Chapter 1

Introduction to Ethical Hacking

Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRACTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

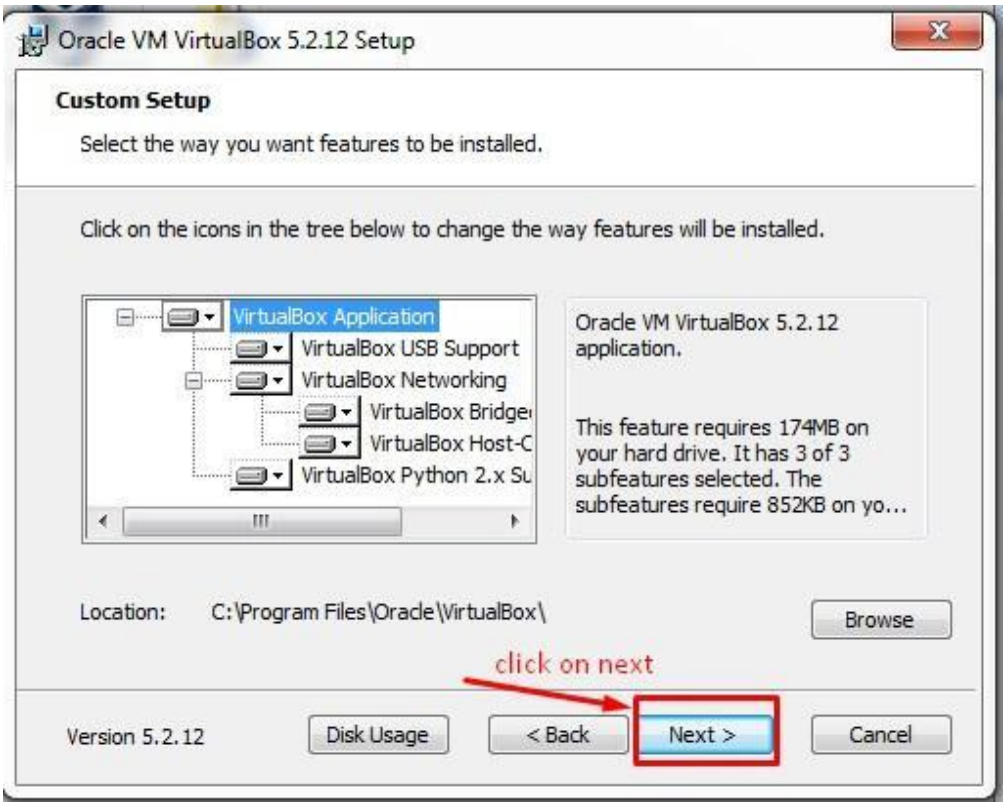
Practical 1: Steps to install VirtualBox on Windows Operating System

Step 1: Download and Install VirtualBox

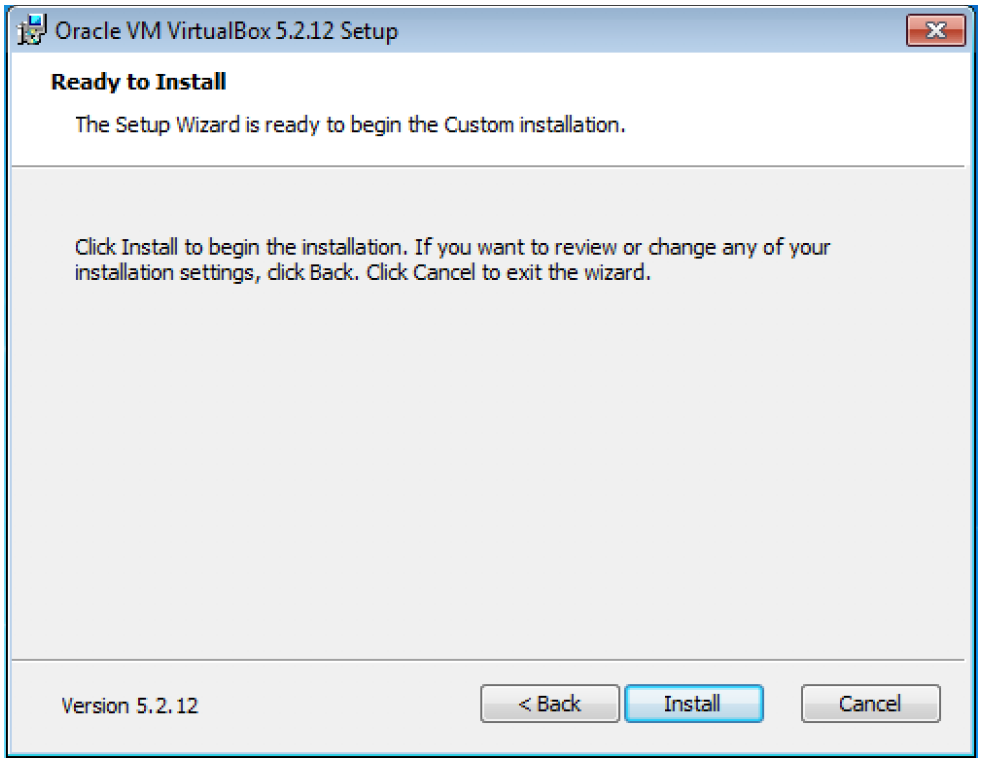
visit www.virtualbox.org/wiki/downloads

under downloads, download VirtualBox setup file for windows hosts

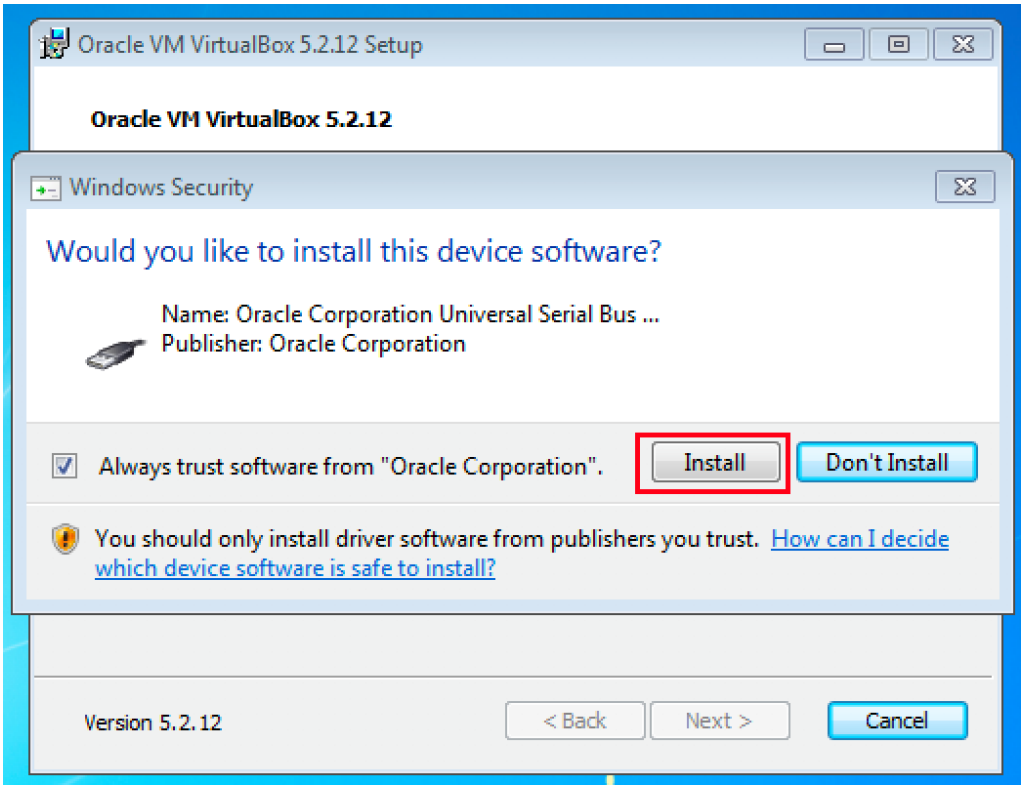
After download, execute setup file to begin VirtualBox installation.



During installation, you will get a network interface warning, Click ***Yes*** to continue (this may interrupt your network connectivity, make sure that you are not downloading any application during the installation process.



During installation, it will prompt to install oracle universal serial bus, make sure to check ***Always trust*** and click ***Install*** to complete VirtualBox installation.

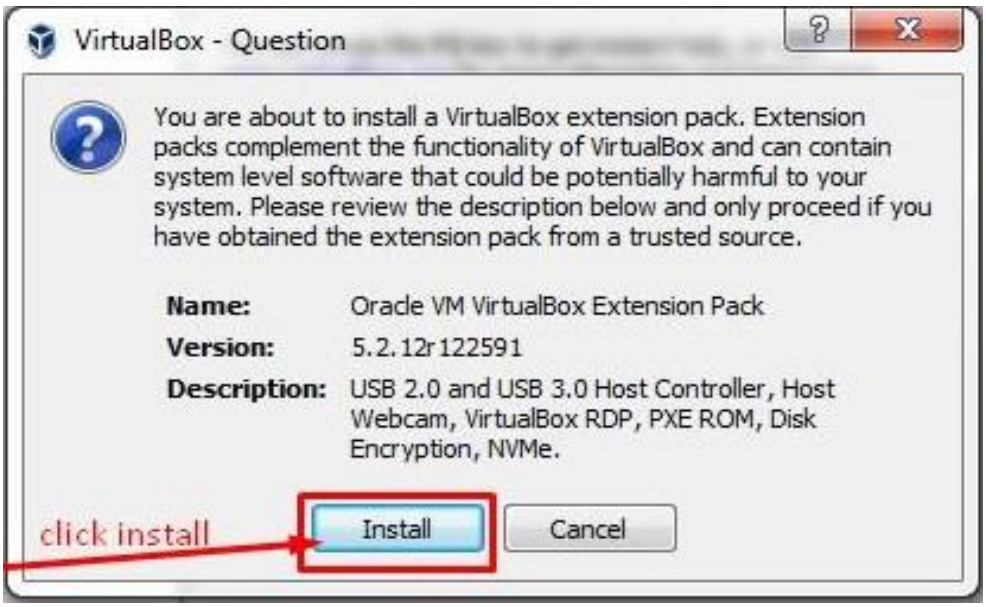


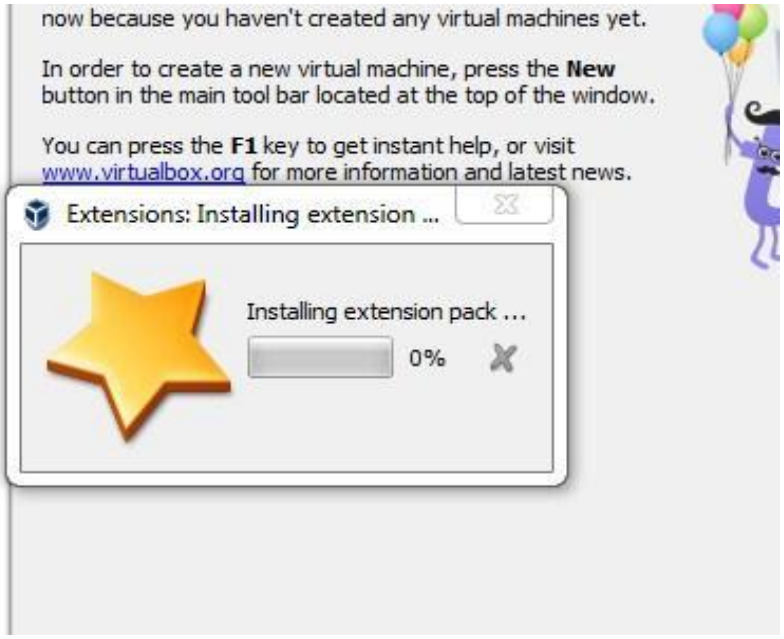
Step 2: Installing Oracle VirtualBox Extension Pack

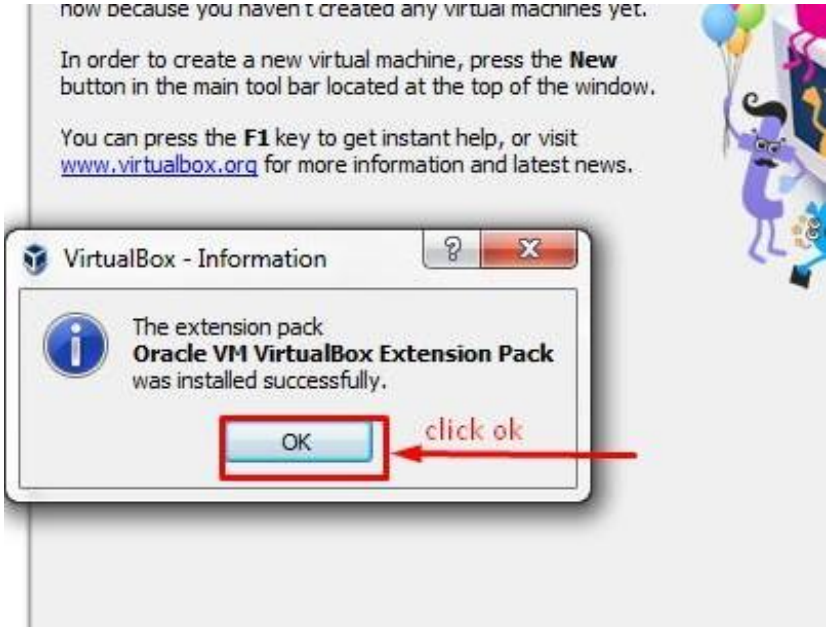
Extension pack extends the functionality of VirtualBox base packages. It allows usage of VRDP (VirtualBox Remote Desktop Protocol), host machine web camera, Virtual USB 2.0/3.0, etc.

Download VirtualBox extension pack for ***All supported platforms*** from following link http://www.virtualbox.org/wiki/downloads (under Oracle VM VirtualBox extension pack).

After download, run extension pack setup file.







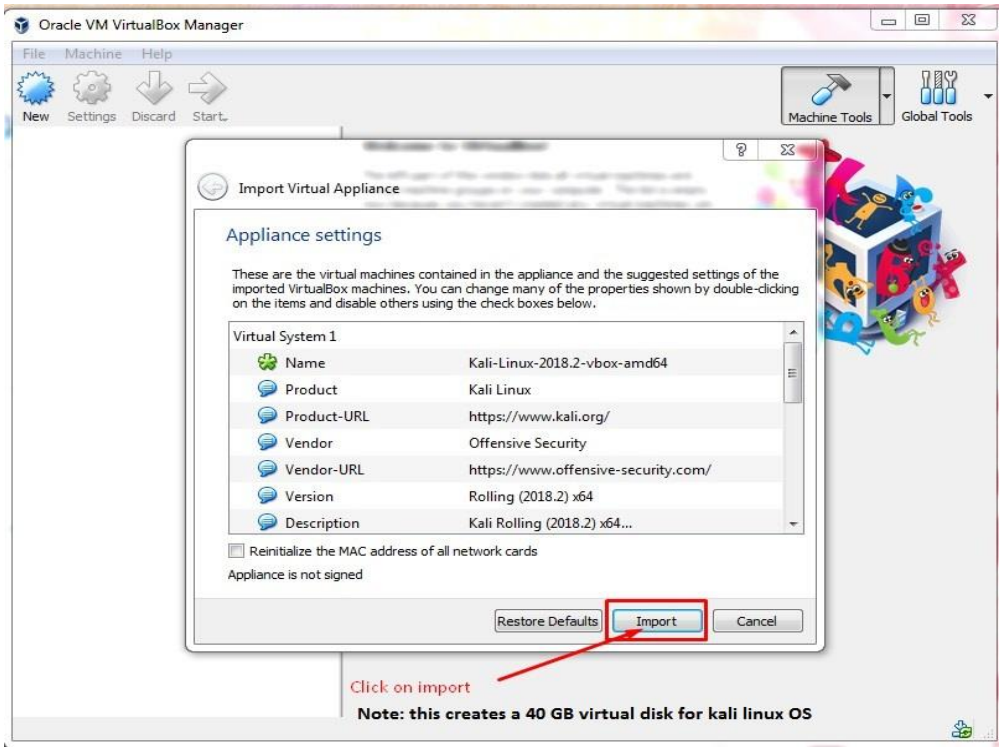
Now, we are ready to install Kali Linux virtual machine.

Practical 2: Installing Kali Linux in VirtualBox

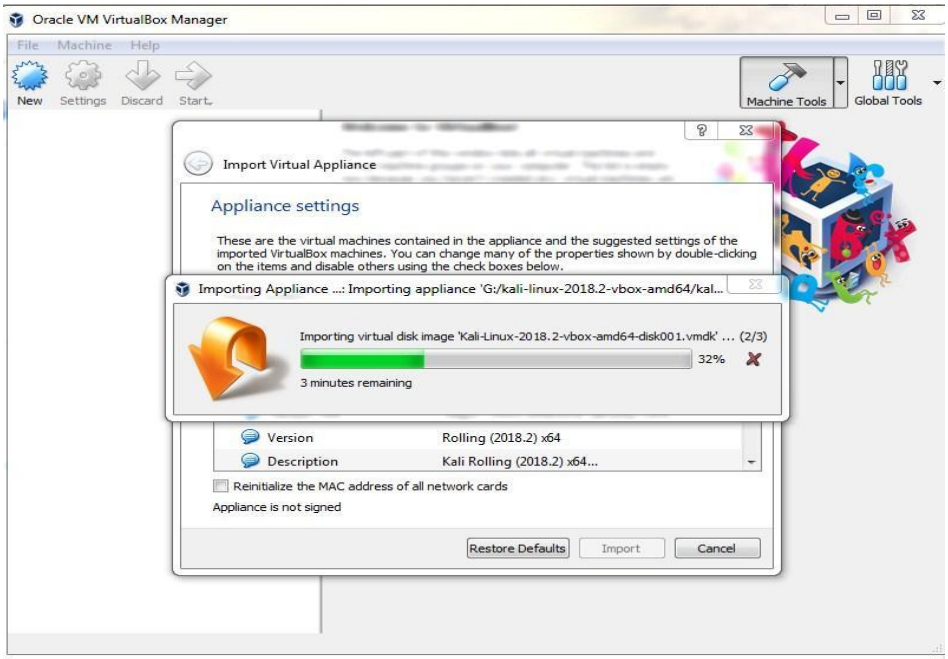
Download Kali Linux VirtualBox image file from following the link (OVA file) https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-hyperv-image-download/

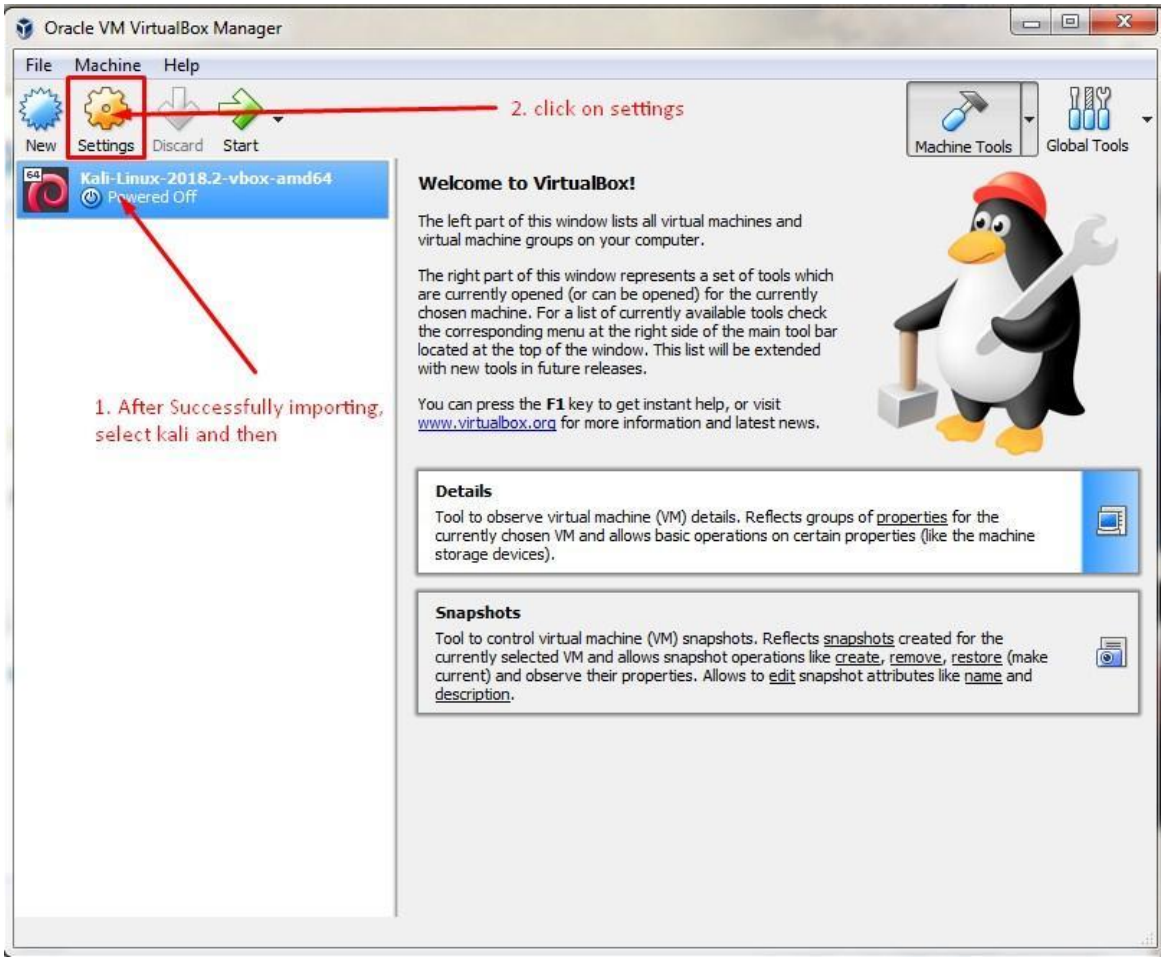
Make sure to verify your system architecture 64-bit/32-bit before you download the virtual image file for VirtualBox. As we have installed Oracle VirtualBox software, we must download VirtualBox image file.

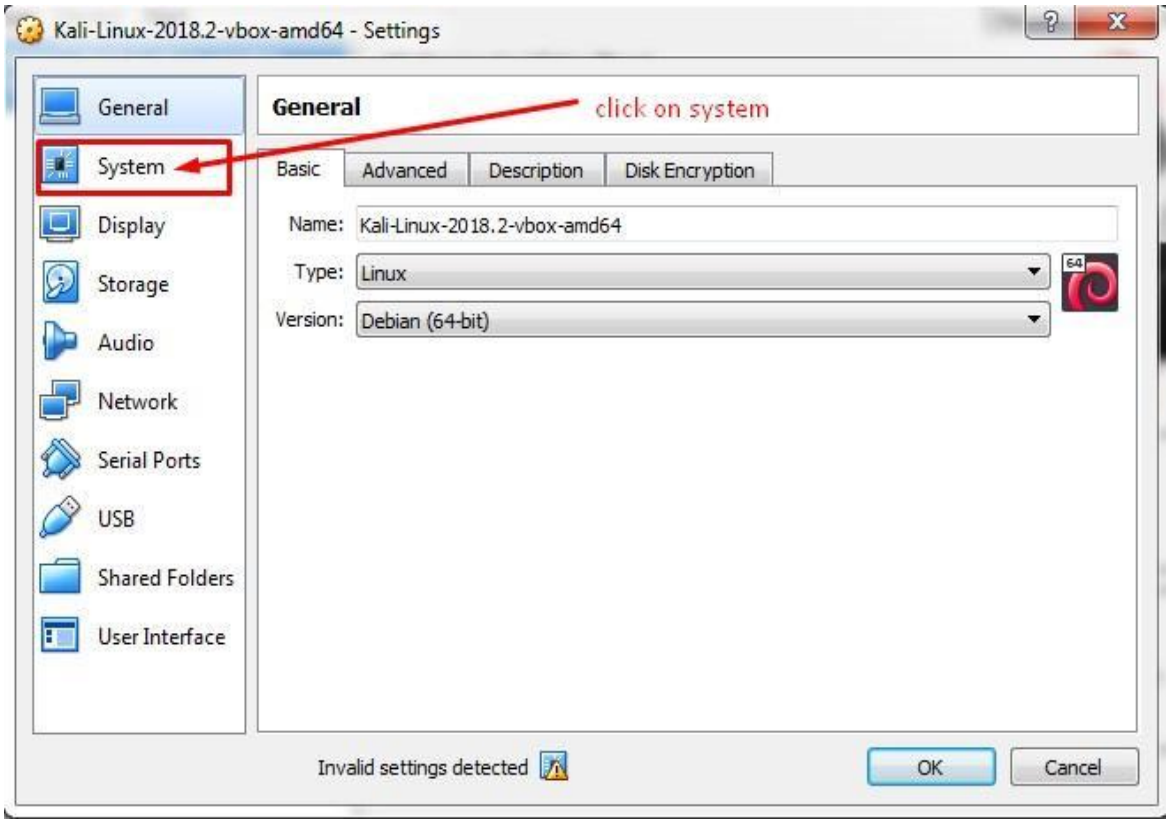
After download, execute .ova file (double-click on file). it starts importing kali Linux into VirtualBox.

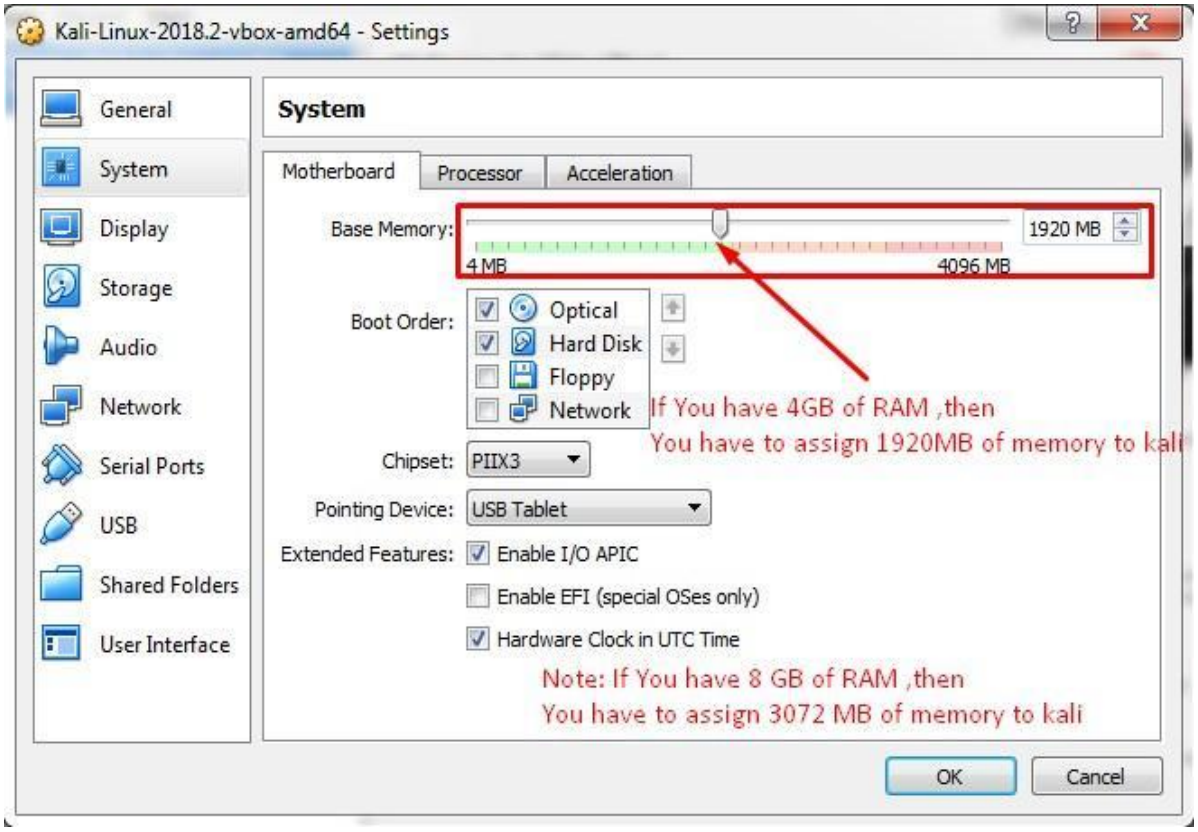


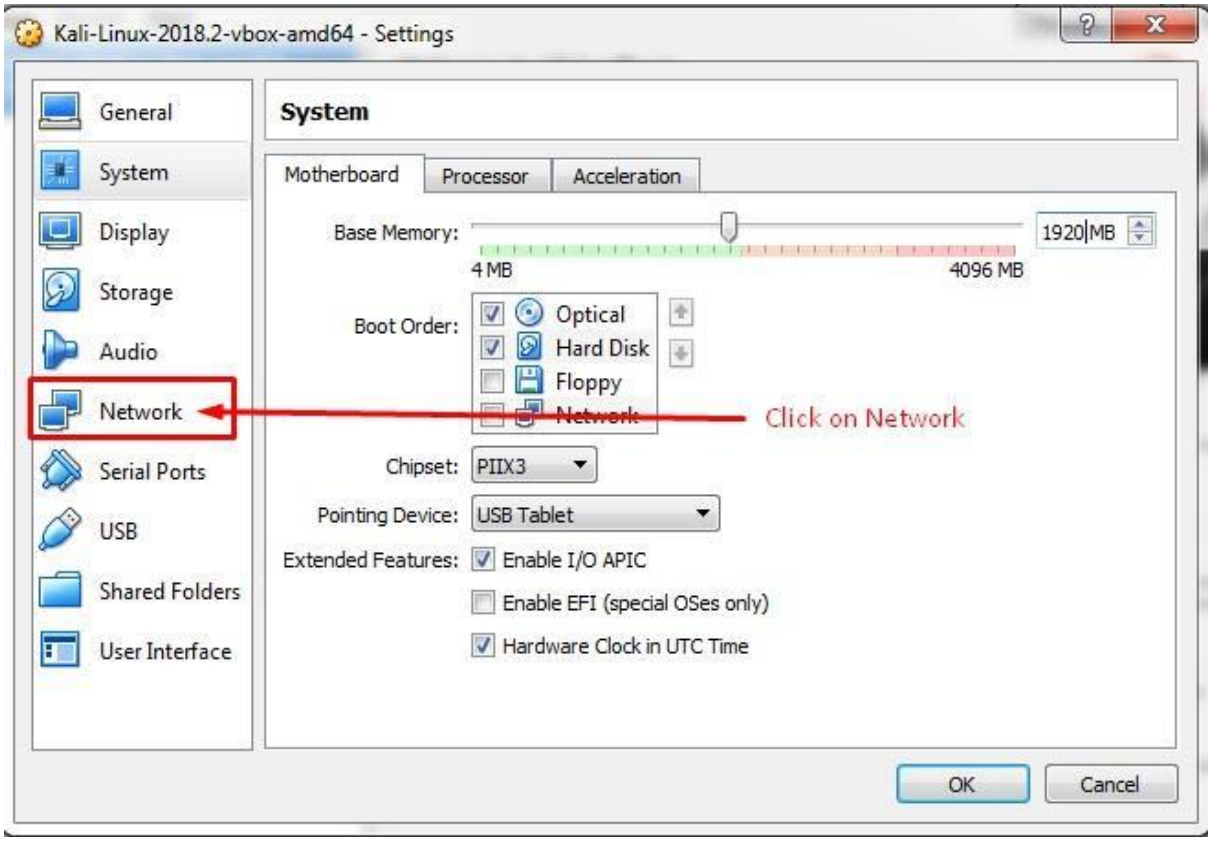
Note: This creates a 40 GB virtual disk for Kali Linux OS

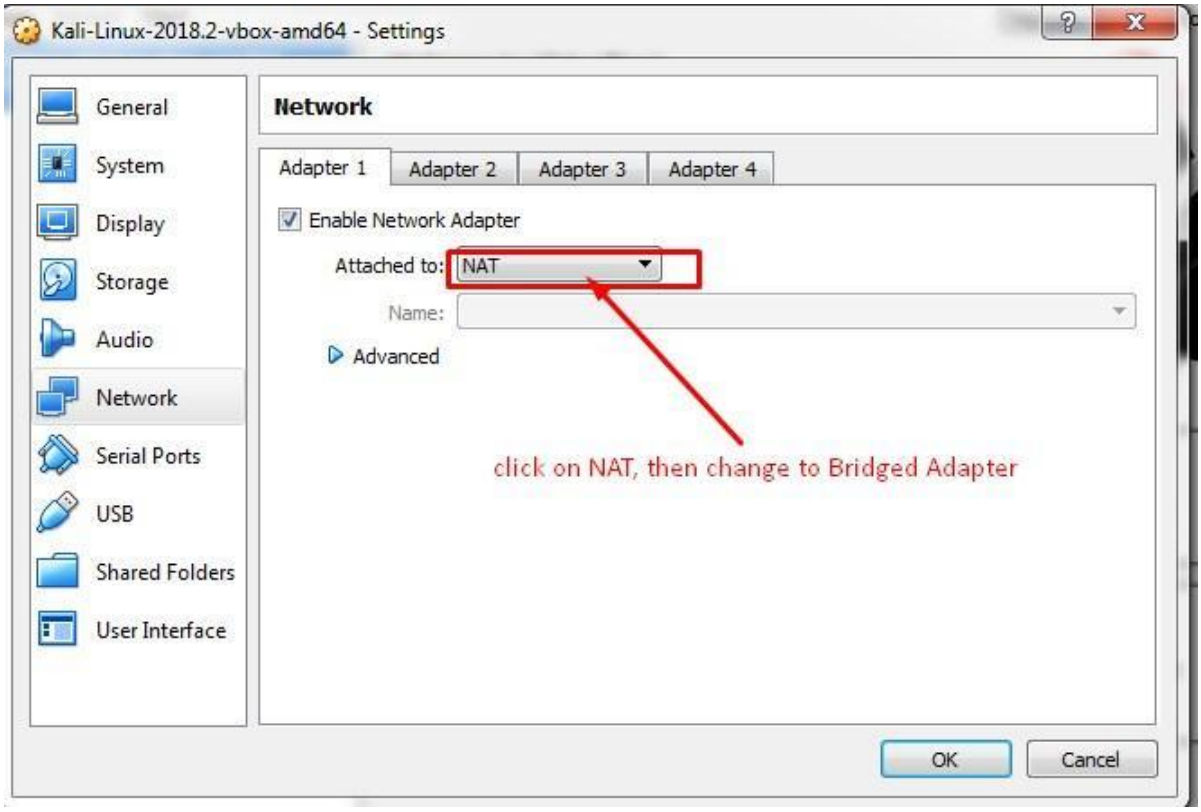


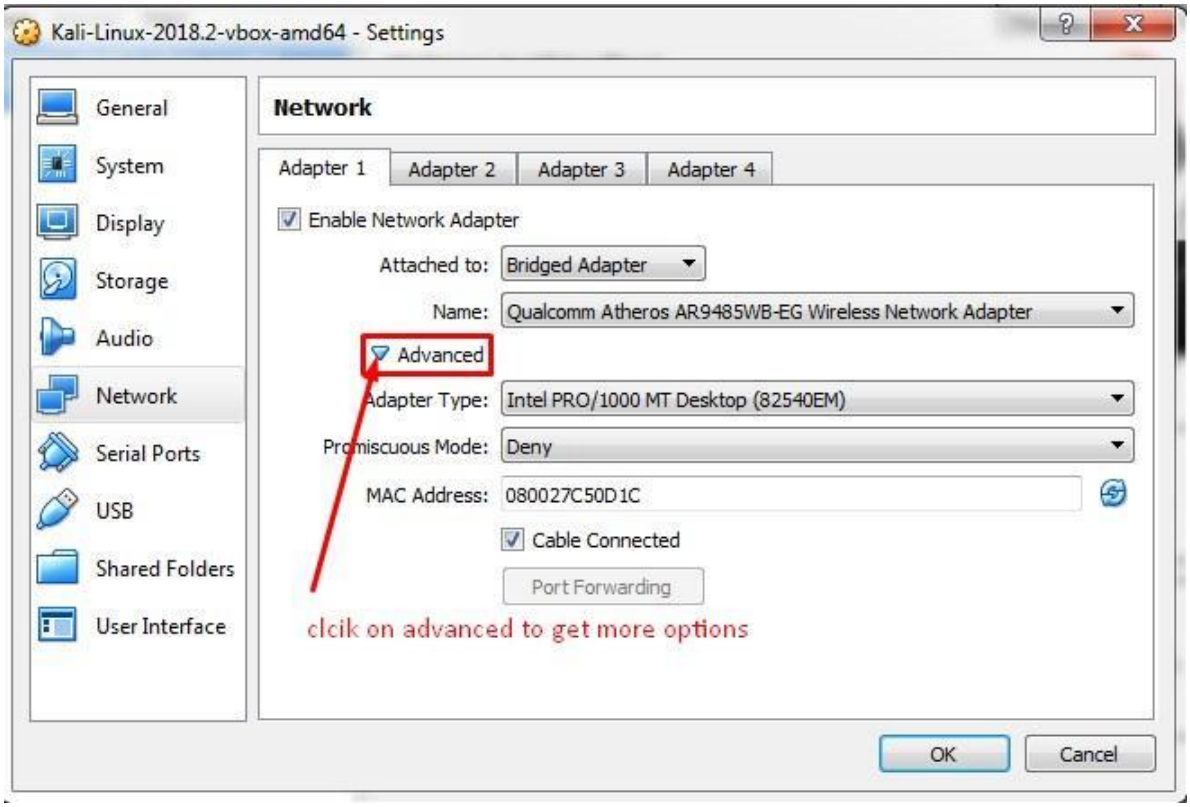

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
2. click on settings
Machine Tools
Global Tools
Kali-Linux-2018.2-vbox-amd64
Powered Off
1. After Successfully importing, select kali and then
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual 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 chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.
Details
Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).
Snapshots
Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.

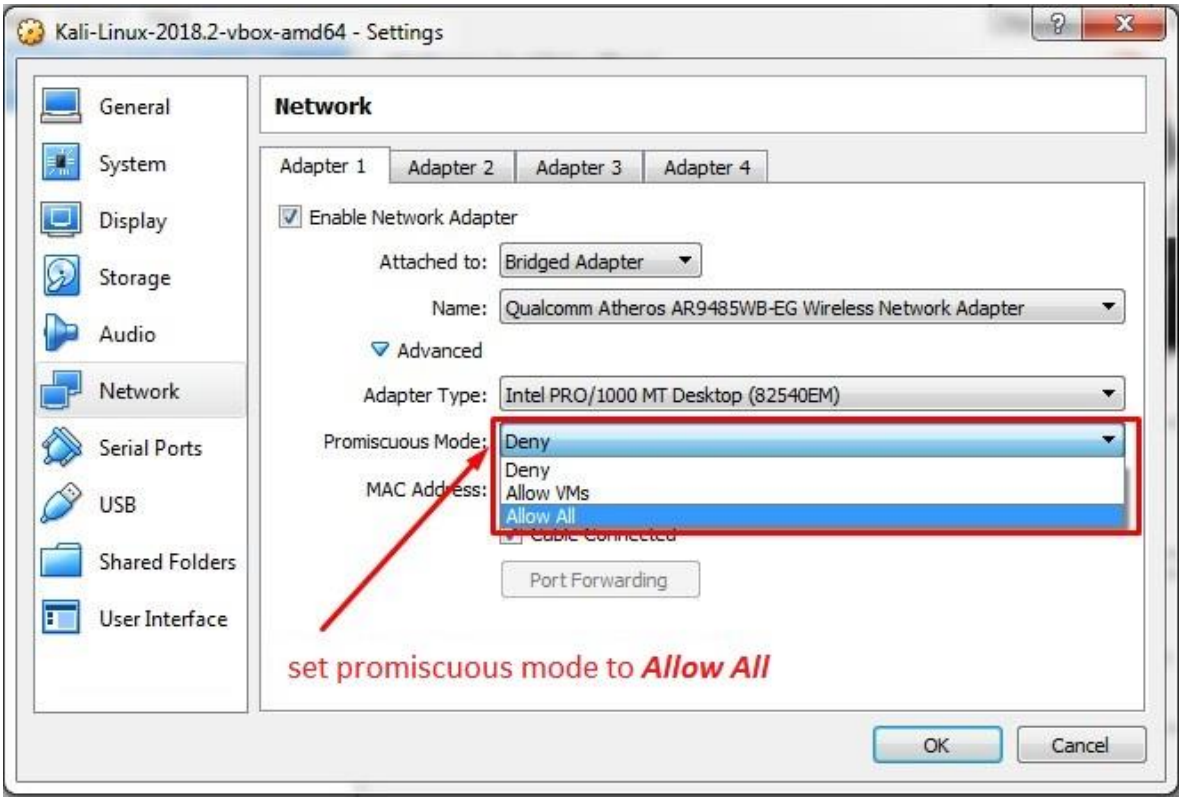

Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
General
click on system
Basic
Advanced
Description
Disk Encryption
Name: Kali-Linux-2018.2-vbox-amd64
Type: Linux
Version: Debian (64-bit)
Invalid settings detected
OK
Cancel

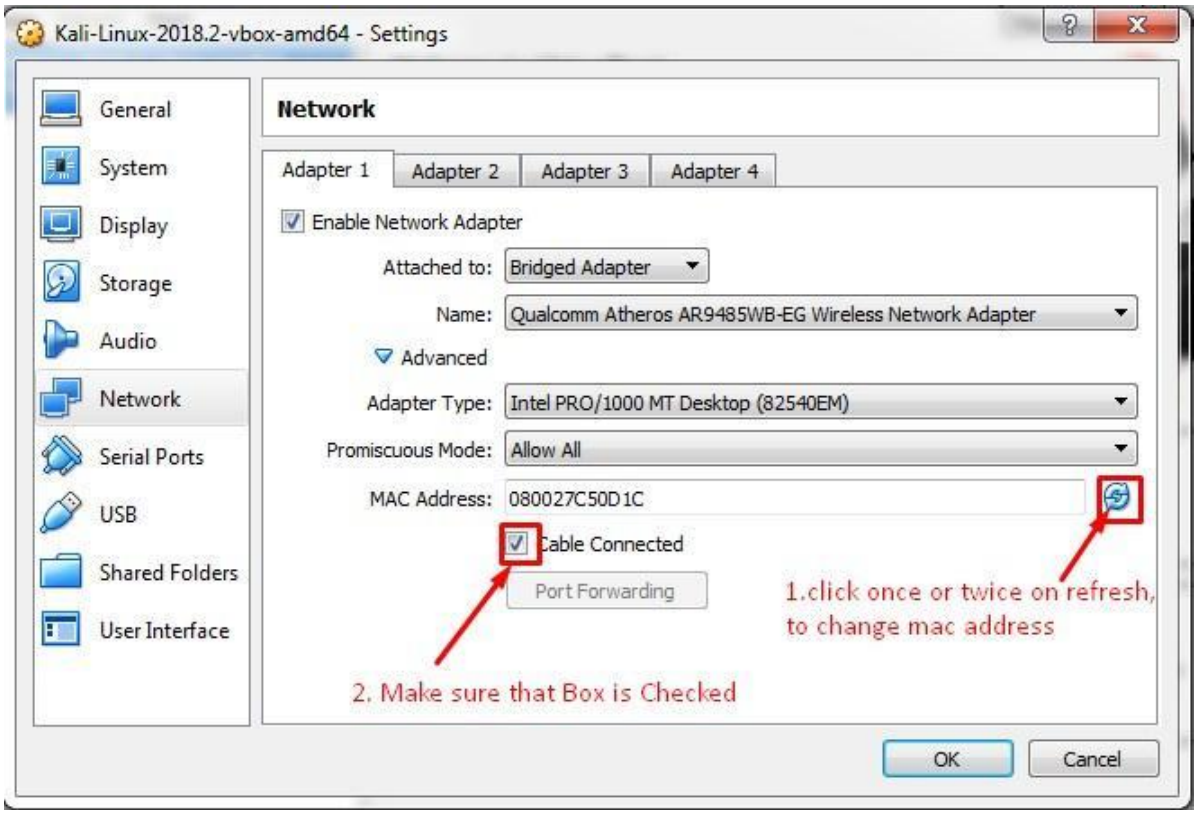

Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
1920 MB
4 MB
4096 MB
Boot Order:
Optical
Hard Disk
Floppy
Network
If You have 4GB of RAM ,then
You have to assign 1920MB of memory to kali
Chipset:
PIIX3
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable EFI (special OSes only)
Hardware Clock in UTC Time
Note: If You have 8 GB of RAM ,then
You have to assign 3072 MB of memory to kali
OK
Cancel

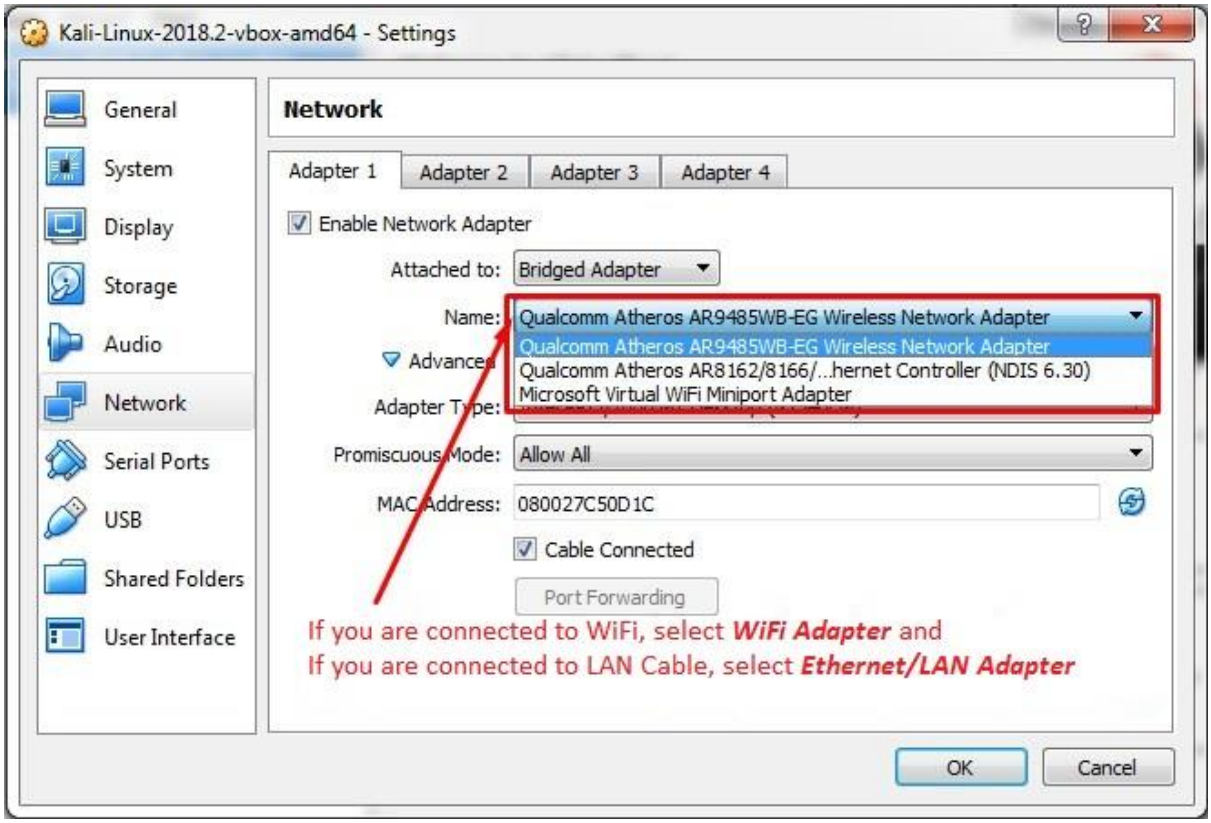

Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
1920 MB
4 MB
4096 MB
Boot Order:
Optical
Hard Disk
Floppy
Network
Click on Network
Chipset:
PIIX3
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable EFI (special OSes only)
Hardware Clock in UTC Time
OK
Cancel


Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced
click on NAT, then change to Bridged Adapter
OK
Cancel

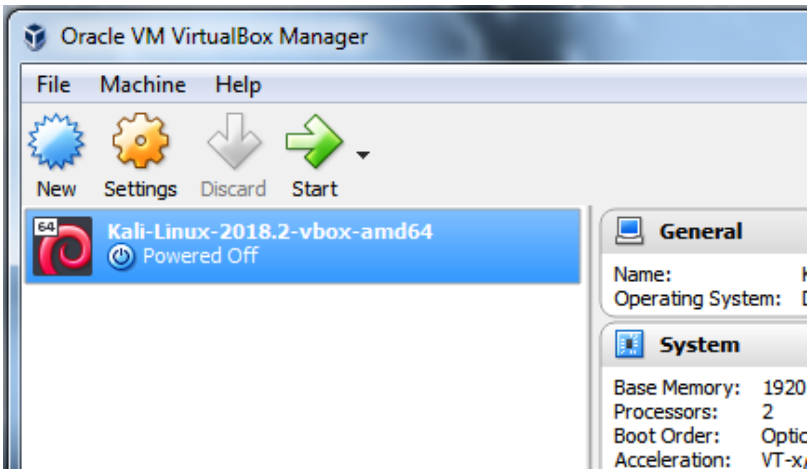

Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Bridged Adapter
Name:
Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Deny
MAC Address:
080027C50D1C
Cable Connected
Port Forwarding
clcik on advanced to get more options
OK
Cancel


Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
Deny
Allow VMs
Allow All
MAC Address:
Port Forwarding
set promiscuous mode to Allow All
OK
Cancel


Kali-Linux-2018.2-vbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
Advanced
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Allow All
MAC Address: 080027C50D1C
Cable Connected
Port Forwarding
1.click once or twice on refresh, to change mac address
2. Make sure that Box is Checked
OK
Cancel



Click ***ok*** to complete basic configuration. From VirtualBox main menu, select Kali Linux and click on start to load kali Linux operating system as shown below.



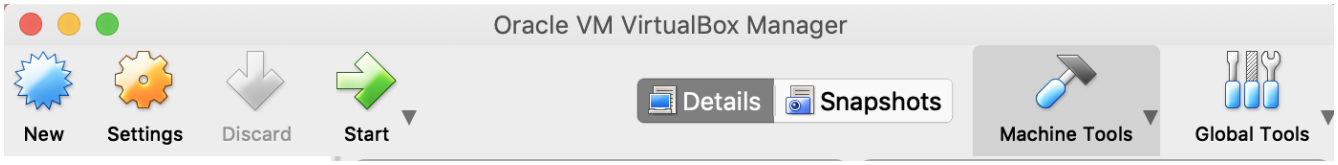
Practical 3: Installing Metasploitable2 in VirtualBox

Metasploitable 2 is a vulnerable machine designed for testing and practice. Metasploitable2 focuses on vulnerabilities at the system level which can be exploited with the help of the Metasploit framework (to be covered in Chapter 6).

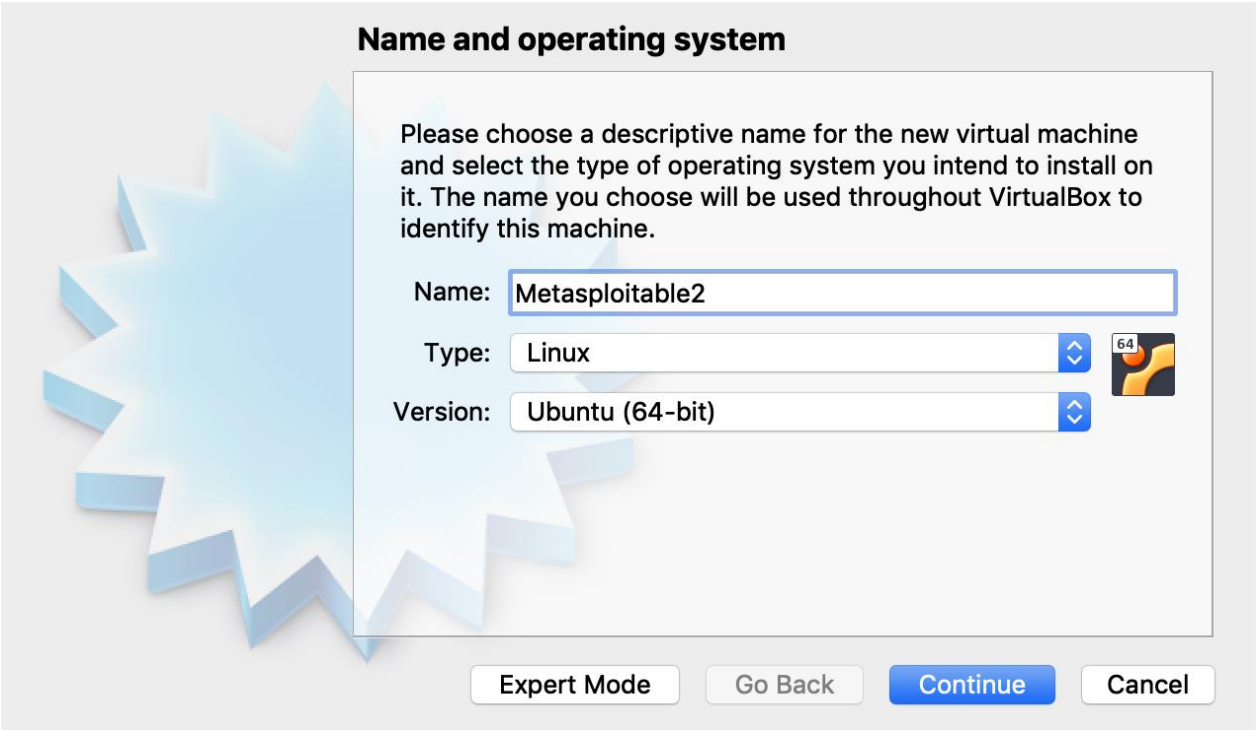
Download Metasploitable2 (Linux) from the following link and extract the .zip file.

"https://sourceforge.net/projects/metasploitable/files/Metasploitable2/"

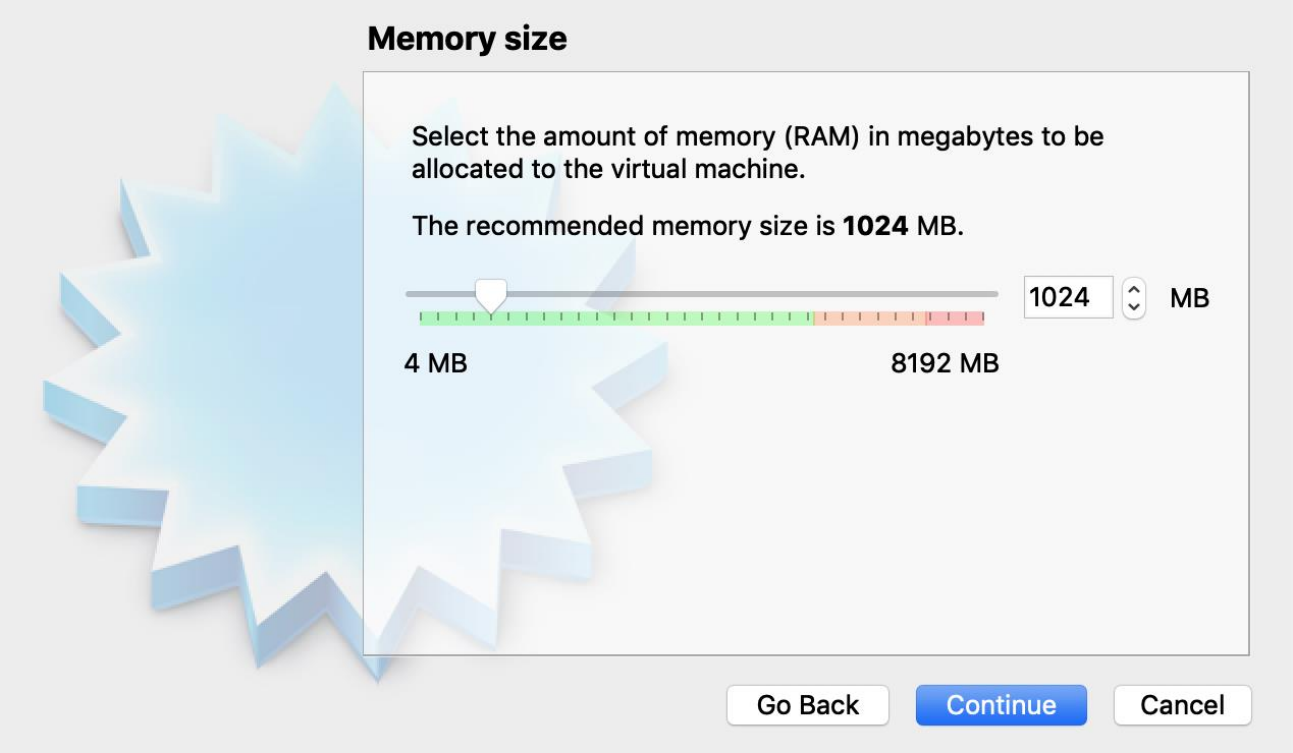
Open VirtualBox and click on New button on the top left corner.



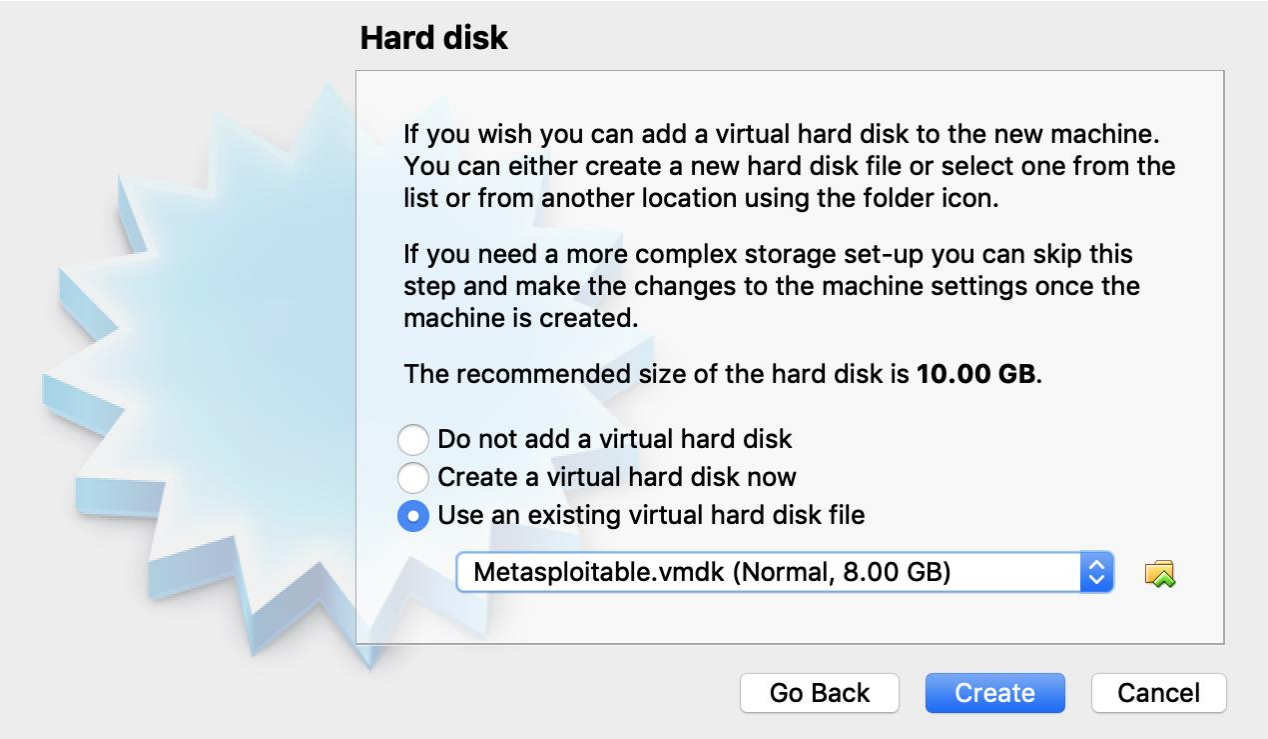
Add **Name**, and select the **Type**, and **Version** as shown in the below image and click on continue



Set Memory size to 1024MB as shown in below screenshot and click on **continue**



On this menu, choose, **Use an existing Virtual hard disk file** and load the **.vmdk** from the extracted directory (Metasploitable2). Click on **Create** to complete the process.



Configure network settings for this virtual machine (as shown in practical 2). Set the network adapter mode to **Bridged** and Promiscuous made to **Allow all.** These settings allow other machines on the network to access this vulnerable virtual machine (Metasploitable 2).

Select Metasploitable2 from VirtualBox menu and click on **Start** to start Metasploitable2 virtual machine. The default login credentials are **login: msfadmin** and **password: msfadmin**

```
 * Starting deferred execution scheduler atd                              [ OK ]
 * Starting periodic command scheduler crond                              [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                               [ OK ]
 * Starting web server apache2                                            [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                          [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

Practical 4: Install Tor Browser in Kali Linux

Step 1: Download Tor Browser

Tor helps in browsing the internet anonymously by hiding Our IP Address. Tor can also be used to access blocked websites. Black-hat Hackers use tor to access the dark web to perform illegal activities by protecting their identity.

Download tor browser from the following link:

https://www.torproject.org/download/download-easy.html.en

Step 2: Tor Browser Installation

Open terminal in Kali Linux, change current location to point the directory that holds previously downloaded file (by default, downloaded files will be saved in ***Downloads*** directory).

```
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
tor-browser-linux64-7.5.6_en-US.tar.xz
root@kali:~/Downloads# tar xvf tor-browser-linux64-7.5.6_en-US.tar.xz
```

execute above commands to extract the downloaded ***tar.xz*** file

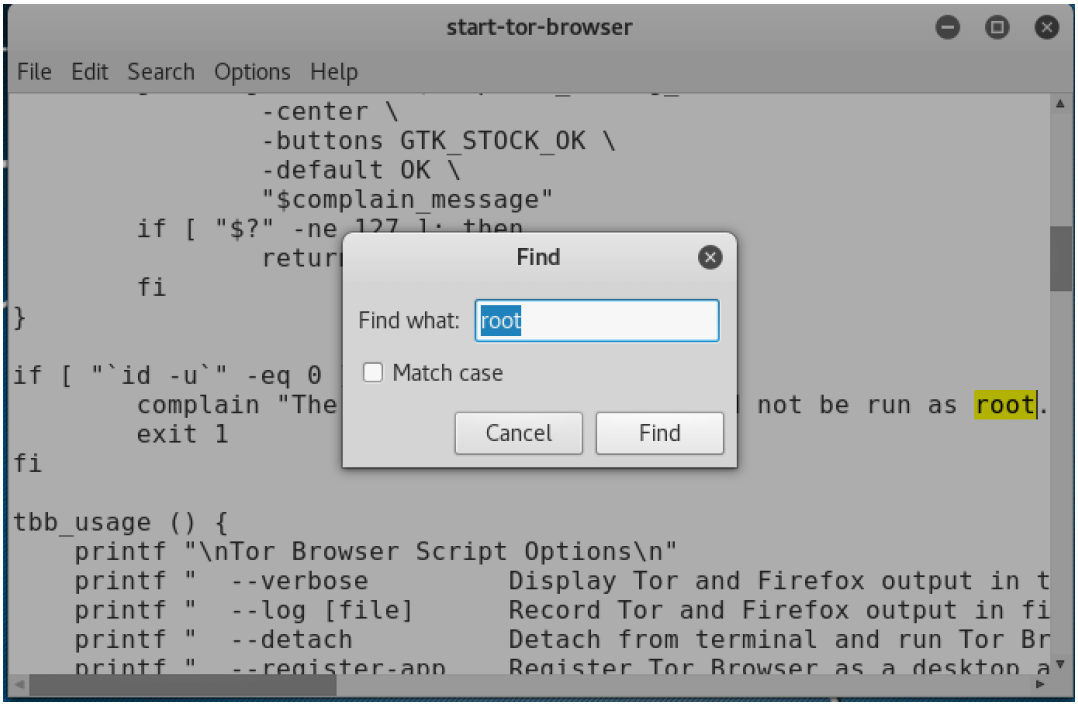
```
root@kali:~/Downloads# ls
tor-browser_en-US  tor-browser-linux64-7.5.6_en-US.tar.xz
root@kali:~/Downloads# cd tor-browser_en-US/
root@kali:~/Downloads/tor-browser_en-US# ls
Browser  start-tor-browser.desktop
root@kali:~/Downloads/tor-browser_en-US# cd Browser/
root@kali:~/Downloads/tor-browser_en-US/Browser# ls
application.ini     libfreeblpriv3.so  libplc4.so         run-mozilla.sh
browser             liblgpllibs.so     libplds4.so        start-tor-browser
chrome.manifest     libmozavcodec.so   libsmime3.so       start-tor-browser.desktop
defaults            libmozavutil.so    libsoftokn3.so     tbb_version.json
dependentlibs.list  libmozsandbox.so   libssl3.so         TorBrowser
dictionaries        libmozsqlite3.so   libxul.so          updater
execdesktop         libnspr4.so        omni.ja            updater.ini
firefox             libnss3.so         platform.ini       update-settings.ini
fonts               libnssckbi.so      plugin-container
icons               libnssdbm3.so      precomplete
icudt58l.dat        libnssutil3.so     removed-files
```

Configuring Tor Browser to run as root:

To run tor browser as the root user, we need to make changes in the ***start-tor-browser*** file. Execute the following command to open and edit the ***start-tor-browser*** file.

```
root@kali:~/Downloads/tor-browser_en-US/Browser# leafpad start-tor-browser
```

After opening the file, search (Ctrl + F) for keyword ***'root'***

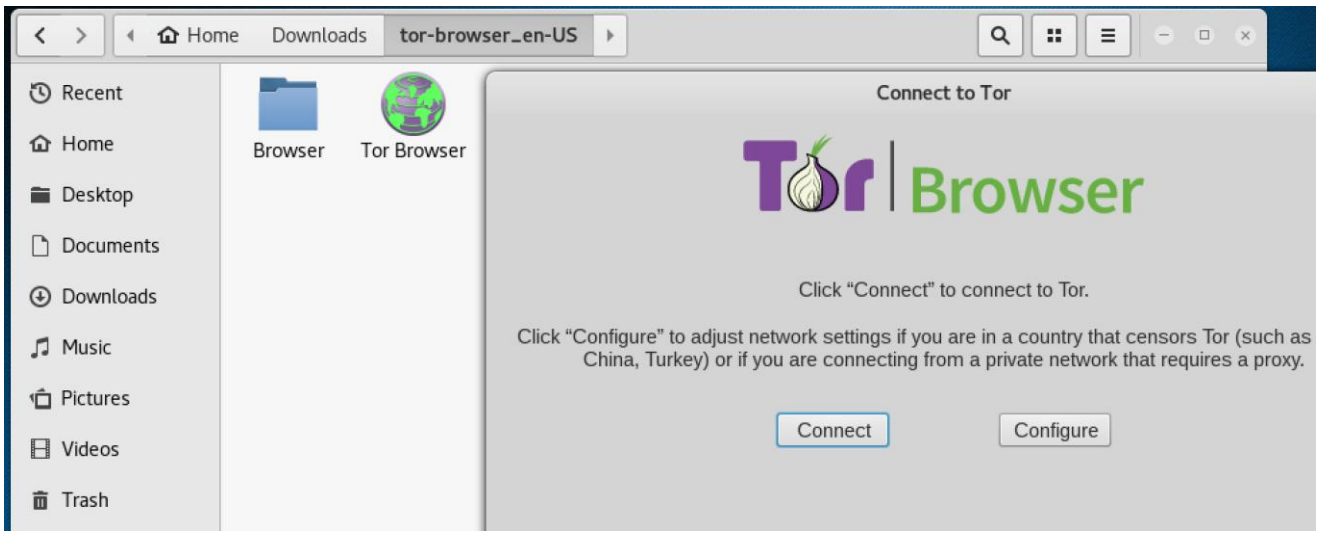


Modify four lines of code in the file as shown below (add **#** at the starting point of each line)

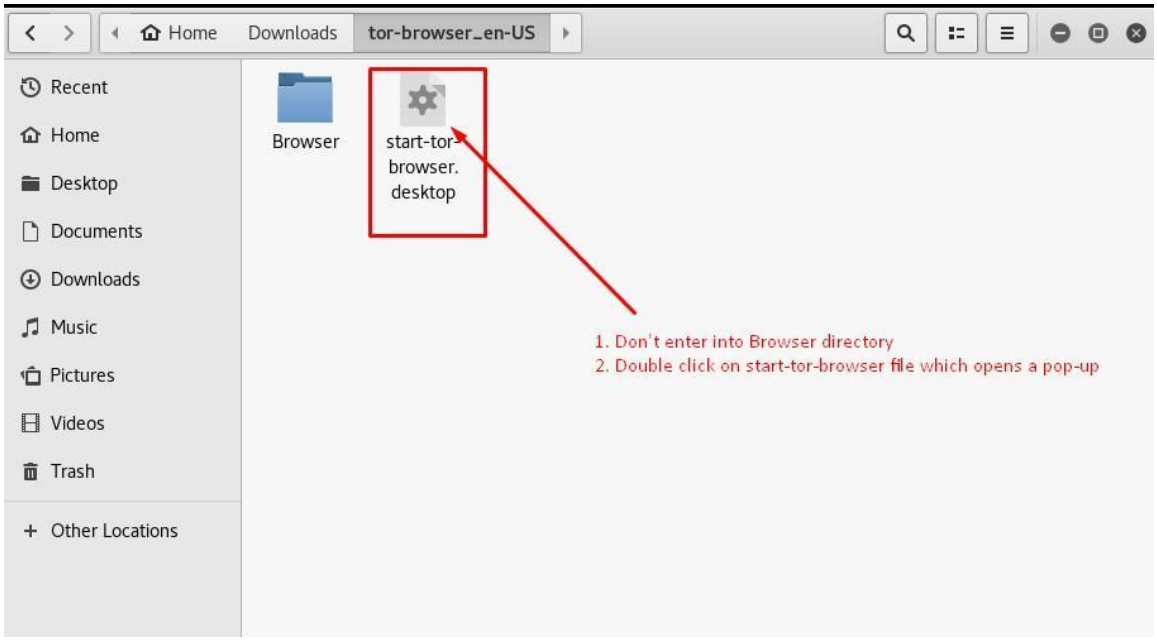
```
#if [ "`id -u`" -eq 0 ]; then
#       complain "The Tor Browser Bundle should not be run as root.  Exiting."
#       exit 1
#fi
```

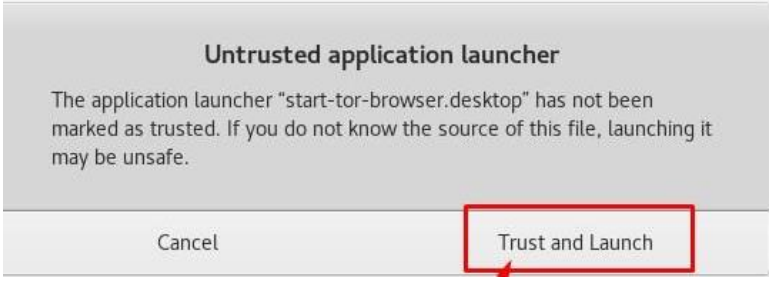
after making the above-said modifications save and close the file.

To start the browser, execute ***Tor Browser*** located in the ***Downloads*** directory



In few cases, we may see the file named as ***start-tor-browser. Desktop,*** double-click on that file if prompted click on ***Trust and Launch*** which opens tor browser.


Home
Downloads
tor-browser_en-US
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
Browser
start-tor-browser.desktop
1. Don't enter into Browser directory
2. Double click on start-tor-browser file which opens a pop-up


Untrusted application launcher
The application launcher "start-tor-browser.desktop" has not been marked as trusted. If you do not know the source of this file, launching it may be unsafe.
Cancel
Trust and Launch

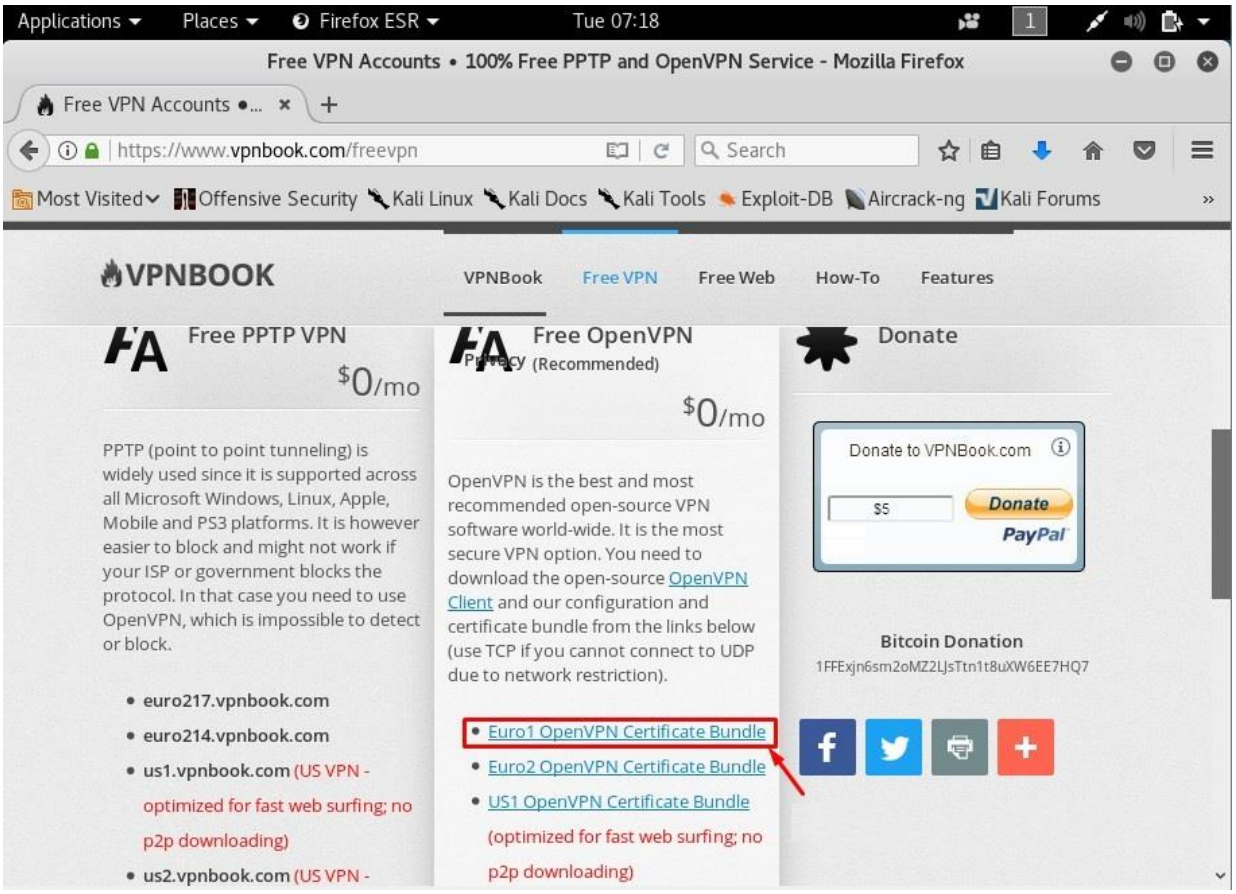
Practical 5: Installing VPNBook in Kali Linux

Virtual Private Network (VPN) is most often used by IT companies to protect sensitive data shared on the network. VPN establishes a virtual point-to-point connection which allows employees in the organization to send or receive data across public networks as if the devices are connected to the organization private network. VPNBook is one such software that enables individuals to run VPN on their personal computer. We can use VPNBook to hide our identity (IP address). VPNBook is a free open-source VPN software.

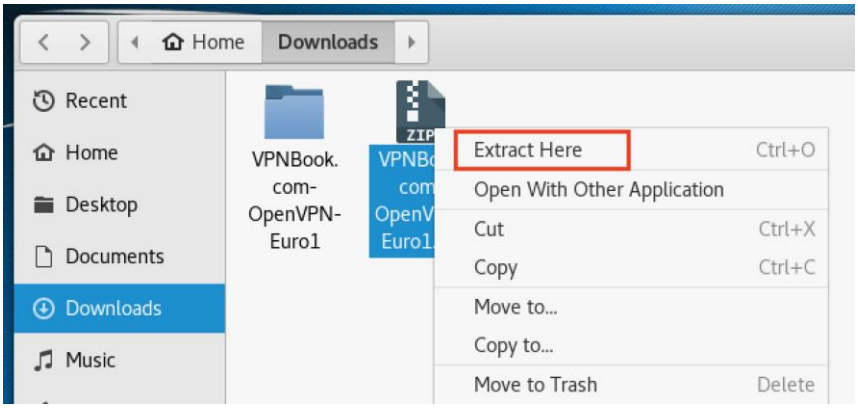
To download VPNBook, visit following website

https://www.vpnbook.com/freevpn

under ***Free OpenVPN*** Option, select any of the bundles to download (***Euro 1 OpenVPN Certificate Bundle*** or ***Euro 2 OpenVPN Certificate Bundle*** is recommended)



Open Download directory and extract ***VPNBook.com-OpenVPN-Euro1.zip***



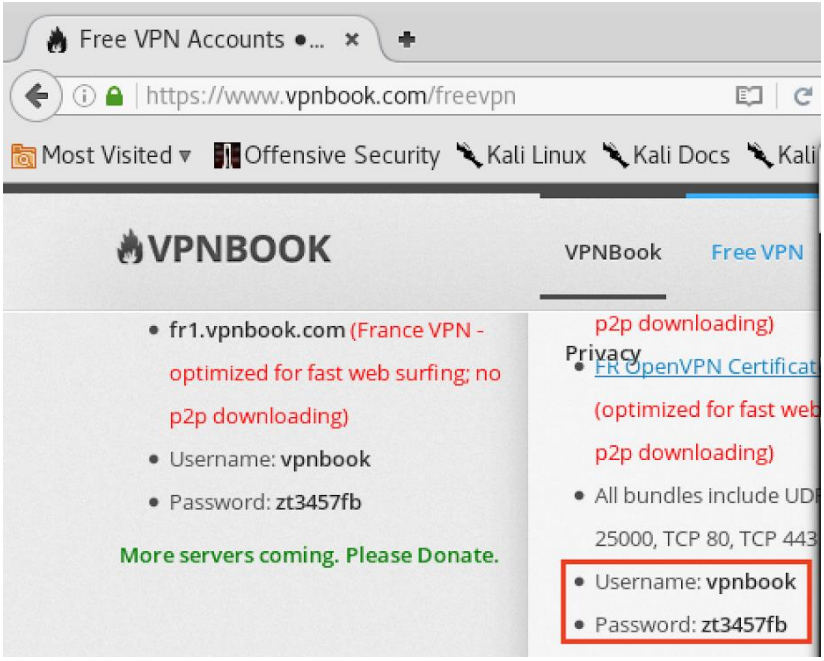
Open terminal in Kali Linux, change current location to point ***Downloads*** directory that holds VPNBook bundle.

```
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
VPNBook.com-OpenVPN-Euro1  VPNBook.com-OpenVPN-Euro1.zip
root@kali:~/Downloads# cd VPNBook.com-OpenVPN-Euro1/
root@kali:~/Downloads/VPNBook.com-OpenVPN-Euro1# ls
vpnbook-euro1-tcp443.ovpn  vpnbook-euro1-udp25000.ovpn
vpnbook-euro1-tcp80.ovpn   vpnbook-euro1-udp53.ovpn
```

Select ***vpnbook-euro1-tcp443.ovpn*** file and execute the following command.

```
root@kali:~/Downloads/VPNBook.com-OpenVPN-Euro1# openvpn vpnbook-euro1-tcp443.ovpn
Wed Jul 11 19:03:42 2018 OpenVPN 2.3.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOL
 [PKCS11] [MH] [IPv6] built on May 23 2016
Wed Jul 11 19:03:42 2018 library versions: OpenSSL 1.0.2h  3 May 2016, LZO 2.08
Enter Auth Username: *******
Enter Auth Password: ********
```

We can get username and password from VPNBook website



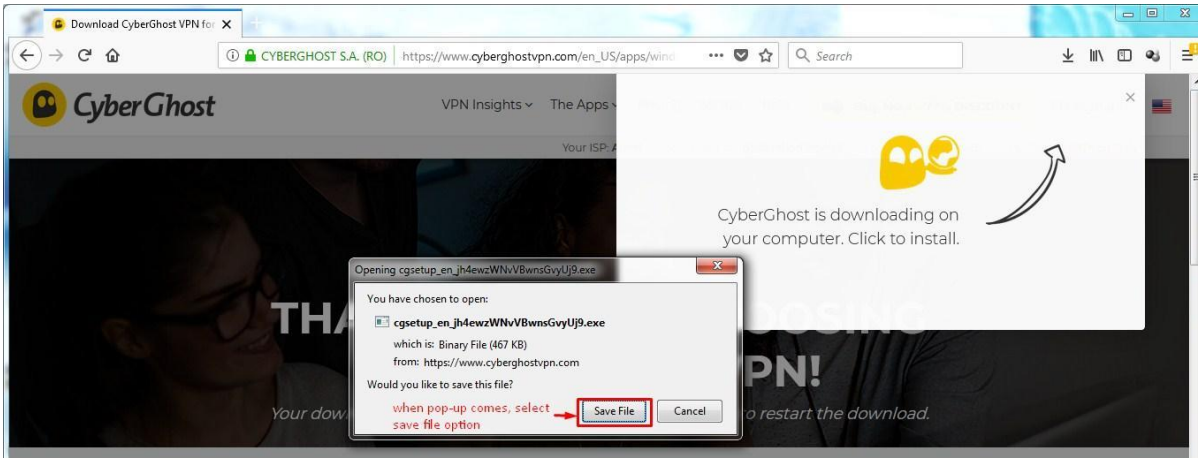
After executing the above command, wait until it displays ***Initialization Sequence Completed*** message***.***

```
Wed Jul 11 19:16:49 2018 TUN/TAP device tun1 opened
Wed Jul 11 19:16:49 2018 TUN/TAP TX queue length set to 100
Wed Jul 11 19:16:49 2018 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Jul 11 19:16:49 2018 /sbin/ip link set dev tun1 up mtu 1500
Wed Jul 11 19:16:49 2018 /sbin/ip addr add dev tun1 local 10.9.0.22 peer 10.9.0.21
Wed Jul 11 19:16:51 2018 /sbin/ip route add 176.126.237.217/32 via 192.168.0.1
Wed Jul 11 19:16:51 2018 /sbin/ip route add 0.0.0.0/1 via 10.9.0.21
Wed Jul 11 19:16:51 2018 /sbin/ip route add 128.0.0.0/1 via 10.9.0.21
Wed Jul 11 19:16:51 2018 /sbin/ip route add 10.9.0.1/32 via 10.9.0.21
Wed Jul 11 19:16:51 2018 Initialization Sequence Completed
```

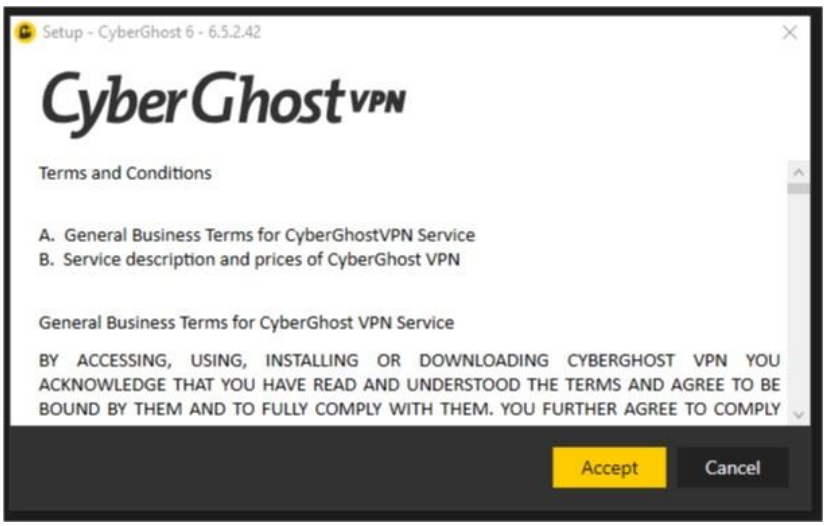
Now we can use any browser to surf the internet anonymously (to confirm, you can visit www.whatismyipaddress.com).

Practical 6: Installing CyberGhost VPN on Windows Platform

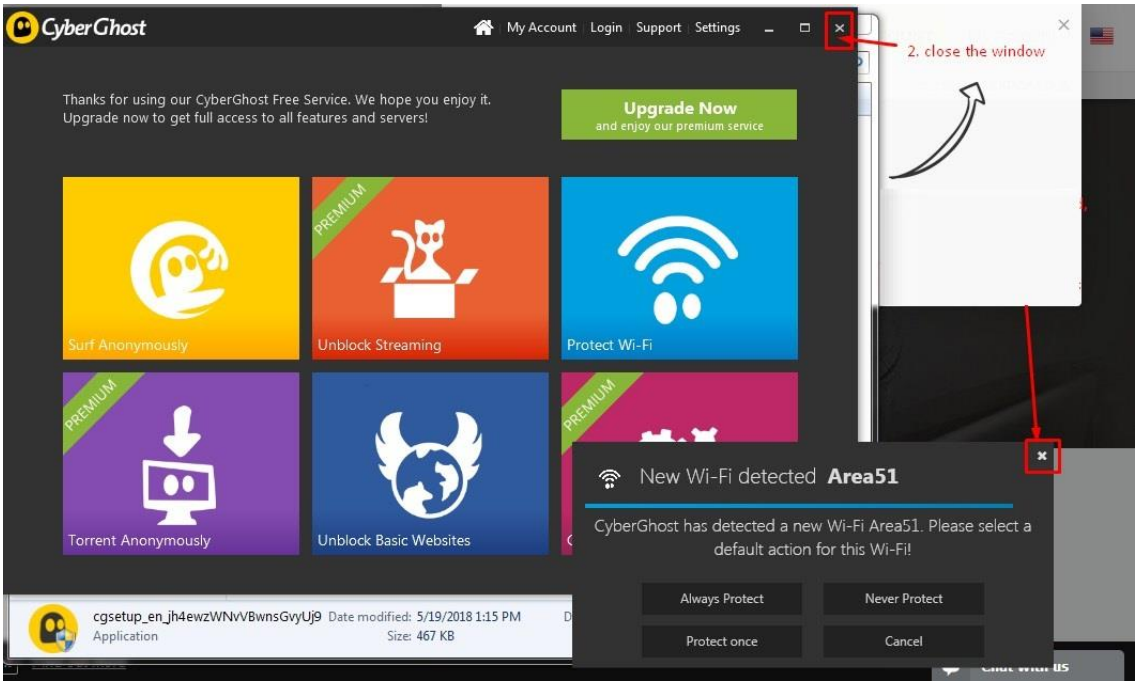
Visit https://www.cyberghostvpn.com/en_US/ to download ***a free version*** of CyberGhost VPN.



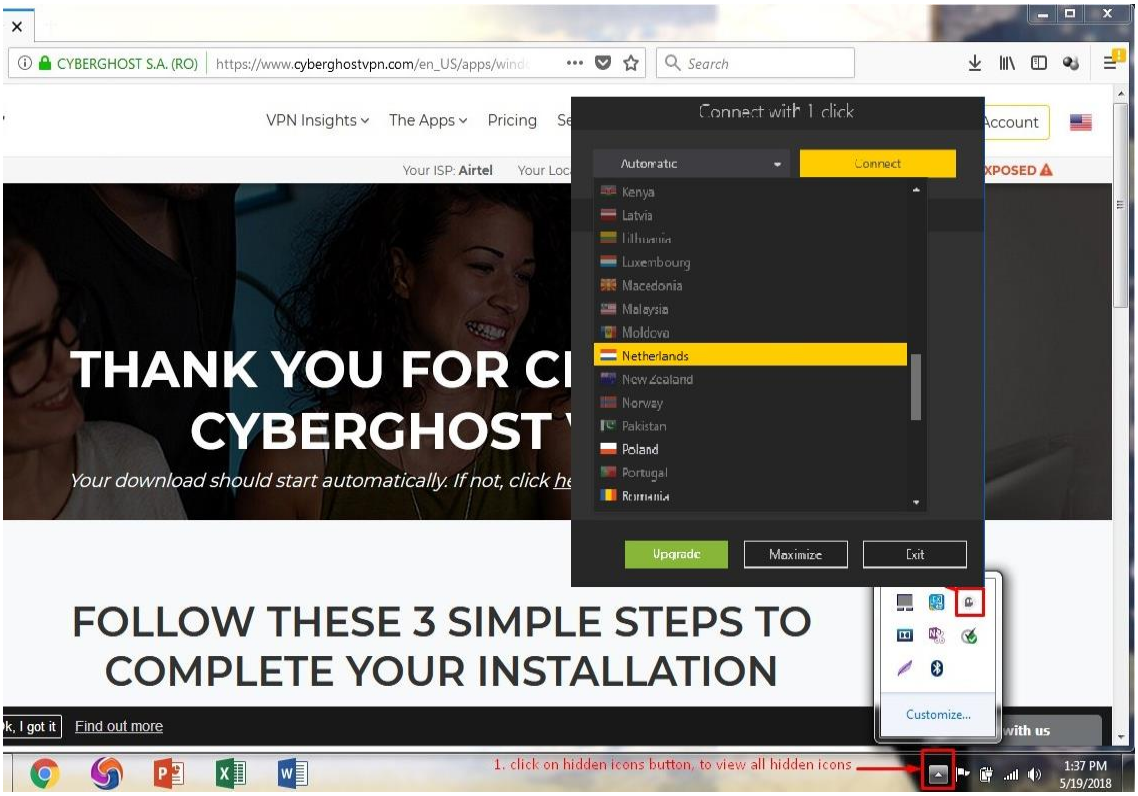
After download, execute setup file to install CyberGhost VPN.



After installation, follow the steps explained in following images to run CyberGhost VPN



To spoof the IP address, right-click on CyberGhost icon and select one of the country as shown below and click on connect.



As we are running the free version of CyberGhost software, we need to wait for a specific time (as shown in below image) to get our IP spoofed.

When we get our turn, CyberGhost VPN software will assign an IP address from the selected country. Now we can use any browser to surf the internet anonymously (to confirm, visit www.ipaddress.com).