

## **Pentesting 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 <sup>[1]</sup>**

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:

## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

### 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

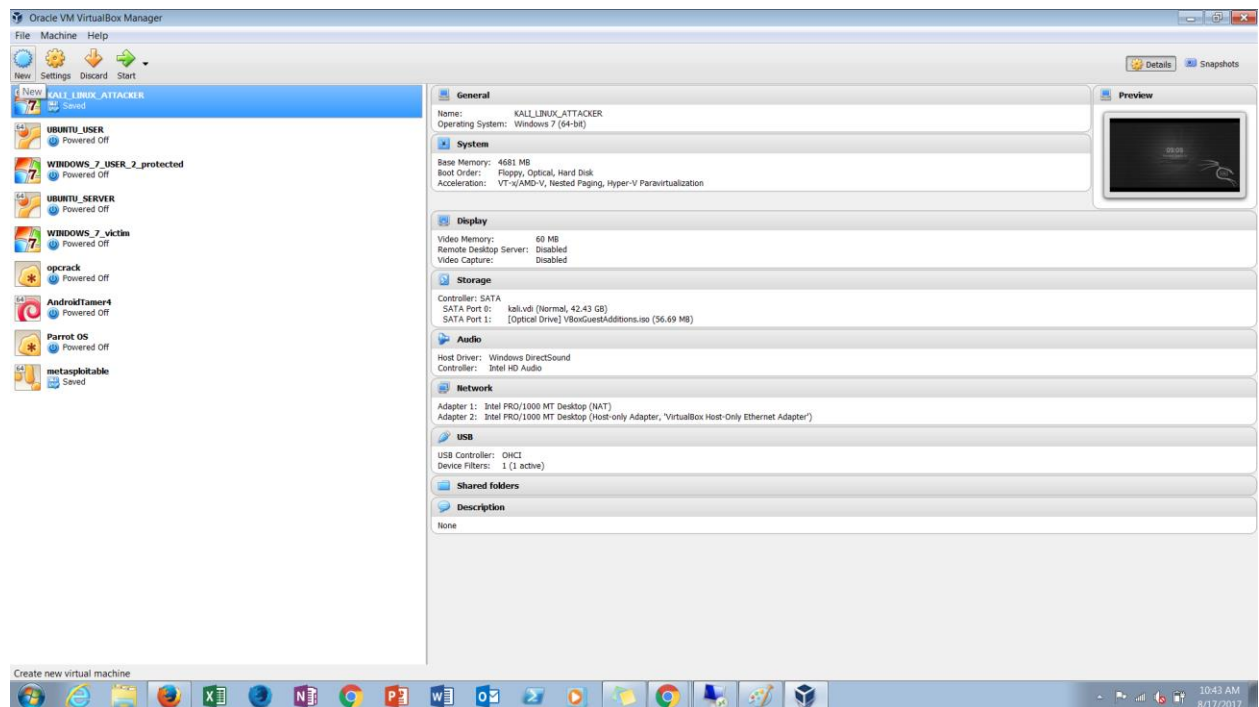
url: <https://www.virtualbox.org/wiki/Downloads>

### 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)

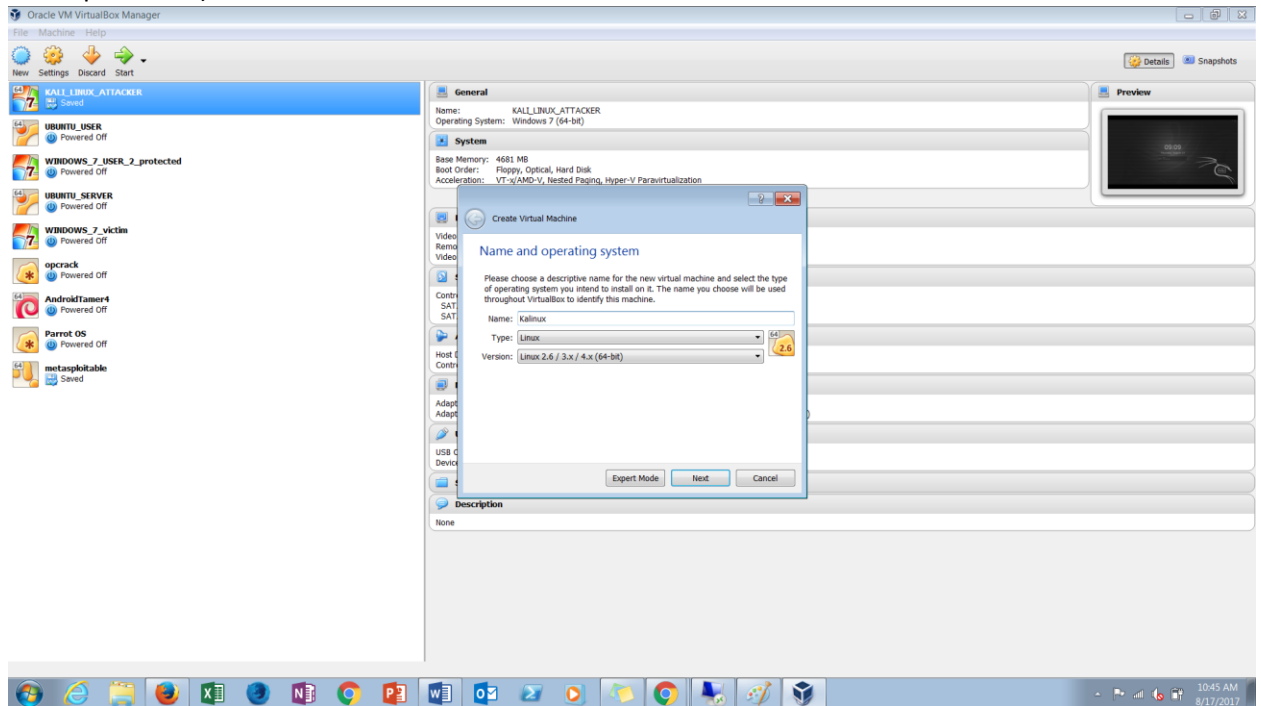
Installing Kali Linux in virtual box

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

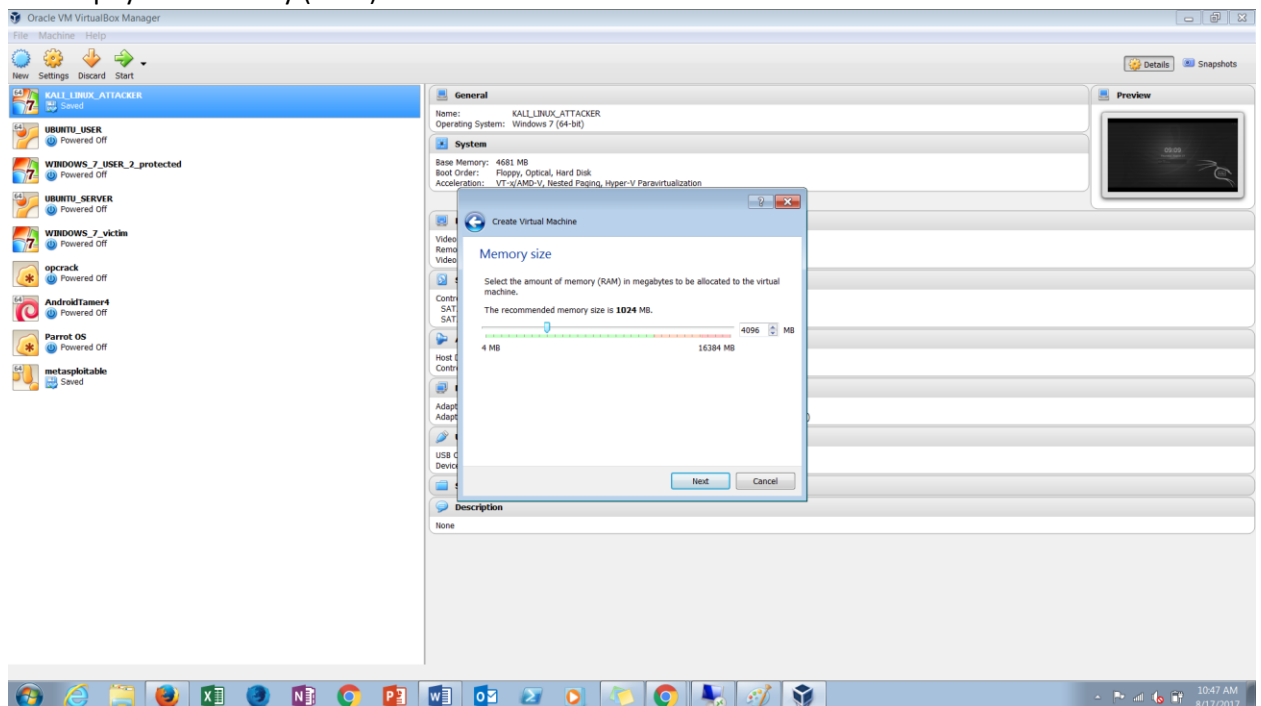


## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

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

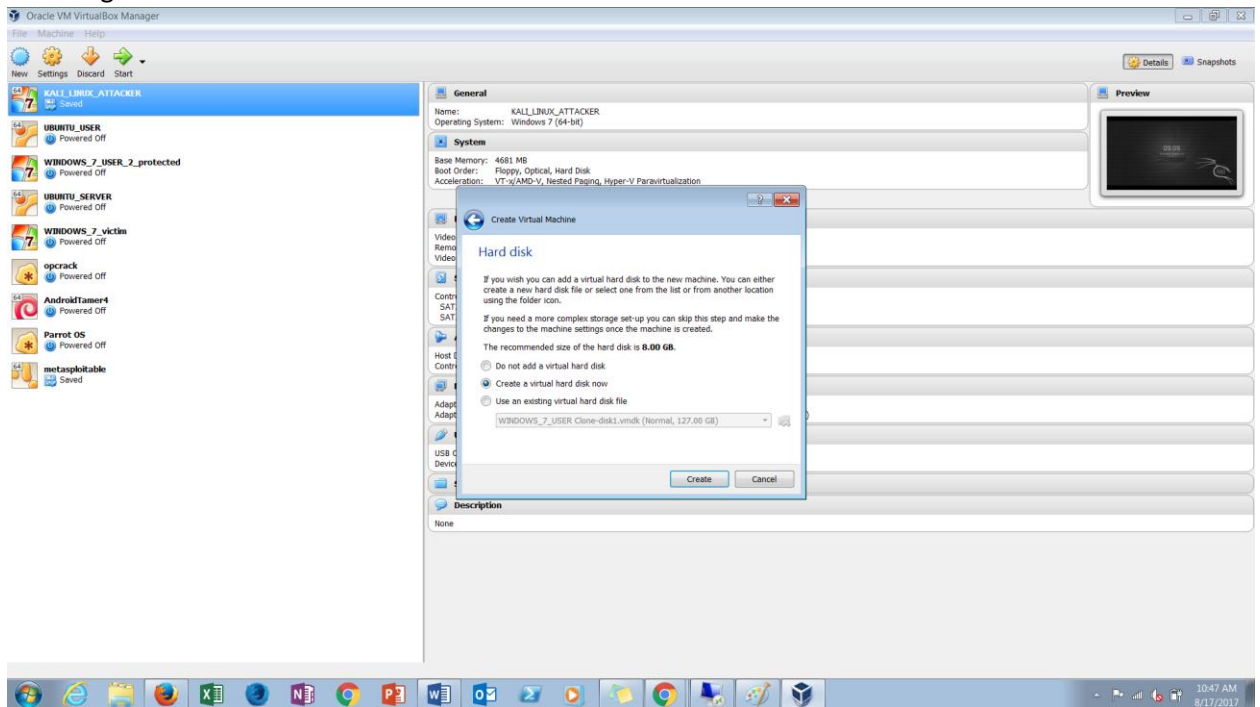


4. Select physical memory (RAM)

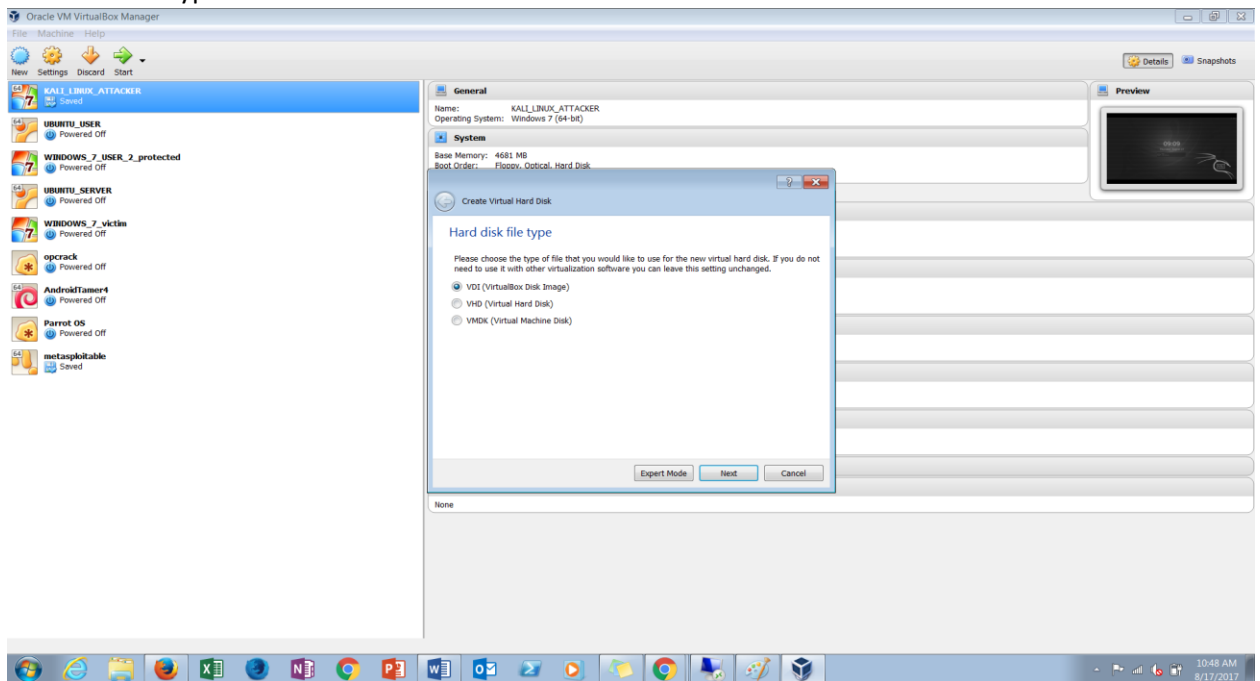


## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

### 5. Creating virtual hard disk

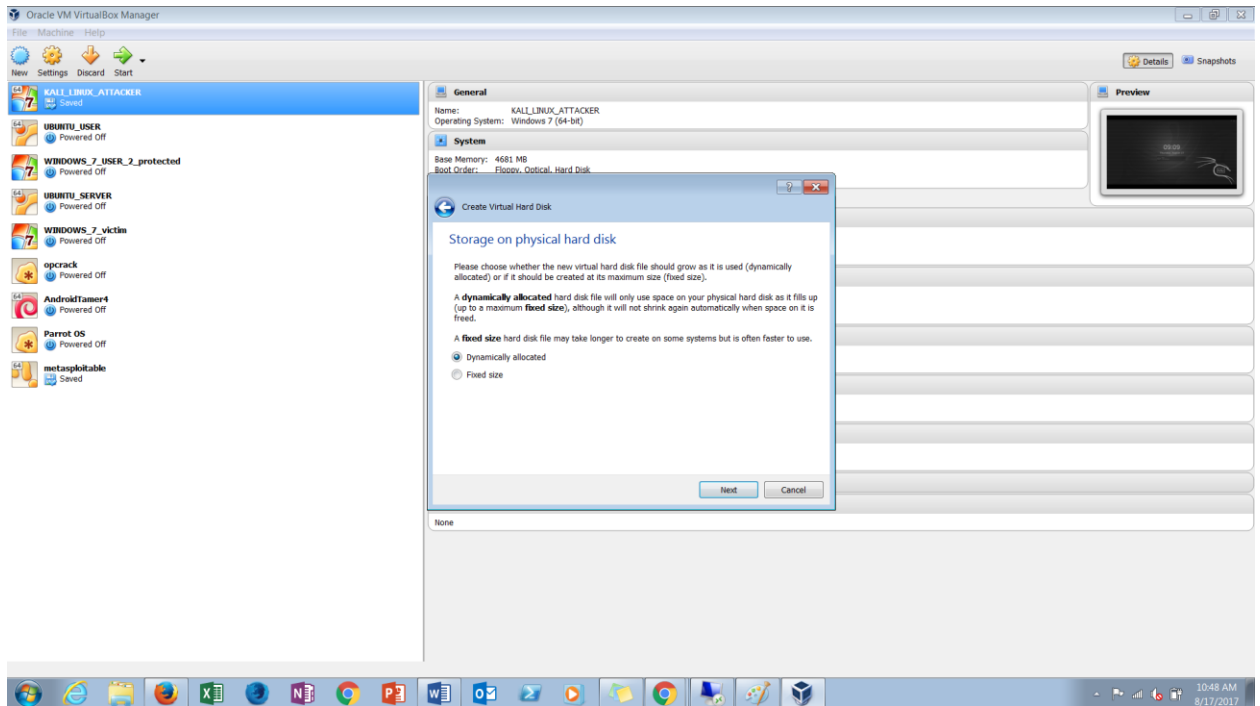


### 6. Hard disk file type VDI

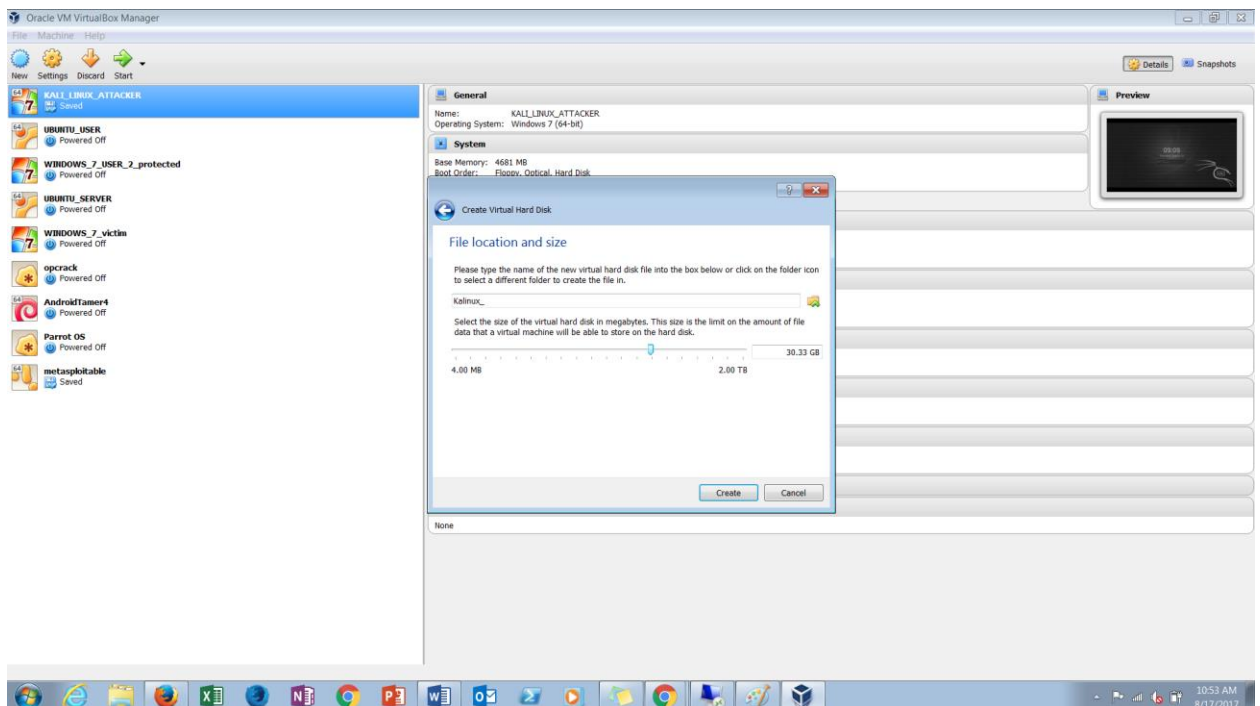


## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

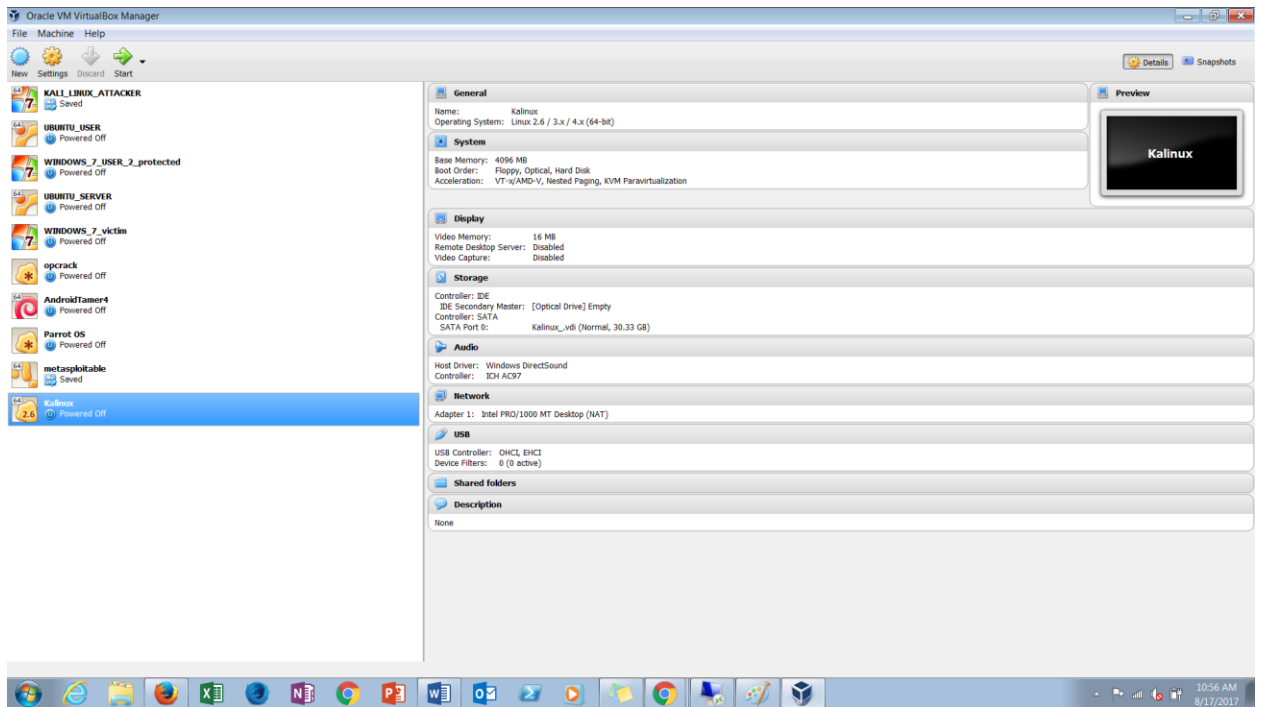
### 7. storage type dynamically allocated



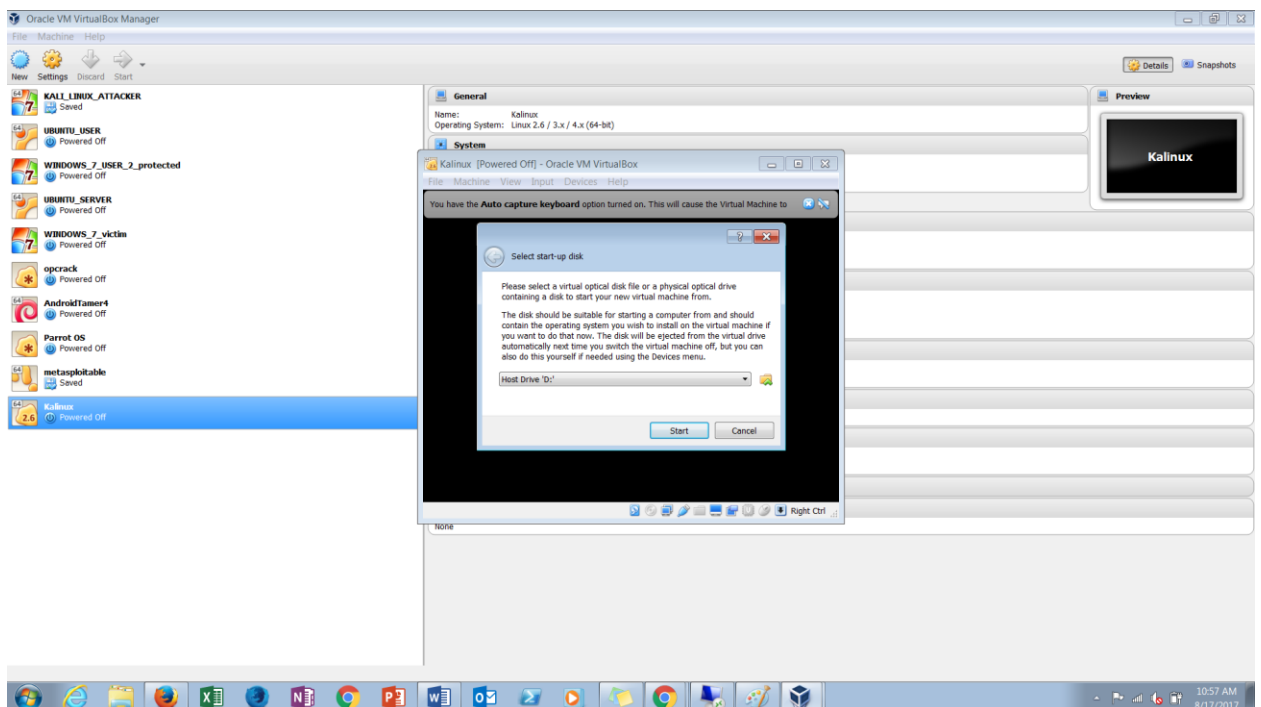
### 8. File location and size (choose more than 30 GB), click on create. Now we successfully created kali instance in Virtual Box



## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

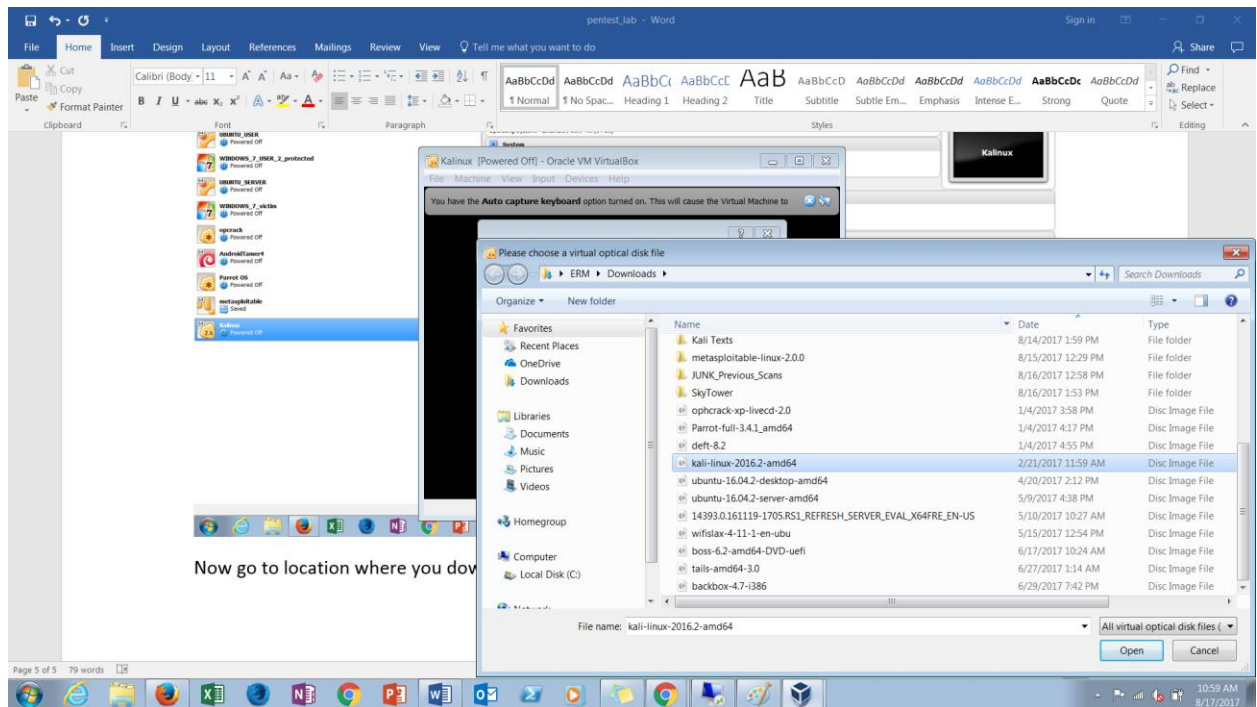


9. Click on created instance, press start button

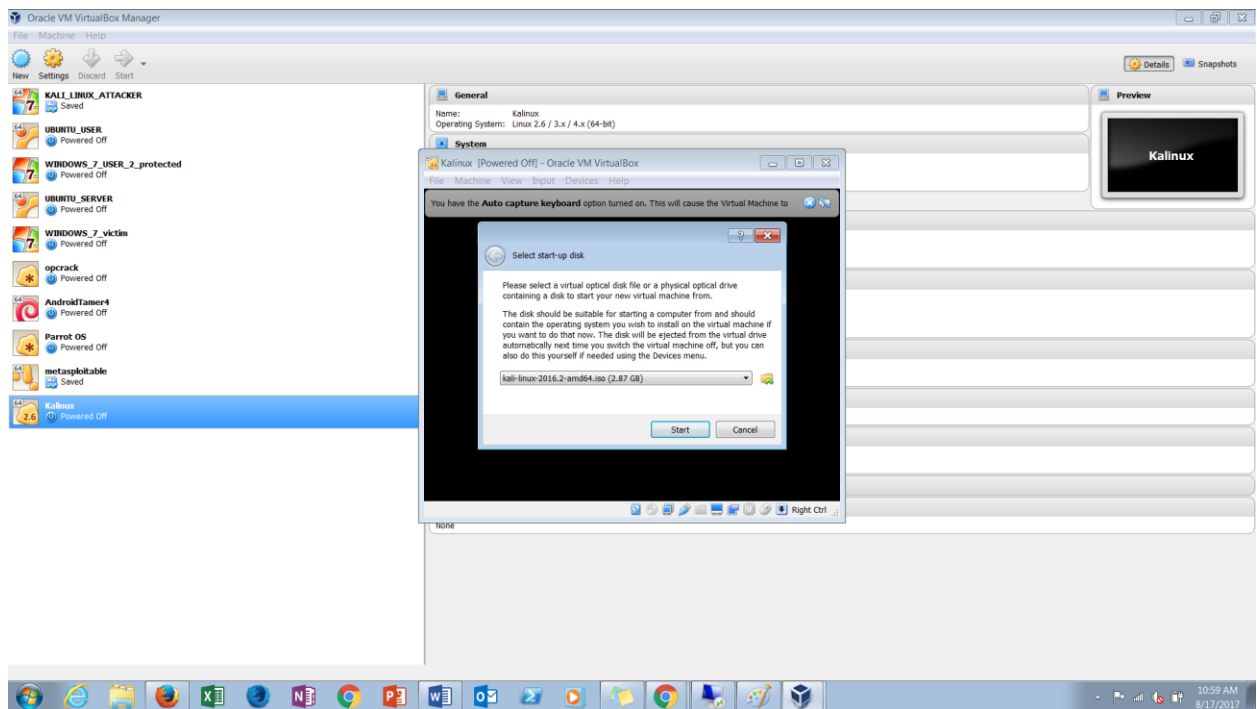


## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

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



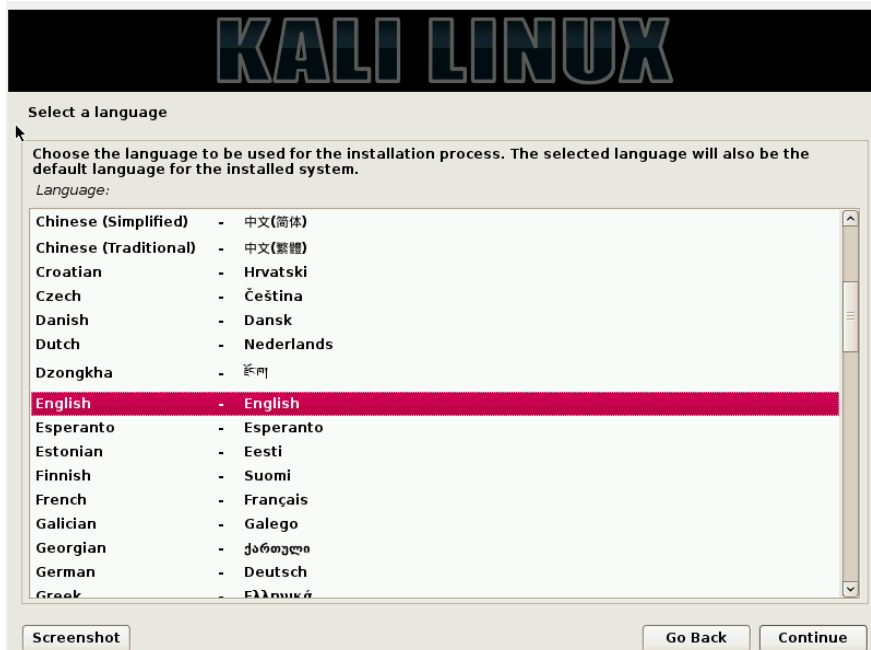
And select it



11. And click on start and choose graphical installation



12. Select language

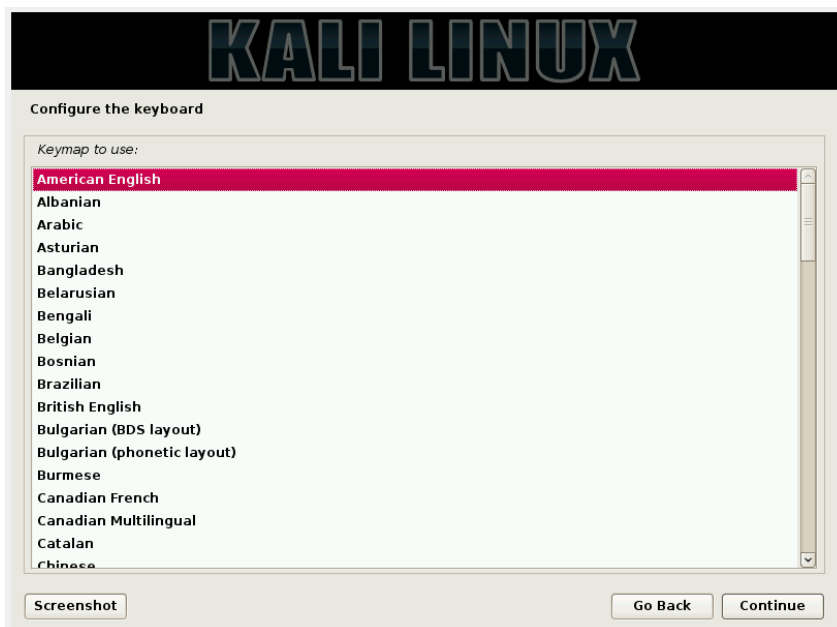




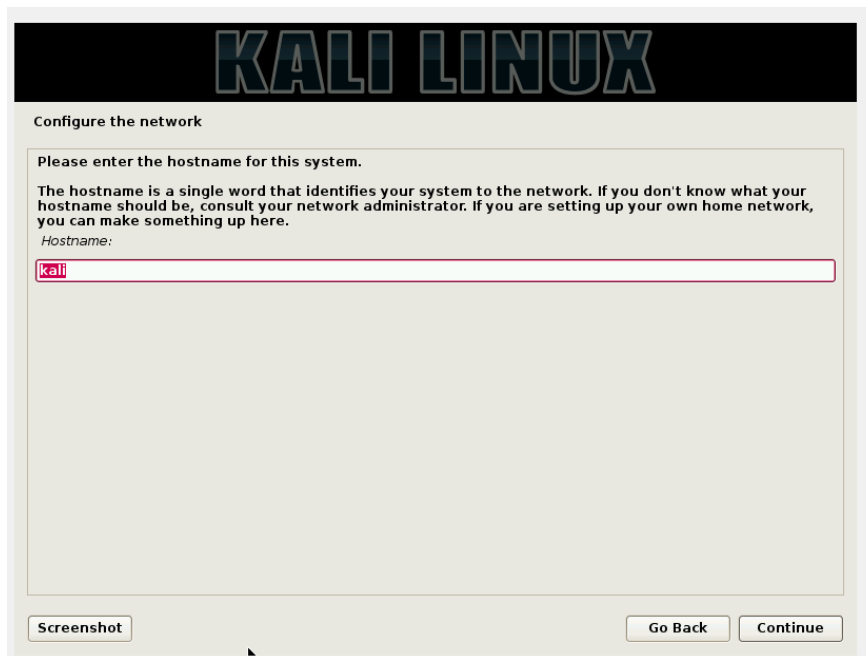
### 13. Location



### 14. Keyboard configuration

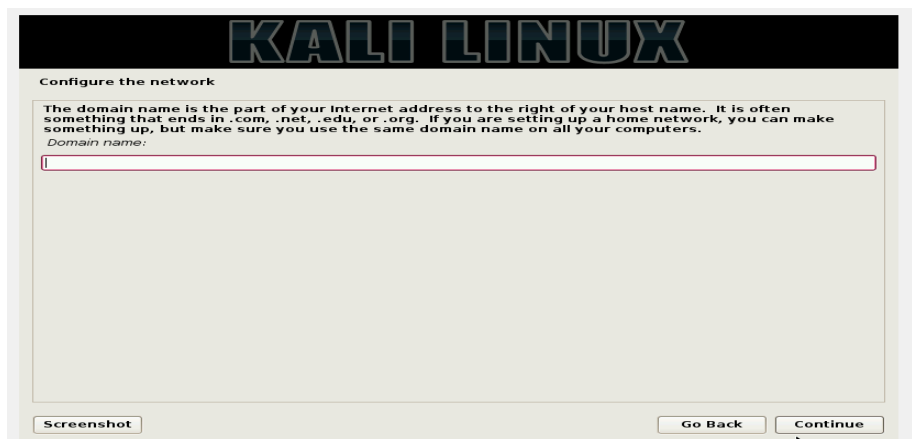


15. Choose Host Name:



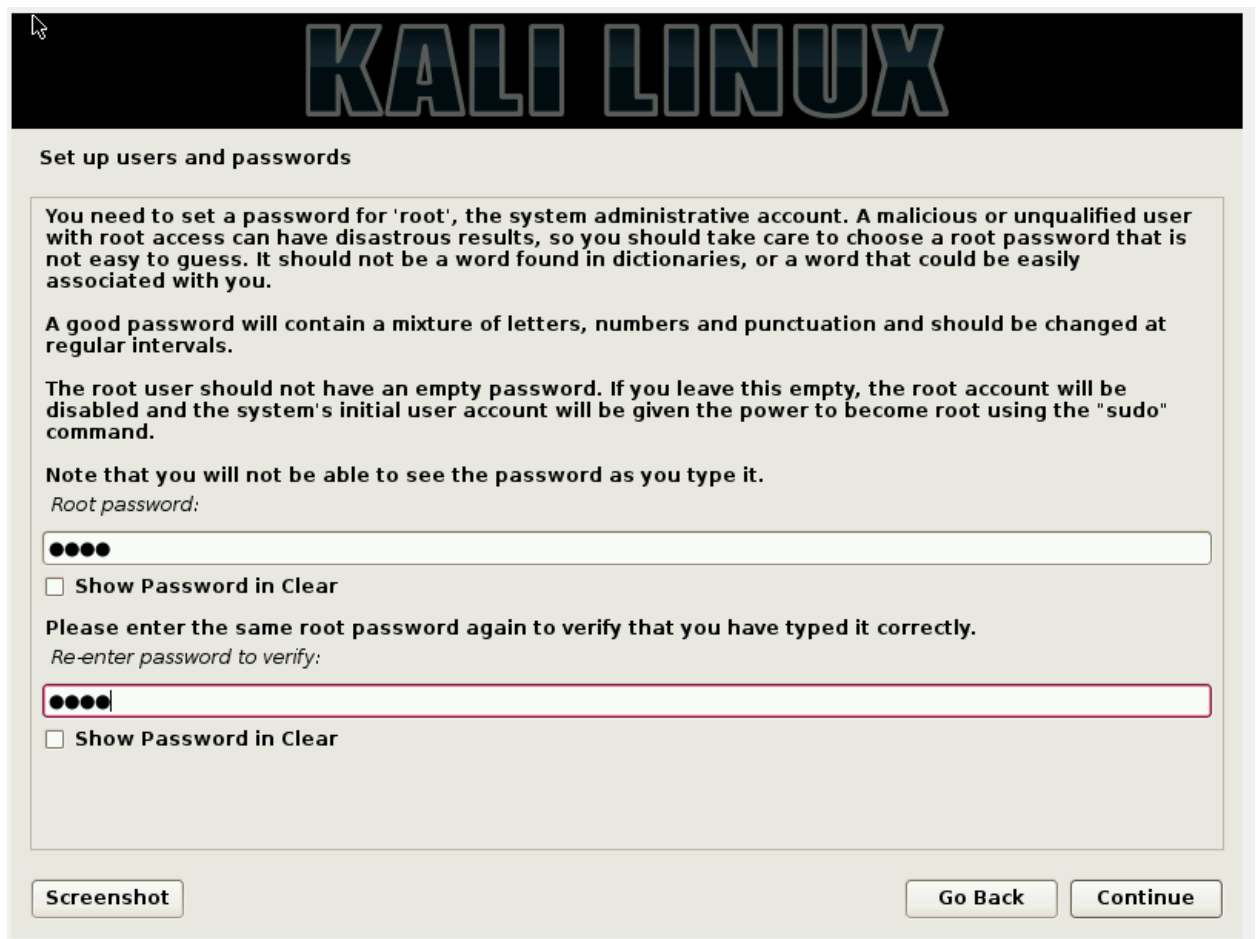
The image shows a Kali Linux network configuration window. At the top, there is a black banner with the text "KALI LINUX" in a stylized, blue, blocky font. Below the banner, the window has a title bar that says "Configure the network". The main content area contains the following text: "Please enter the hostname for this system." followed by "The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here." Below this text, there is a label "Hostname:" and a text input field containing the word "kali". At the bottom of the window, there are three buttons: "Screenshot" on the left, and "Go Back" and "Continue" on the right.

16. You can leave domain name, click next



The image shows a Kali Linux network configuration window. At the top, there is a black banner with the text "KALI LINUX" in a stylized, blue, blocky font. Below the banner, the window has a title bar that says "Configure the network". The main content area contains the following text: "The domain name is the part of your internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers." Below this text, there is a label "Domain name:" and a text input field that is currently empty. At the bottom of the window, there are three buttons: "Screenshot" on the left, and "Go Back" and "Continue" on the right.

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



**KALI LINUX**

### 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.

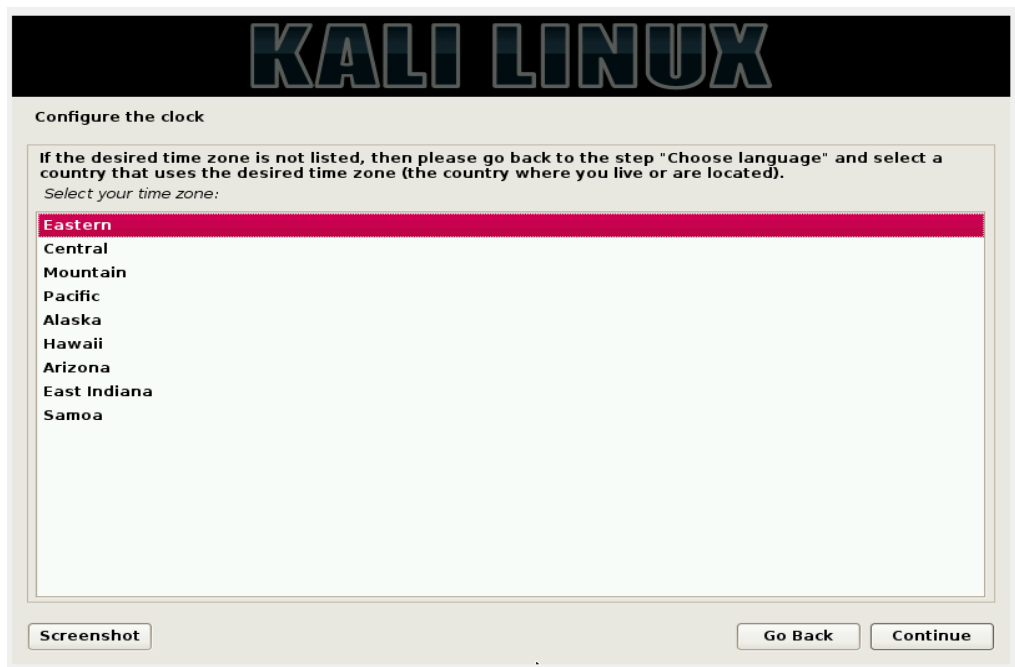
Re-enter password to verify:

●●●●●

☐ Show Password in Clear

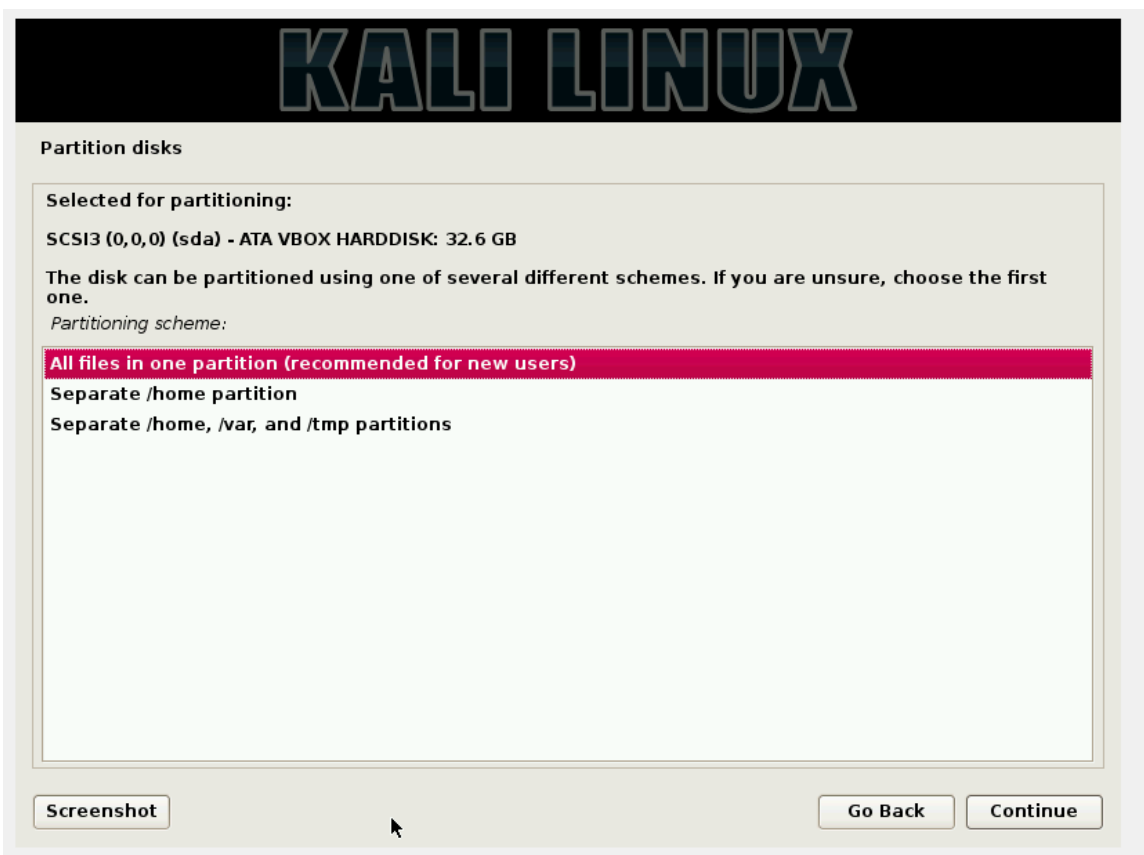
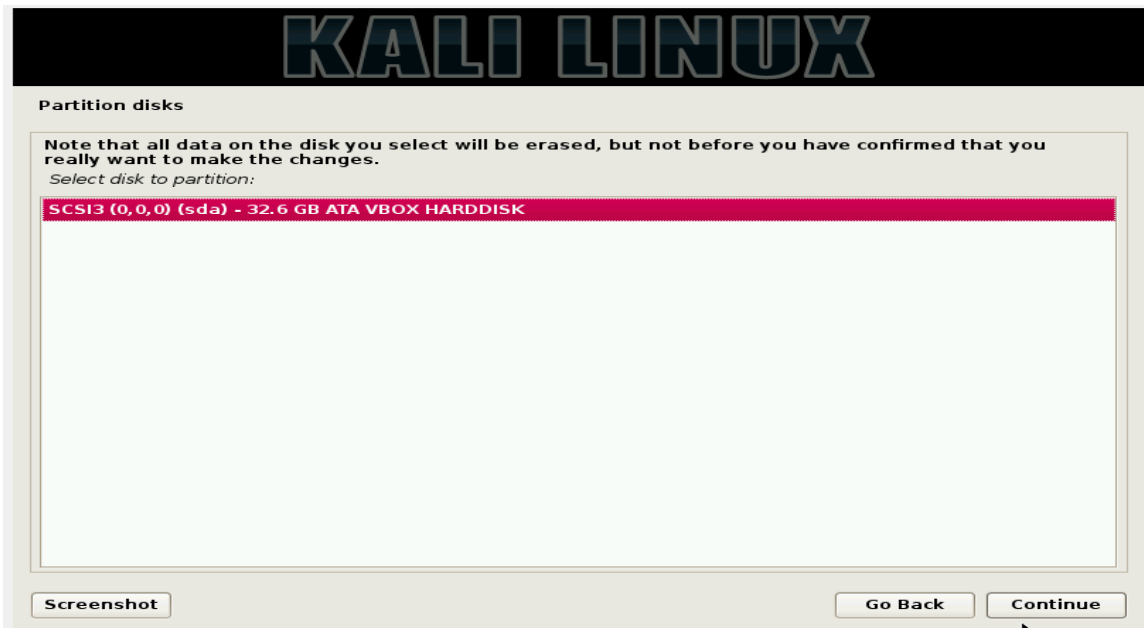
[Screenshot](#) [Go Back](#) [Continue](#)

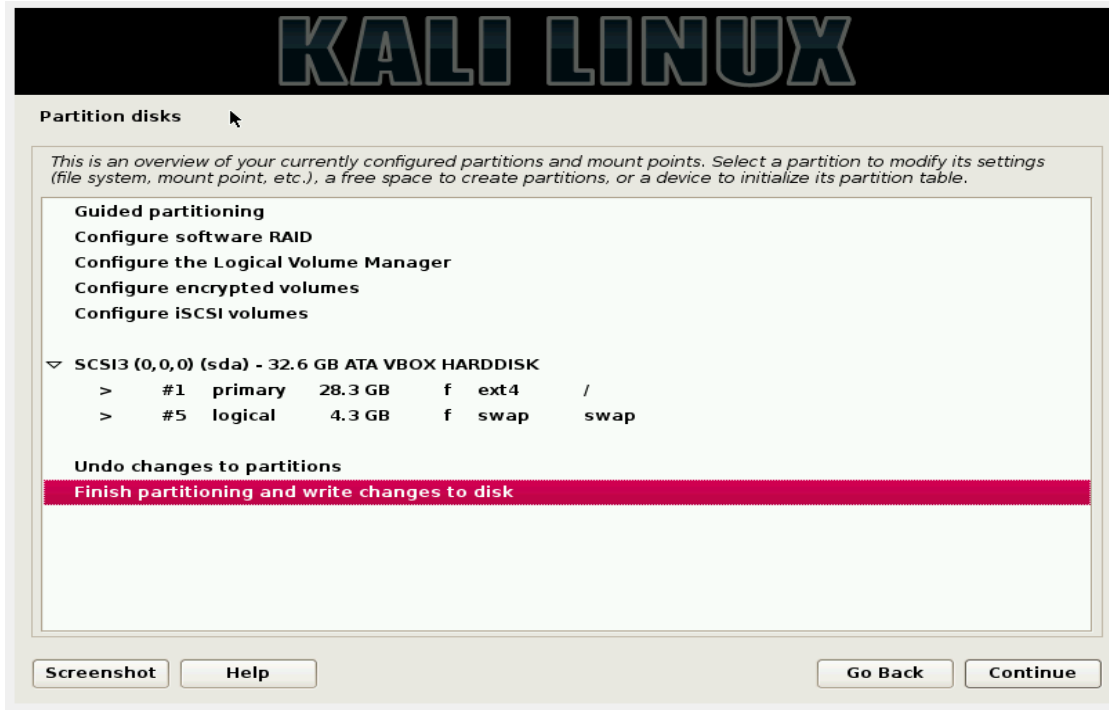
## 18. Clock



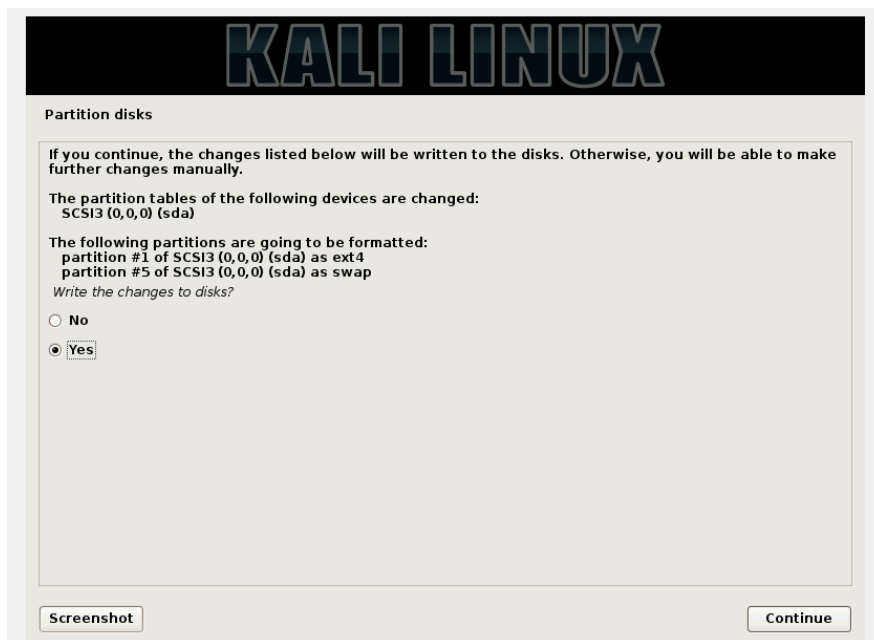
## 19. Disk Partition

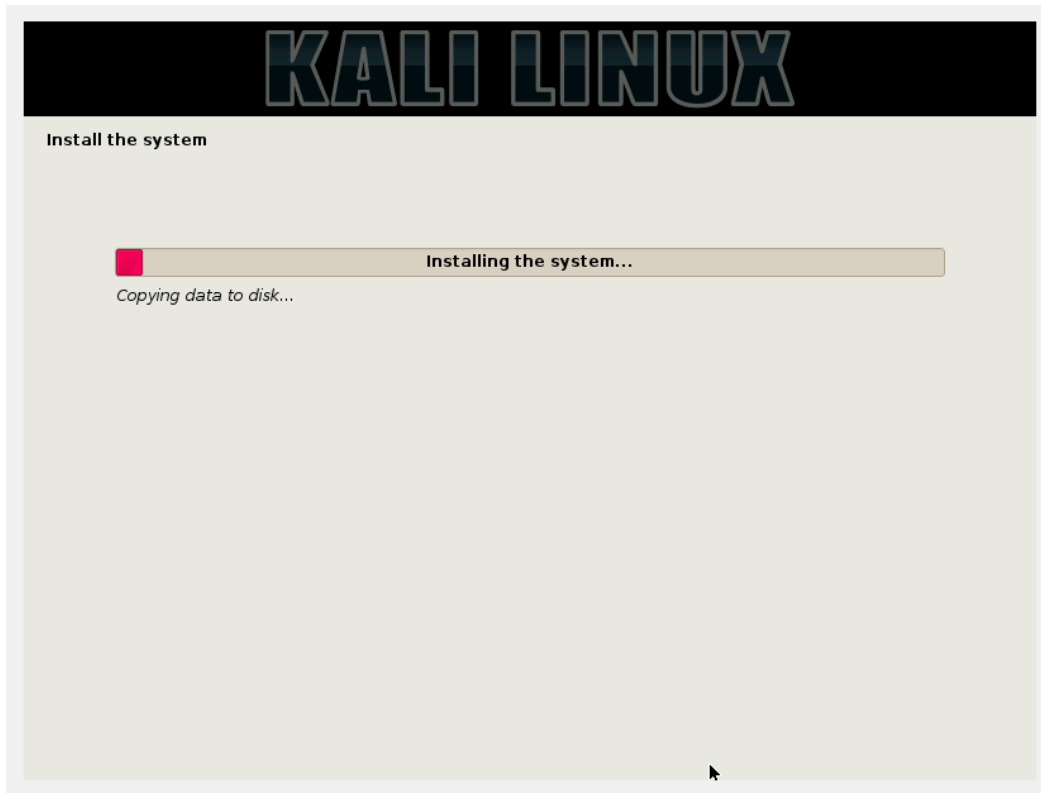




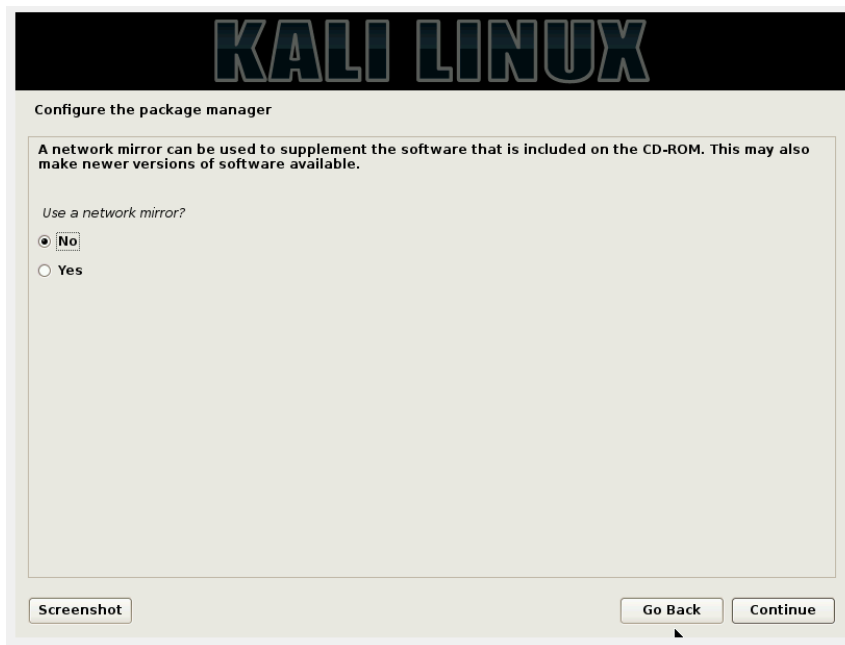


20. Select 'yes', to keep changes





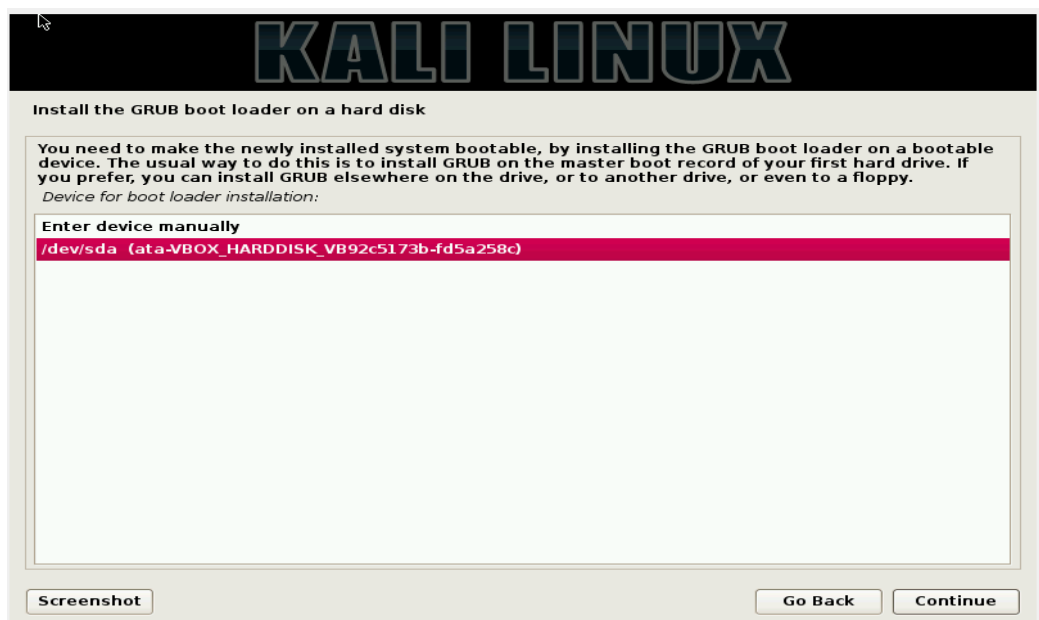
21. Select 'no' for network mirror



22. Press 'yes'

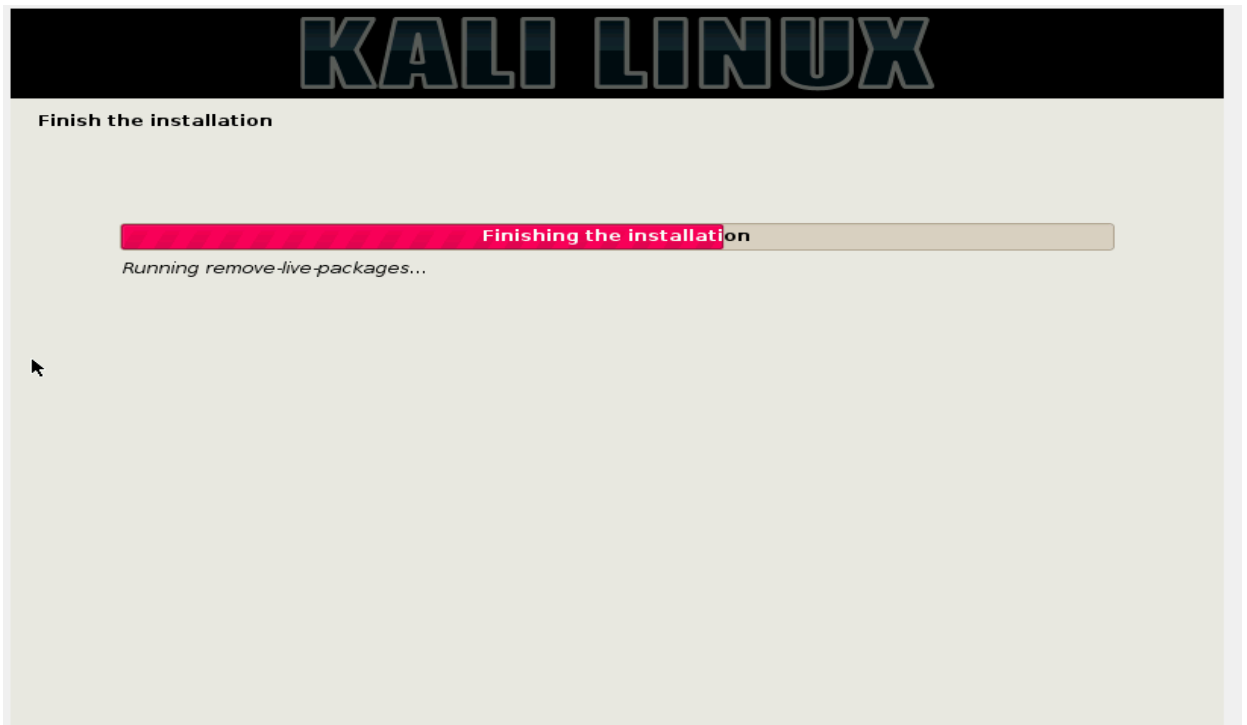
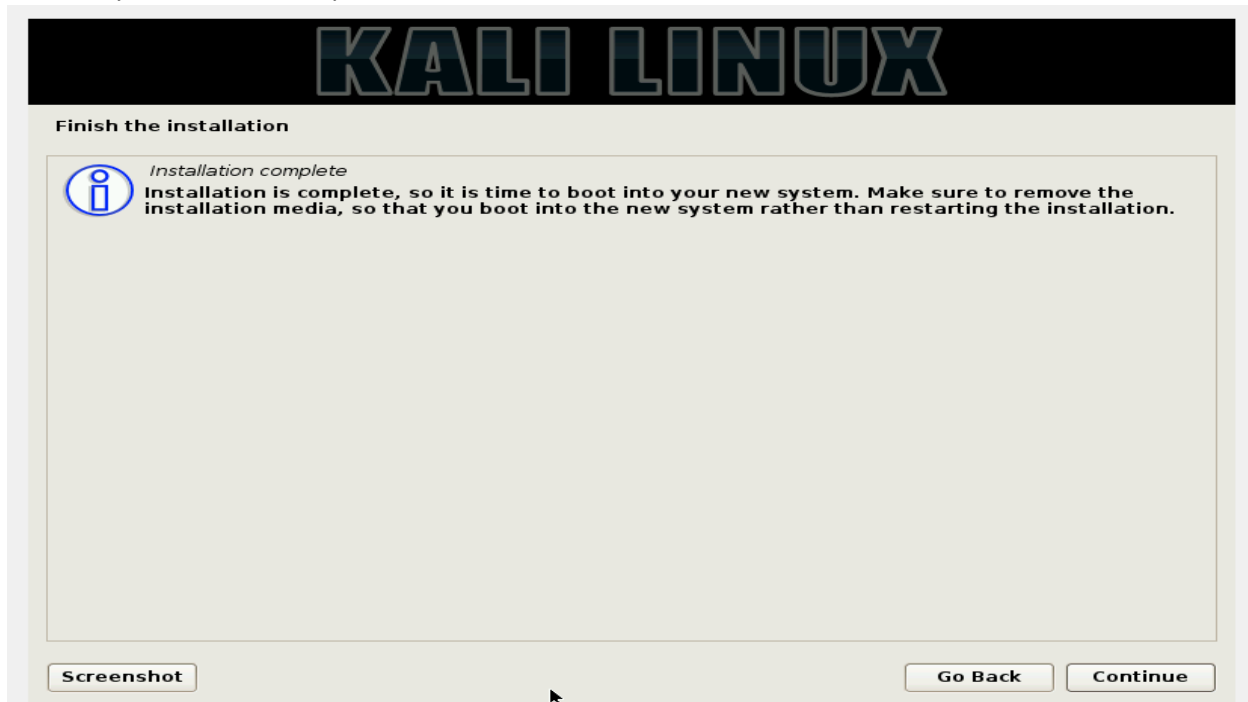


24. Select /dev/sda





25. Finally, installation completed

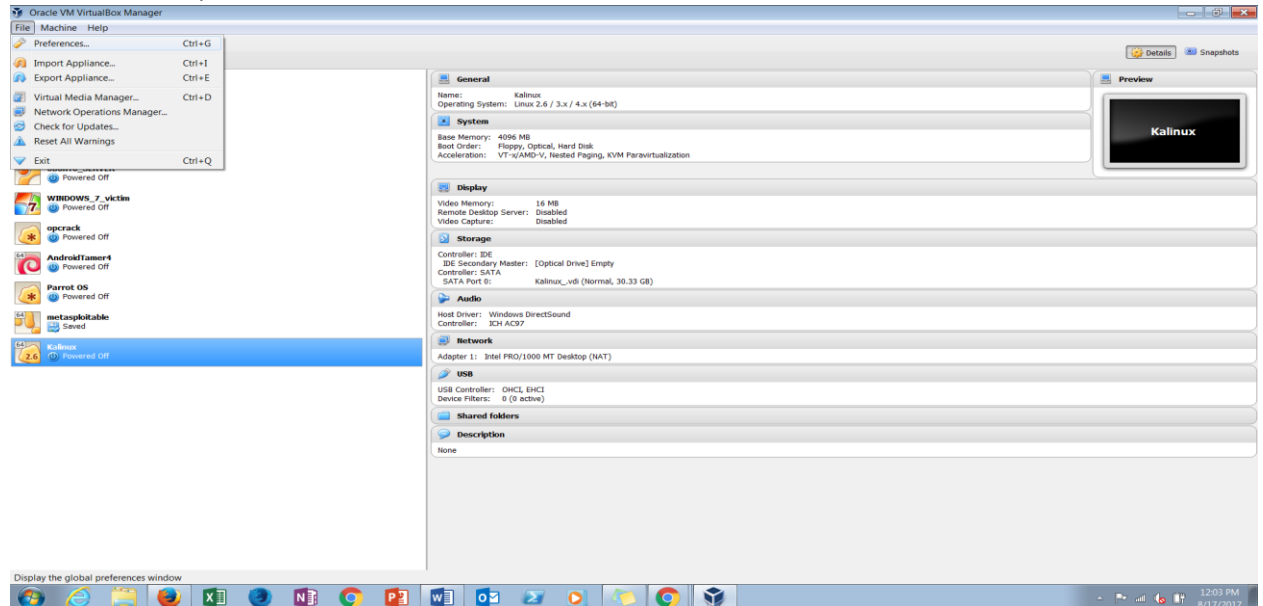


## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

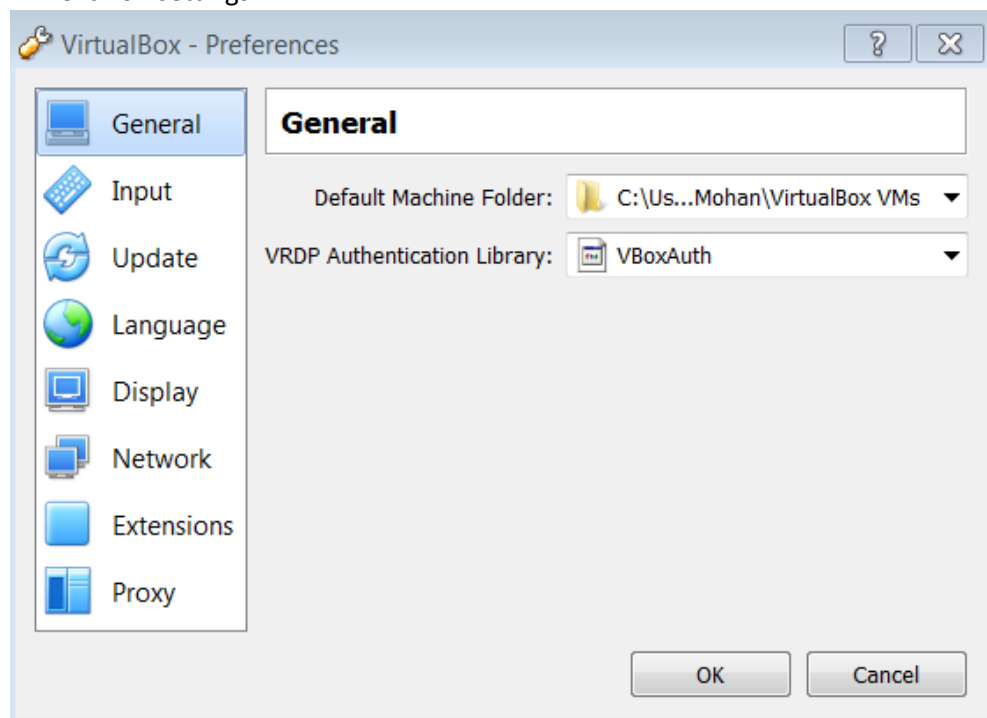
### Step 3: Network settings

Now, we are configuring host only settings,

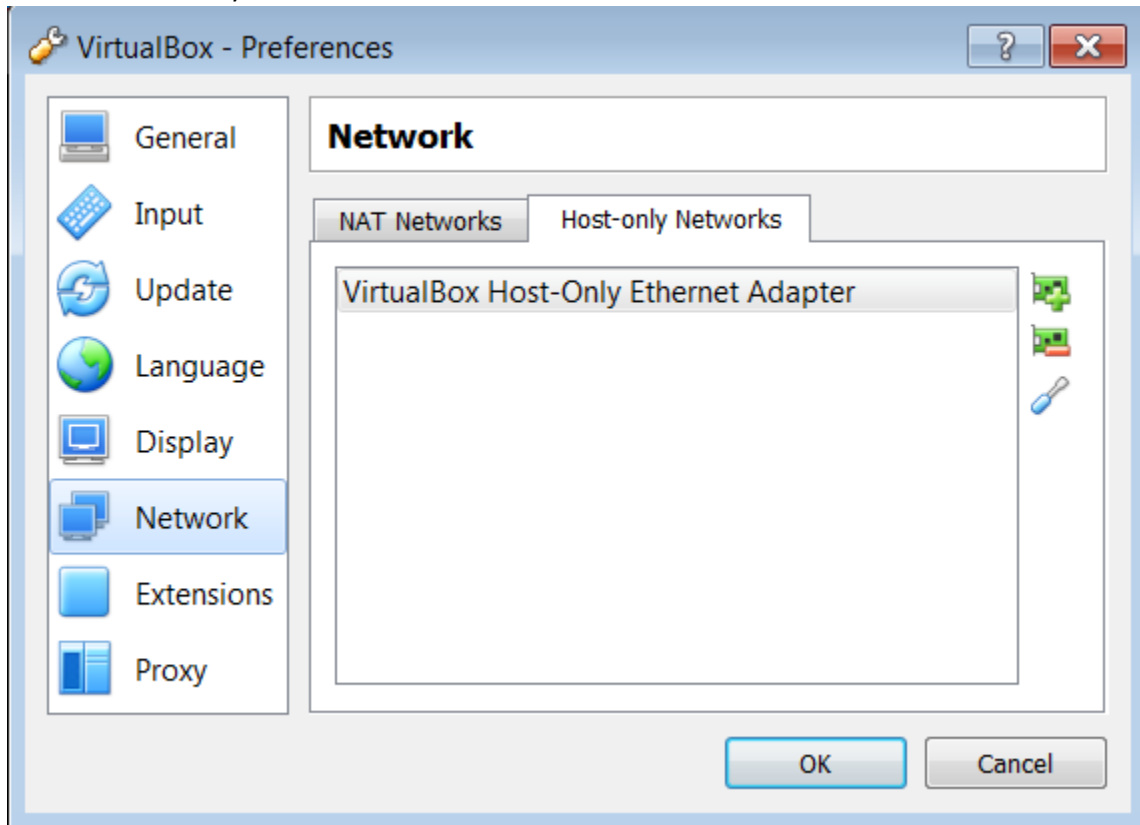
#### 1. Goto file -> preferences



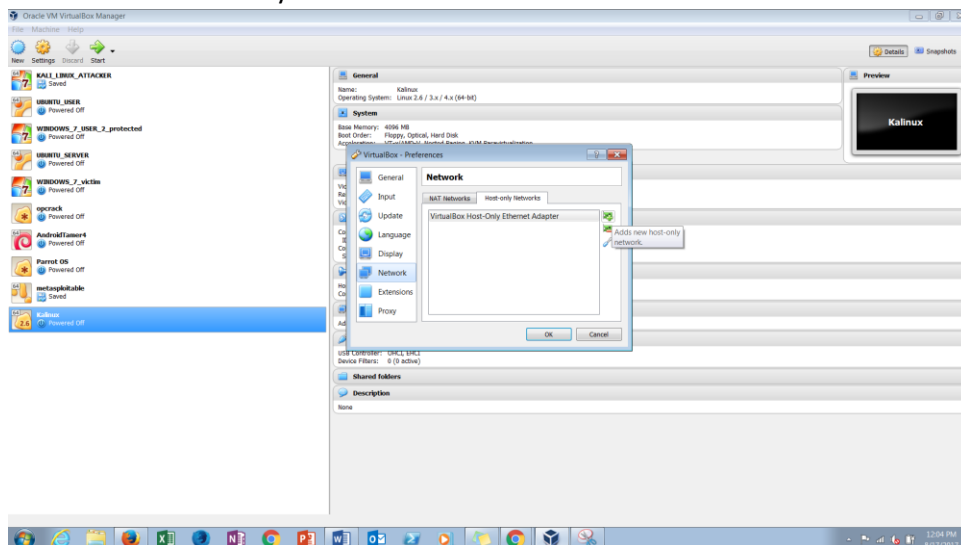
#### 2. Click on settings

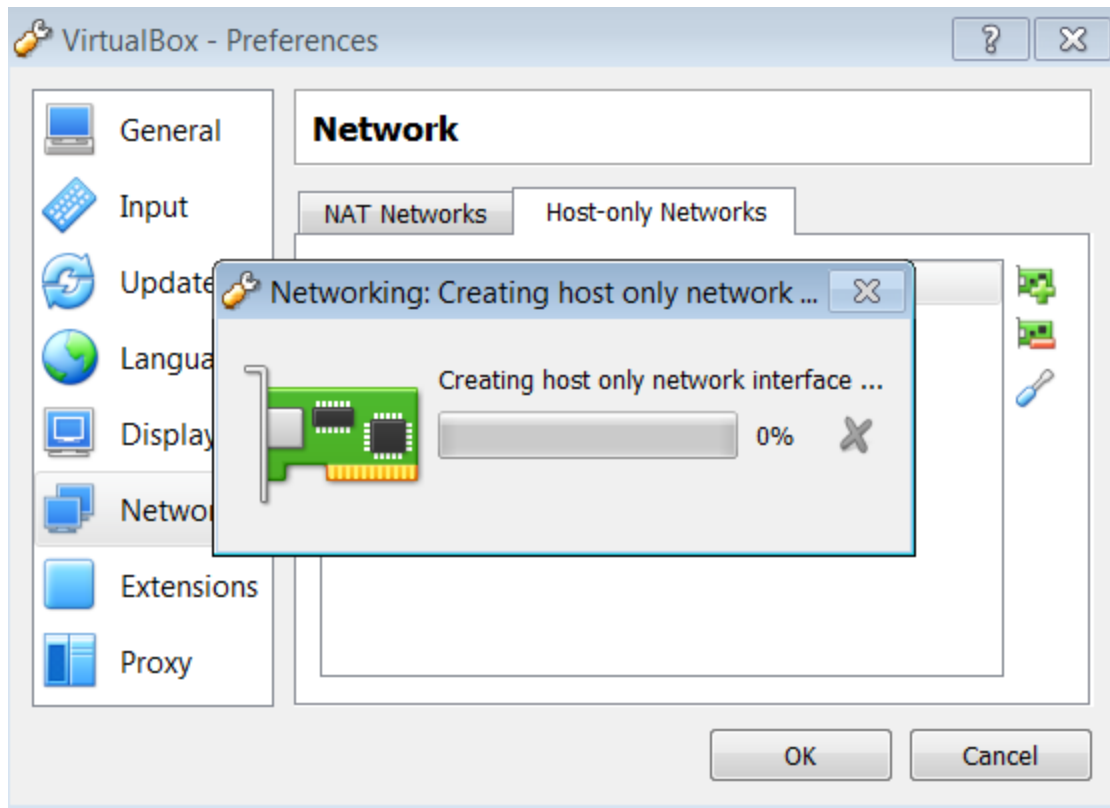


3. Select host only network

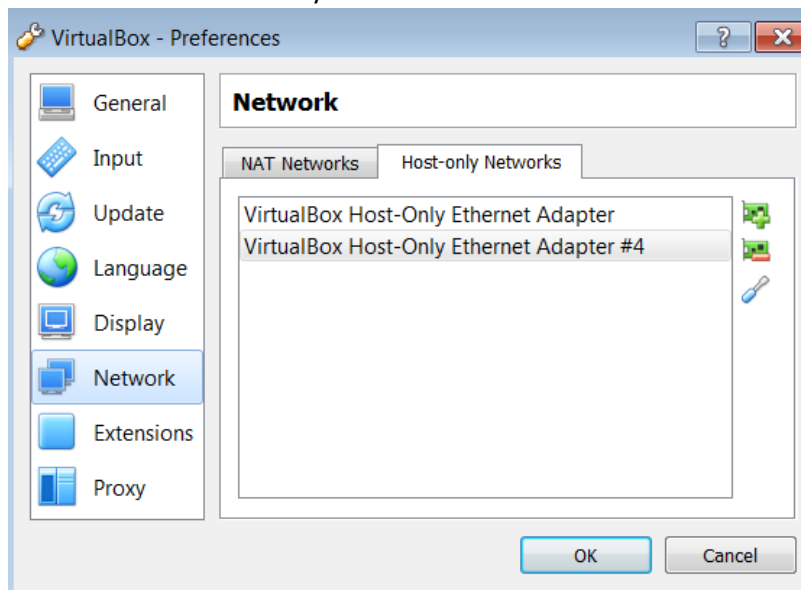


4. Select add new only host network



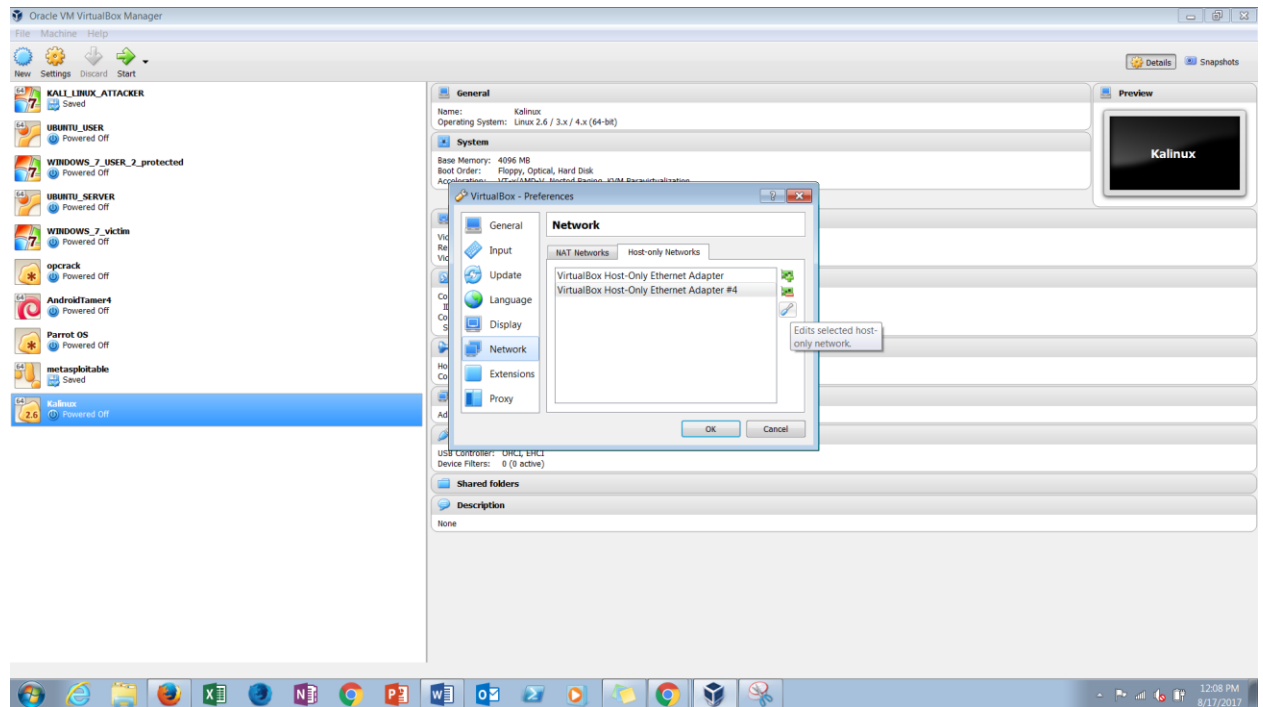


5. Created new host only network

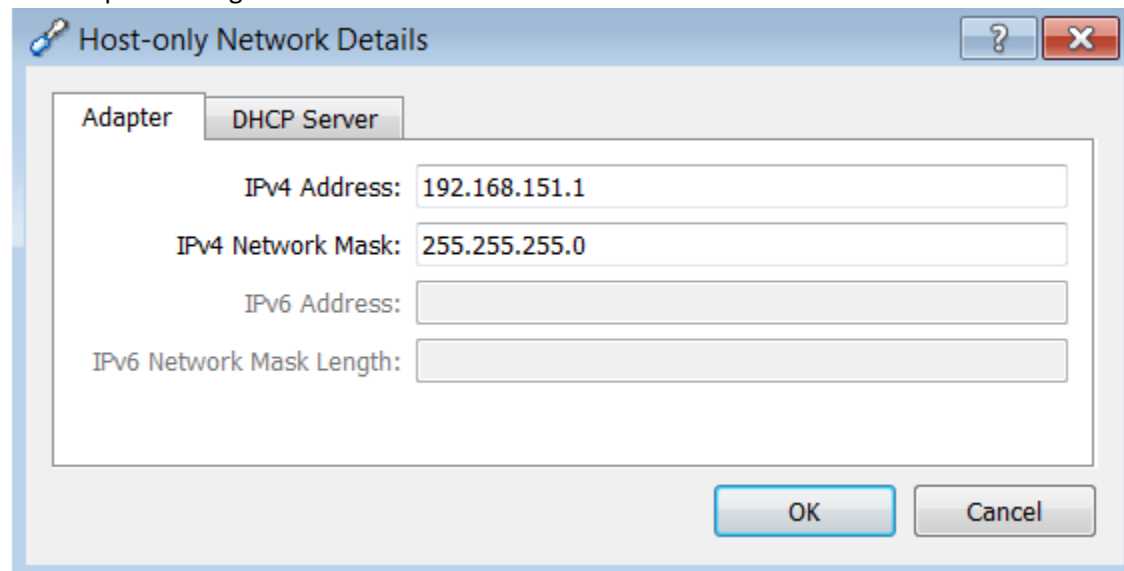


## Tutorial: Penetration Testing lab with Virtual Box (Host only network configuration)

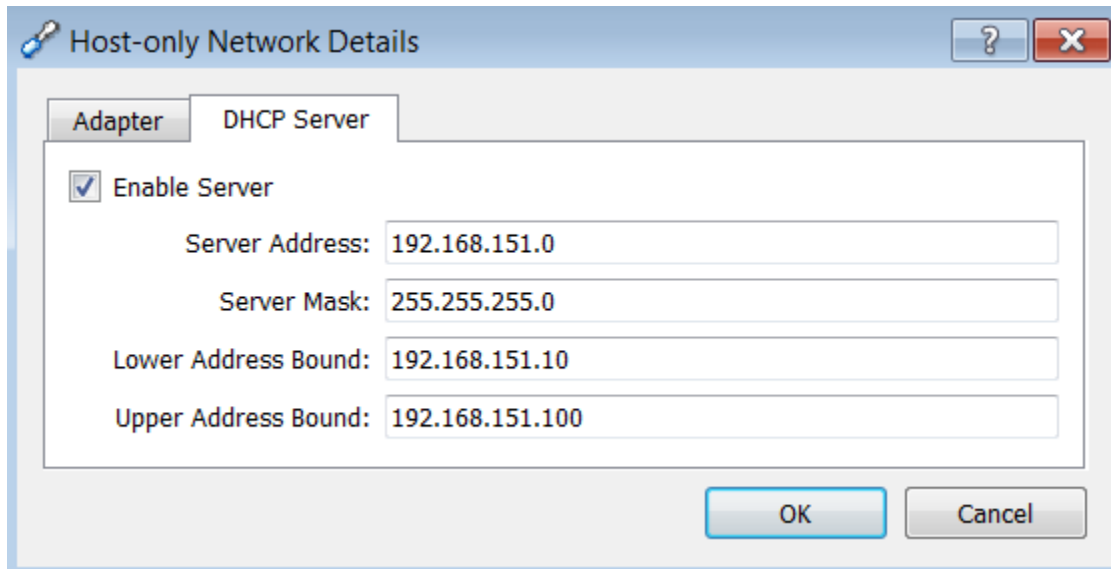
### 6. Click on “edit”



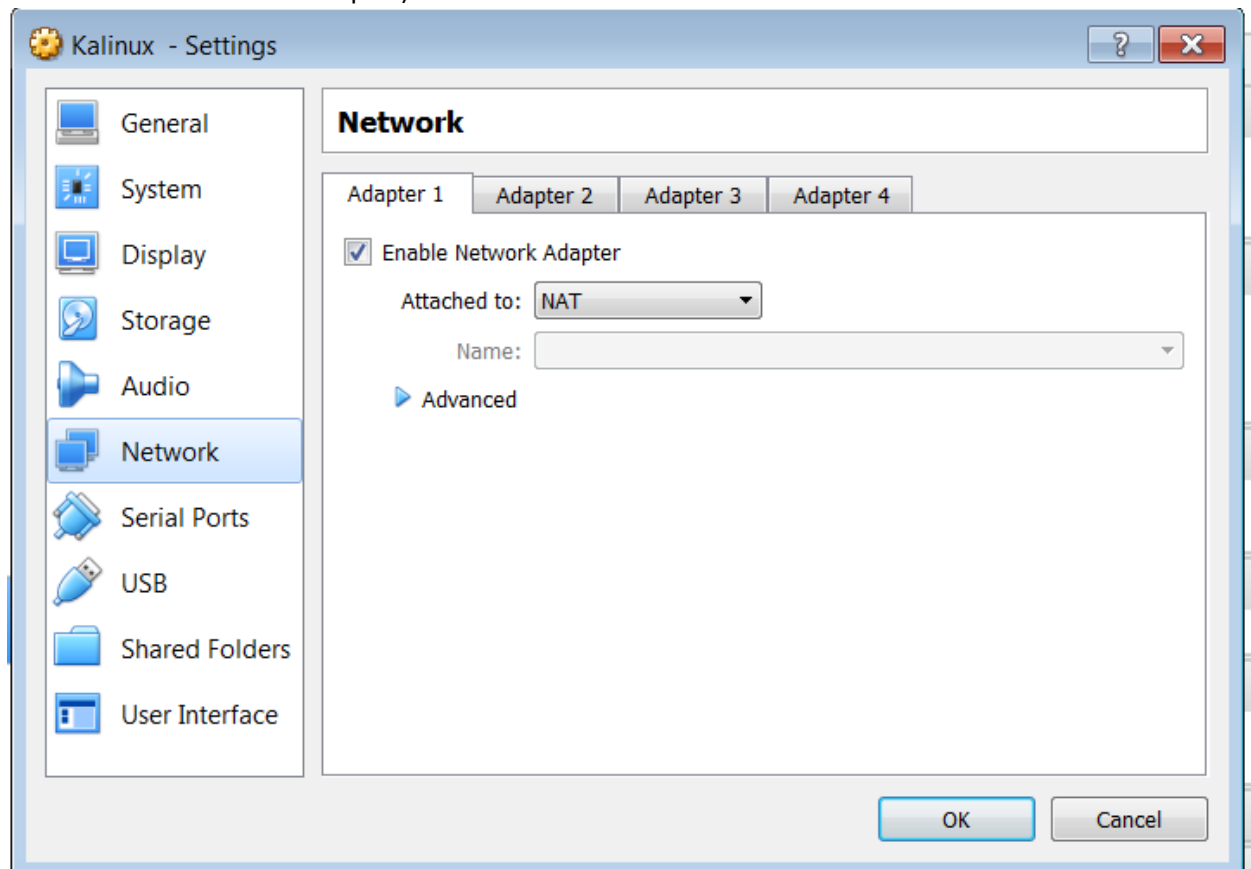
### 7. Adapter settings

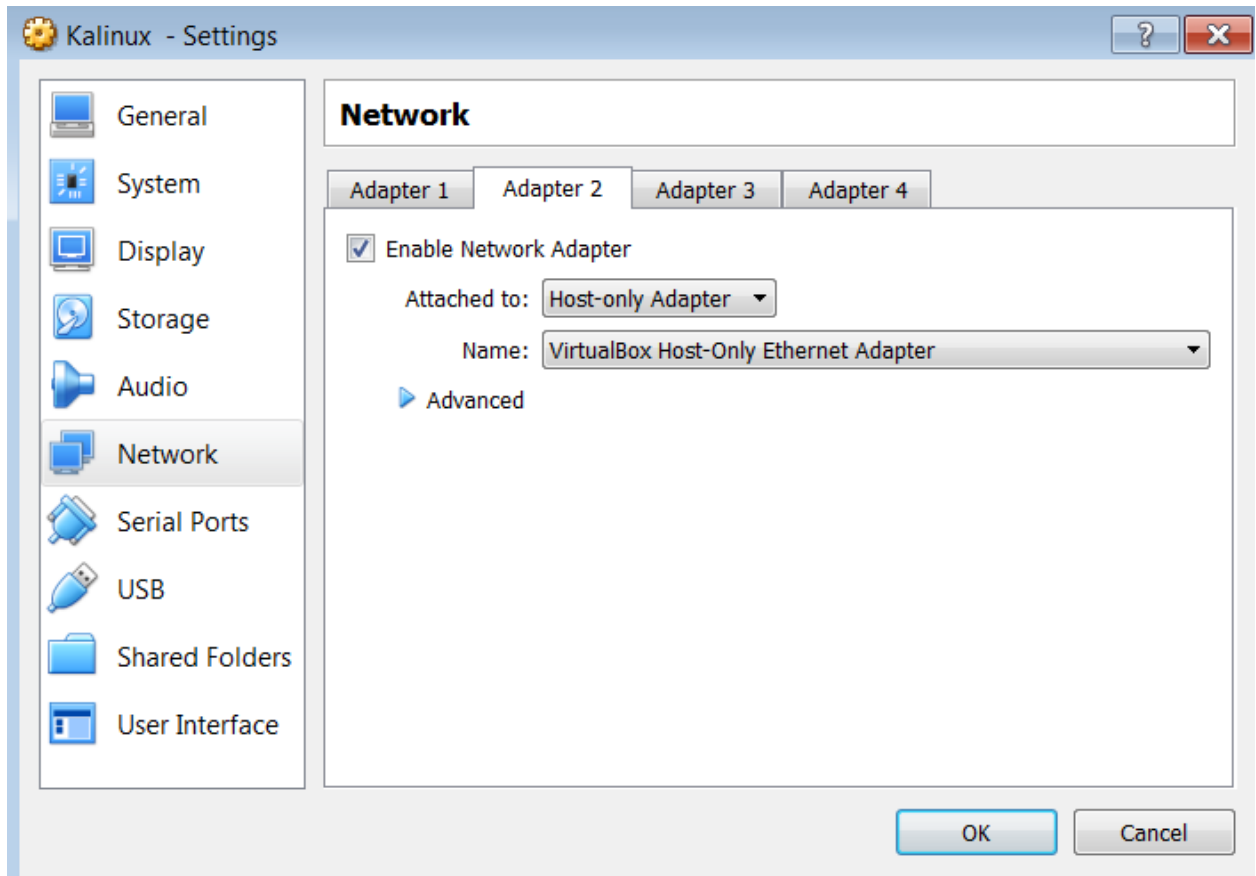


8. Click on enable DHCP server

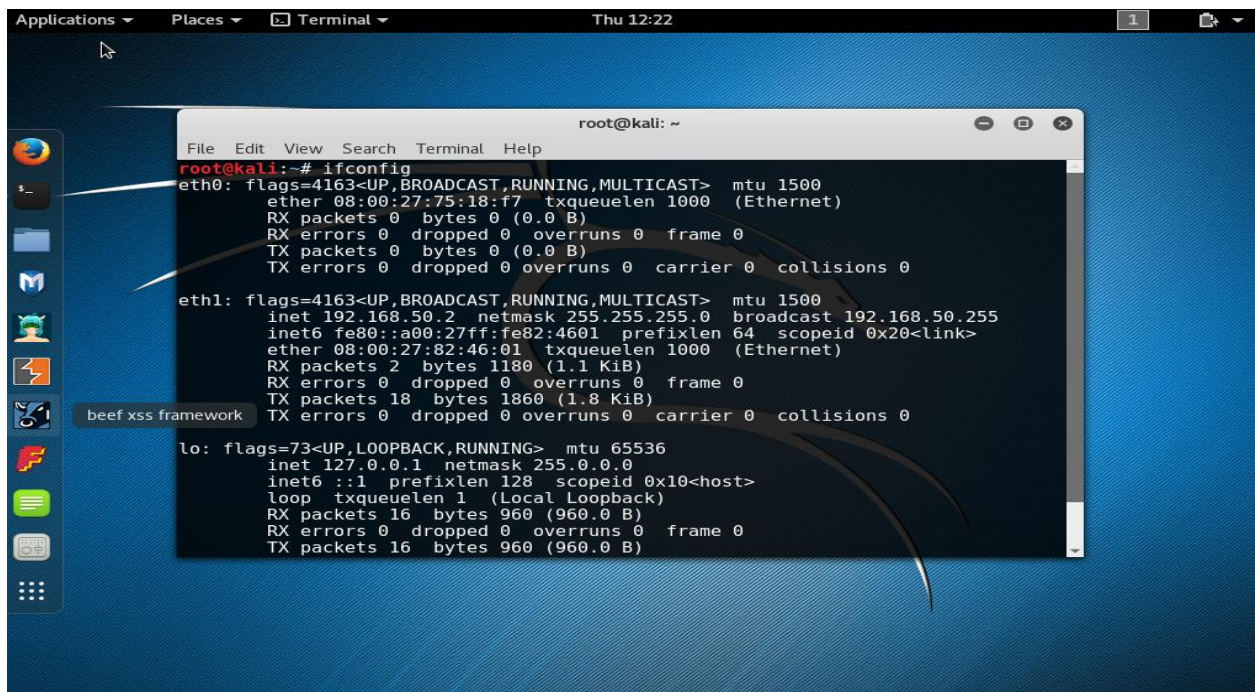


Now select your guest OS (in this case kali linux -> goto settings-> select network -> choose adapter 1 and select NAT -> choose Adapter 2 and select -> Host only network please verify you selected enable network adapter)

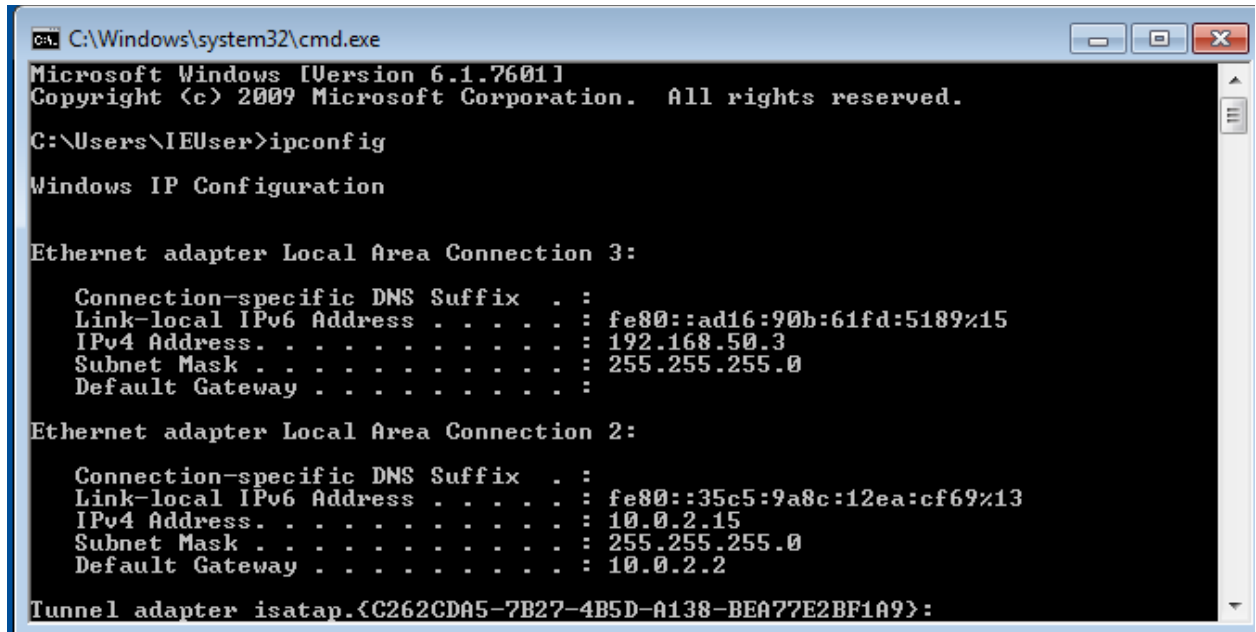




9. Start your guest os (in this case kali ) and check IP address of kali box by using 'ifconfig' command



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



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::ad16:90b:61fd:5189%15
    IPv4 Address. . . . . : 192.168.50.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

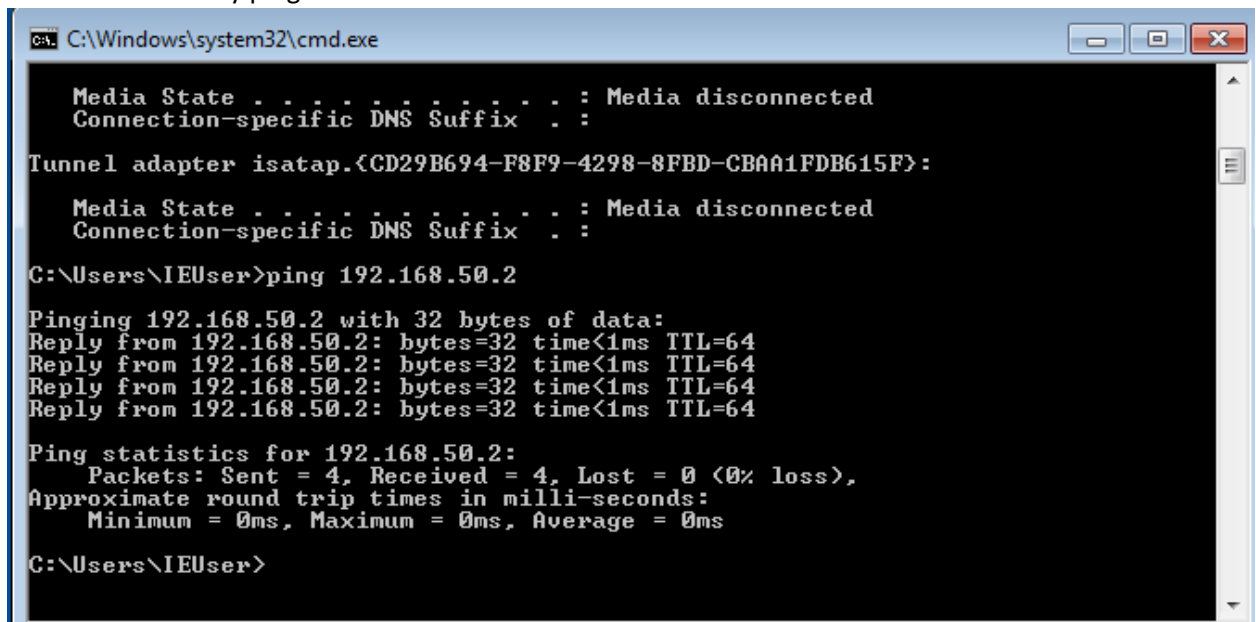
Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::35c5:9a8c:12ea:cf69%13
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.2

Tunnel adapter isatap.{C262CDA5-7B27-4B5D-A138-BEA77E2BF1A9}:

```

11. We successfully ping kali box from windows 7



```
C:\Windows\system32\cmd.exe

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{CD29B694-F8F9-4298-8FBD-CBAA1FDB615F}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

C:\Users\IEUser>ping 192.168.50.2

Pinging 192.168.50.2 with 32 bytes of data:
Reply from 192.168.50.2: bytes=32 time<1ms TTL=64
Reply from 192.168.50.2: bytes=32 time<1ms TTL=64
Reply from 192.168.50.2: bytes=32 time<1ms TTL=64
Reply from 192.168.50.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\IEUser>
```



12. NMAP scan result from kali

```
Nmap scan report for 192.168.50.3
Host is up (0.00032s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
MAC Address: 08:00:27:F3:C6:E0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.2
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.50.2 are closed
```

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

```
root@kali:/etc/network# cat interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
address 192.168.50.10
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
root@kali:/etc/network#
```

**Reference:**

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