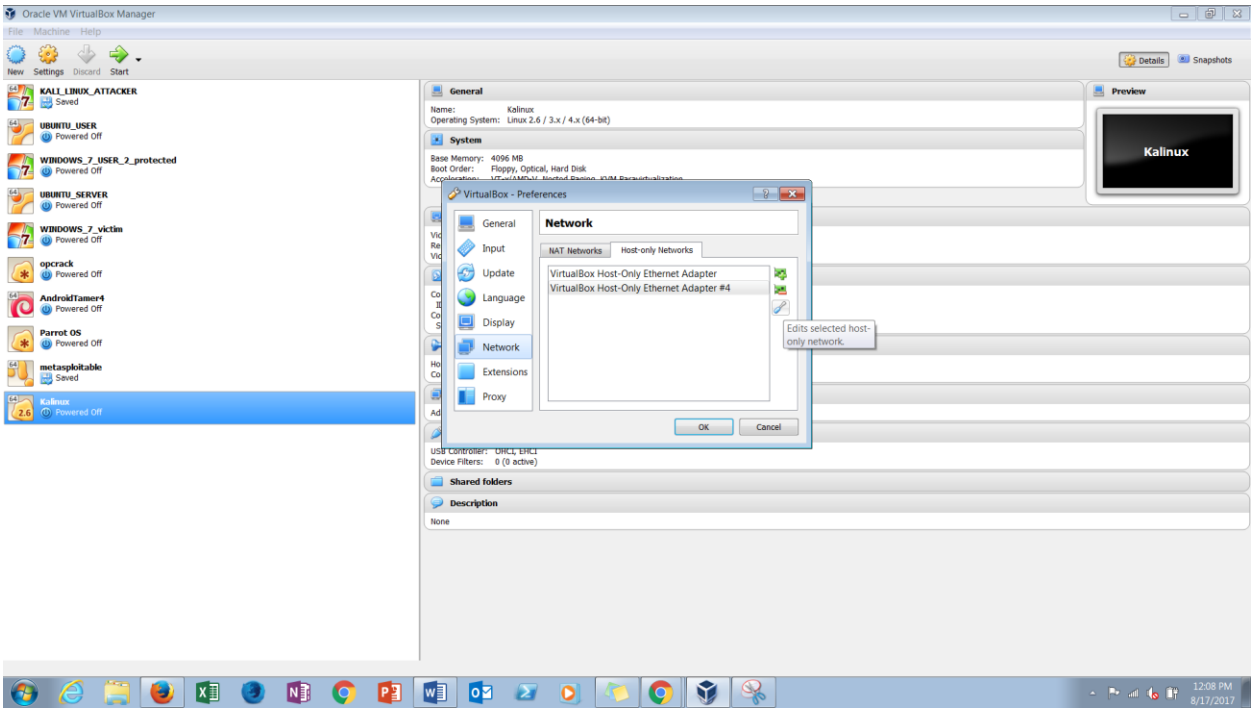




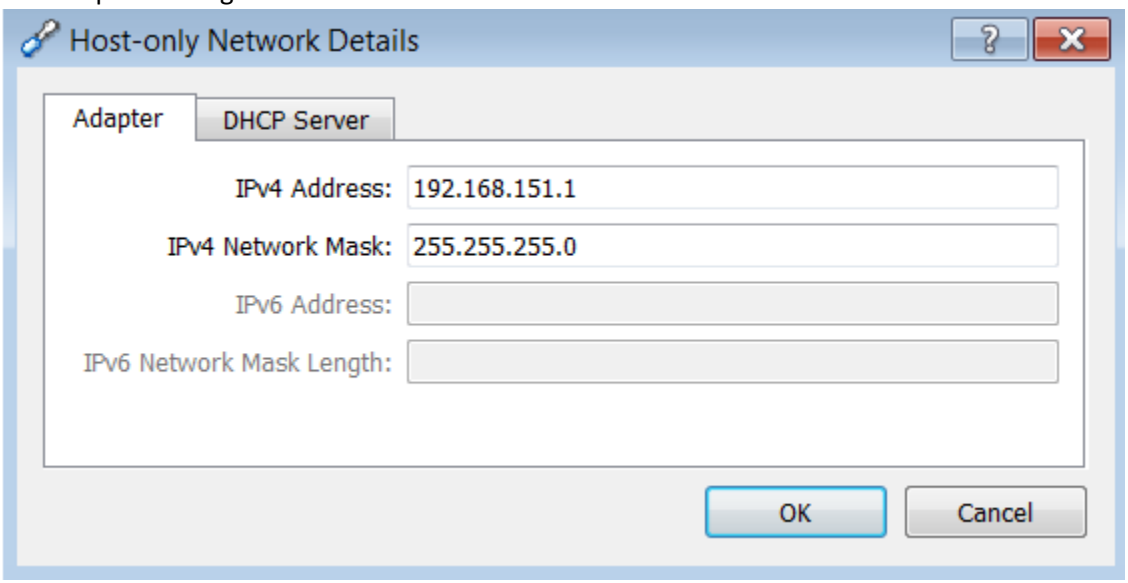
5. Created new host only network



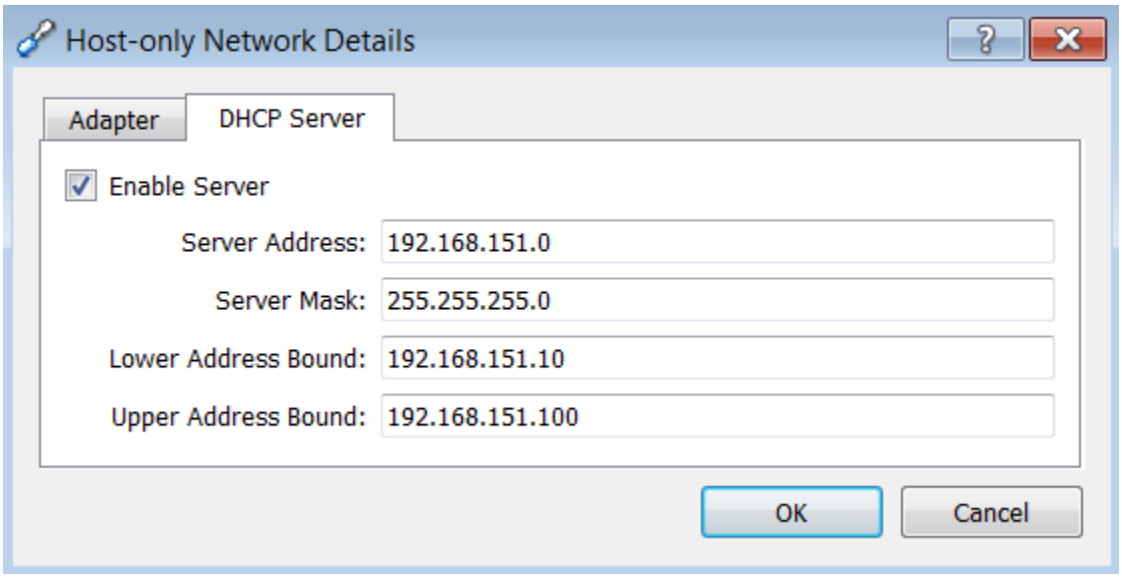
6. Click on “edit”



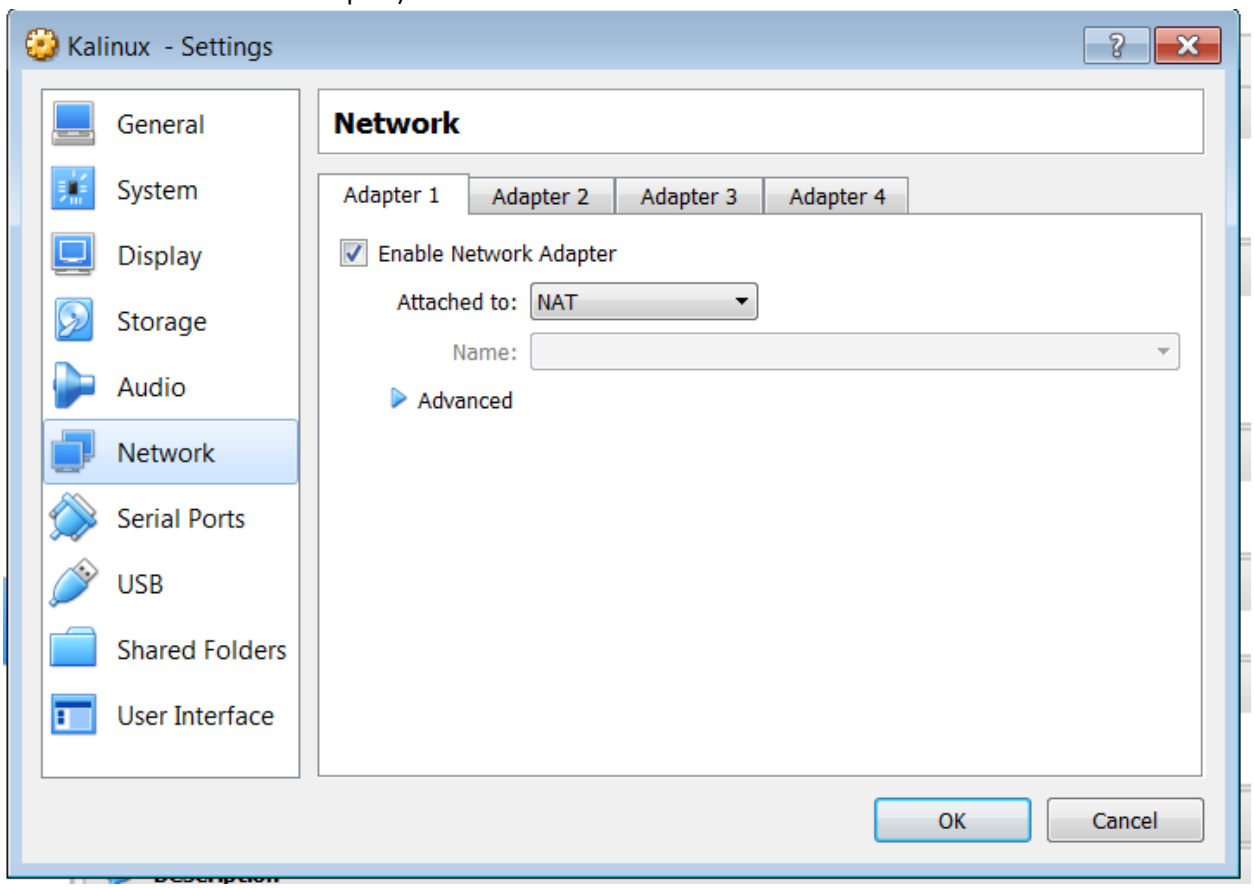
7. Adapter settings

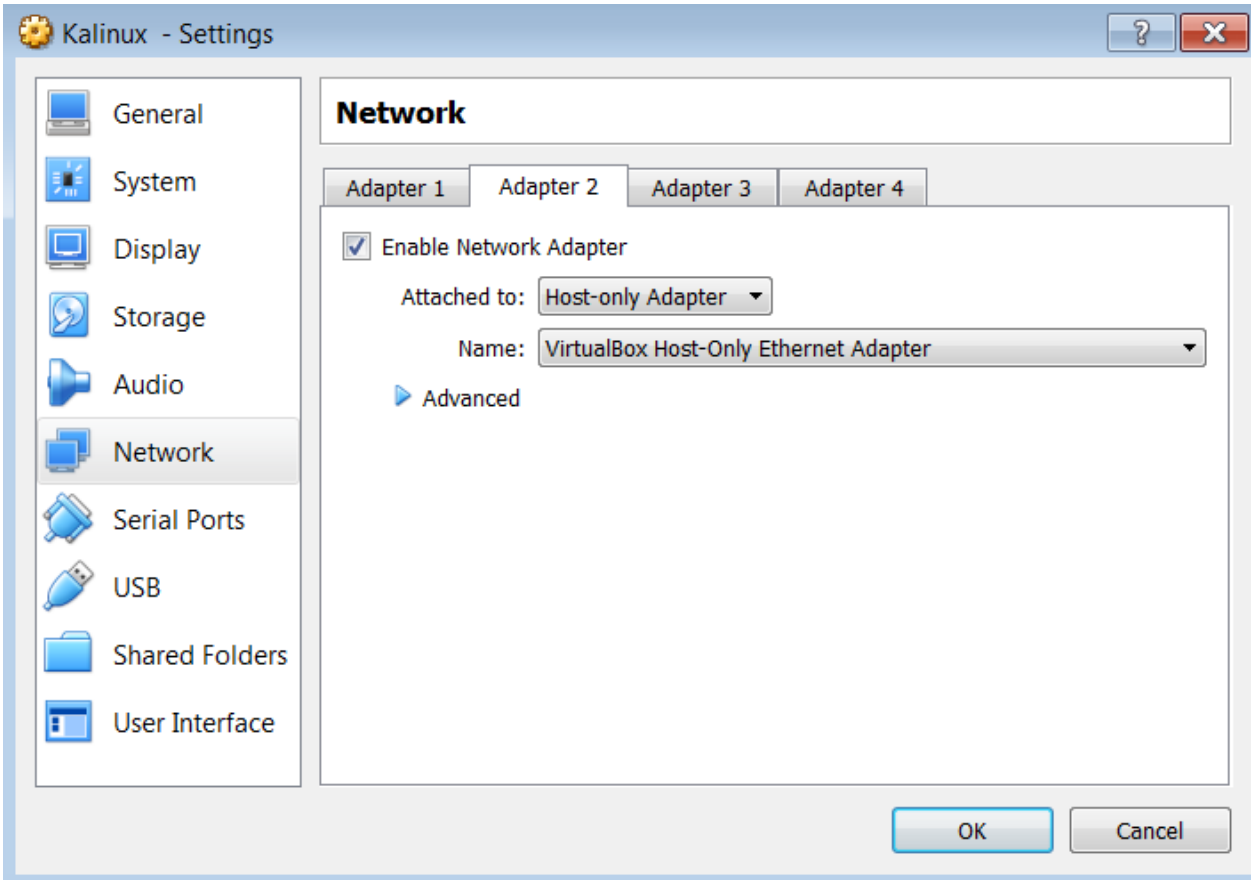


8. Click on enable DHCP server

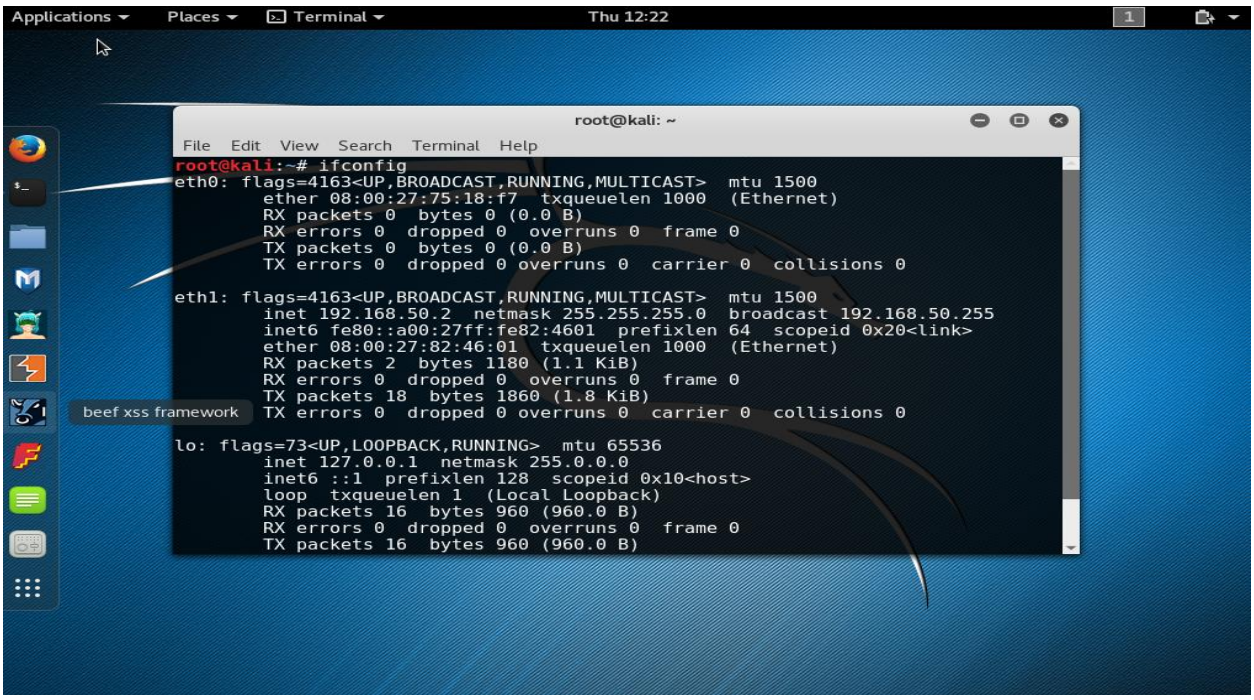


Now select your guest OS (in this case kali linux -> goto settings-> select network -> choose adapter 1 and select NAT -> choose Adapter 2 and select -> Host only network please verify you selected enable network adapter)

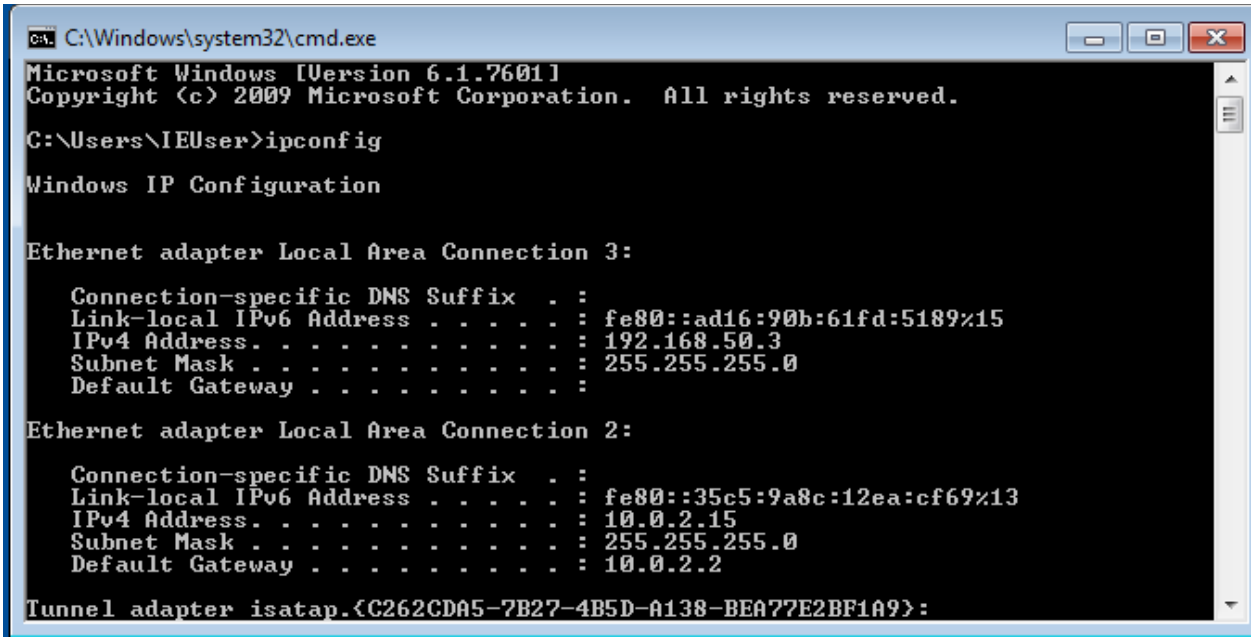




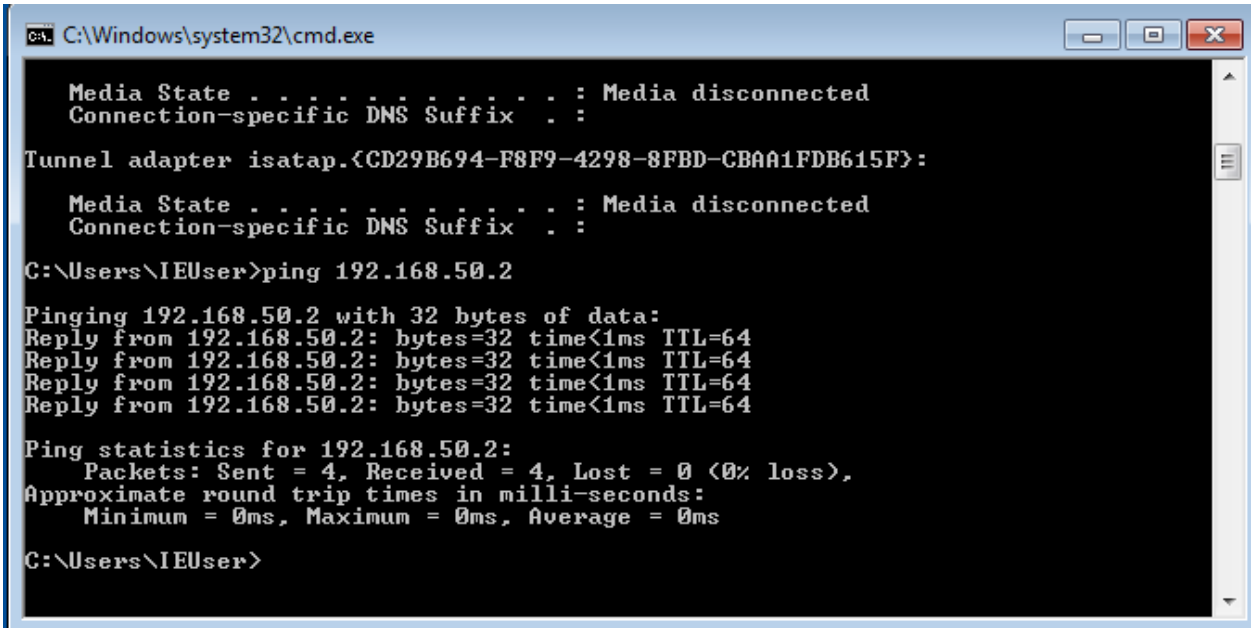
9. Start your guest os (in this case kali) and check IP address of kali box by using 'ifconfig' command



10. Same way you can install windows 7, and verify IP address of windows box by using ‘ipconfig’

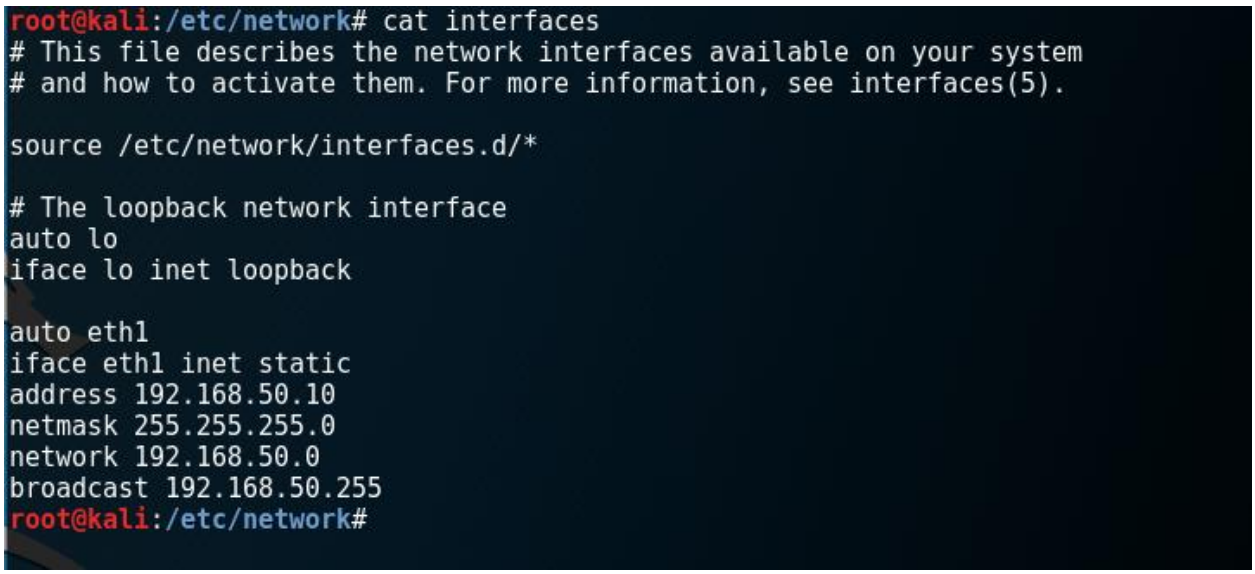


11. We successfully ping kali box from windows 7



12. NMAP scan result from kali

13. You can also configure Static IP address to guest operating system
    From root Goto-> etc->network and open interfaces and make changes as following screenshot



Reference:

1. https://www.virtualbox.org/manual/ch06.html