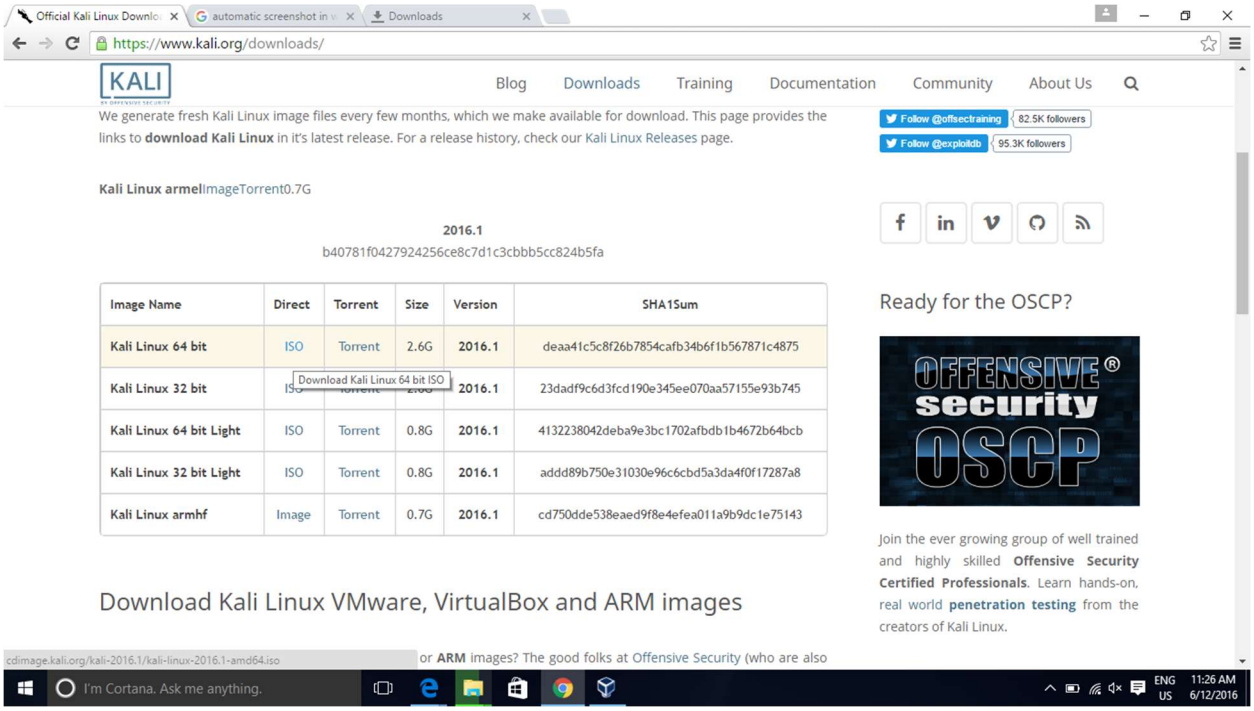
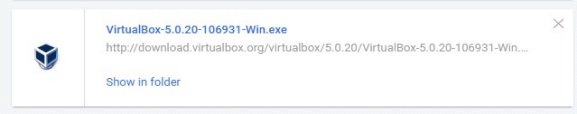
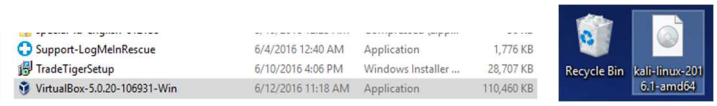
Practical No 1: Setting up our own Ethical Hacking Test LAB.

First download virtual box and also Download Kali Linux ISO File

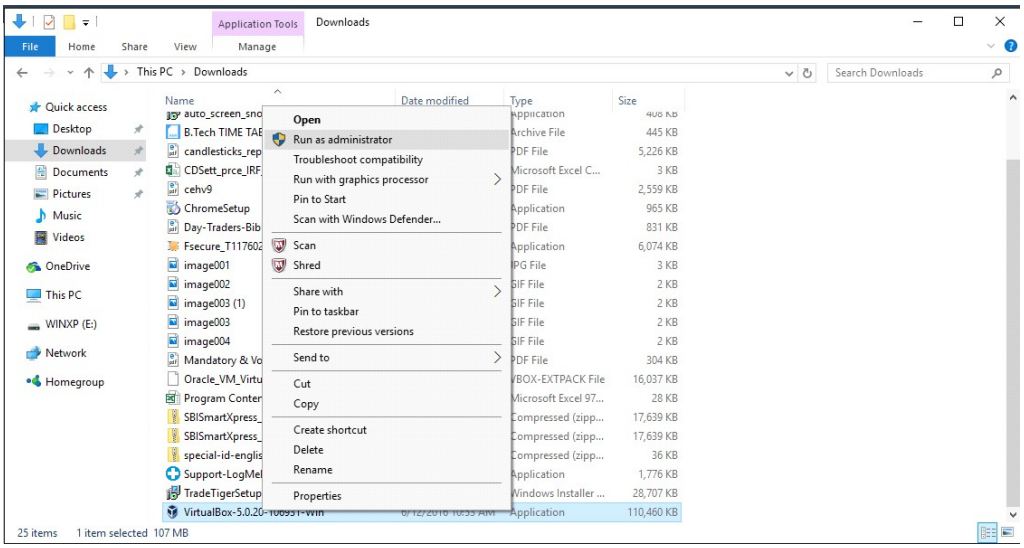




Have the two files ready before you begin

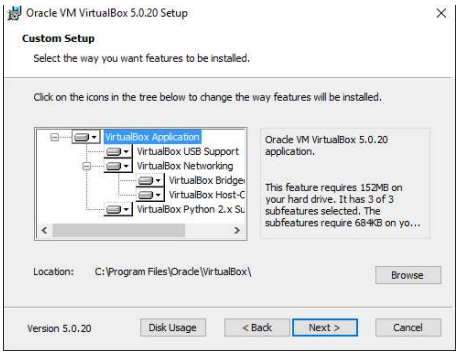


First install Virtual box by right clicking and selecting run as administrator

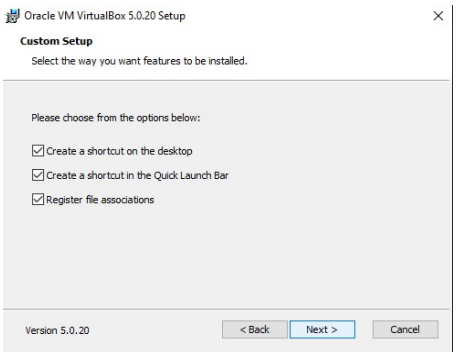


Click Next in the Below Image

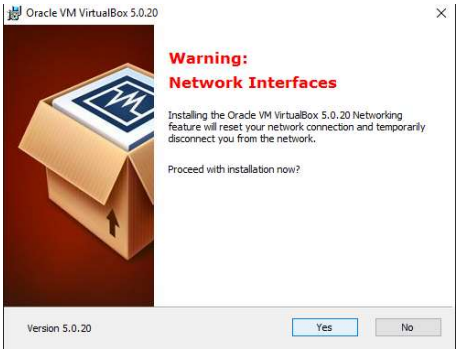
Click Next



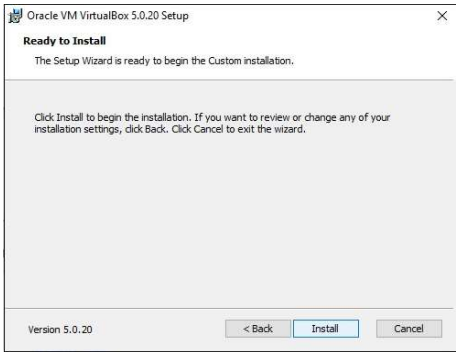
Click Next



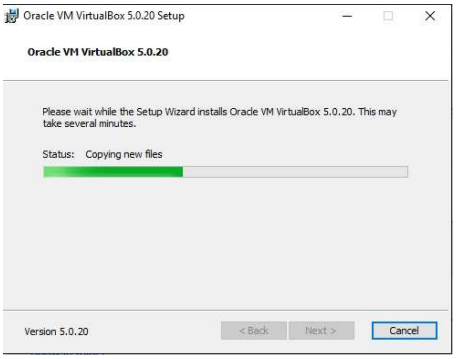
Click YES



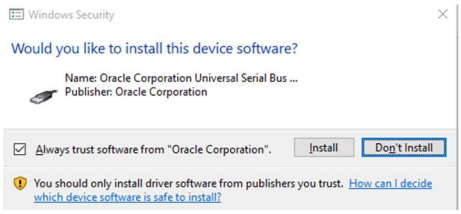
Click Install



Wait



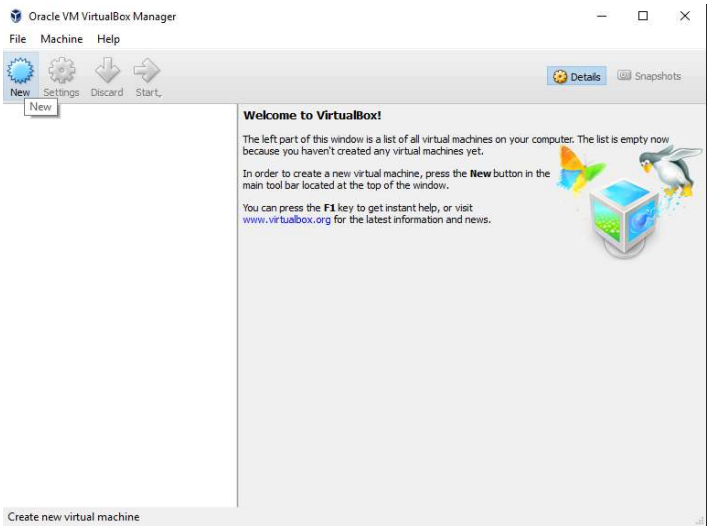
Click Install Here



Click Finish

After the Above step installation of virtual box will be completed we will proceed installing Kali in it as soon as it starts

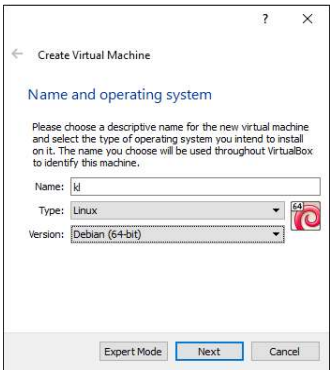
Click New Button Here



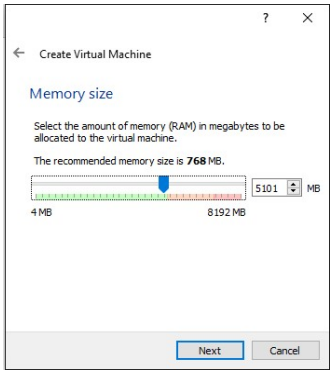
Give some name in the name box

Select Linux as Type

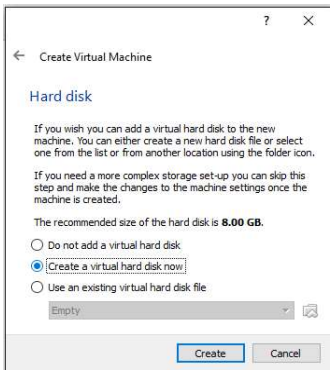
Select Debian 32 or 64 as Version Click Next



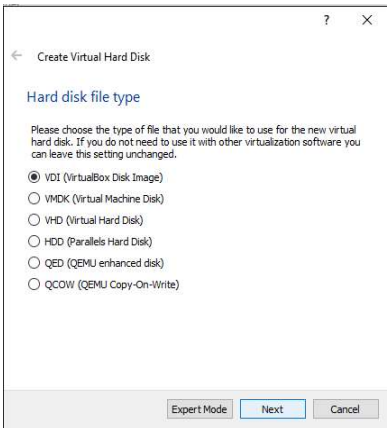
Give the amount of ram you want to allocate to your VM (it has to be in green limit) (minimum 3 GB recommended) and Click on Next



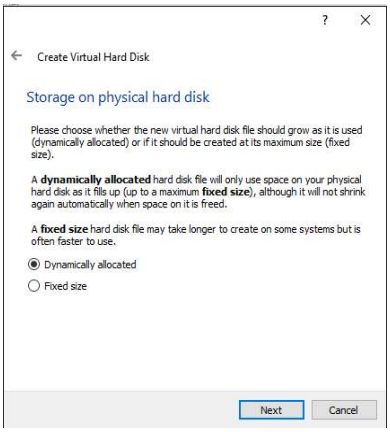
Select Create a virtual hard disk now option and click Create Button.



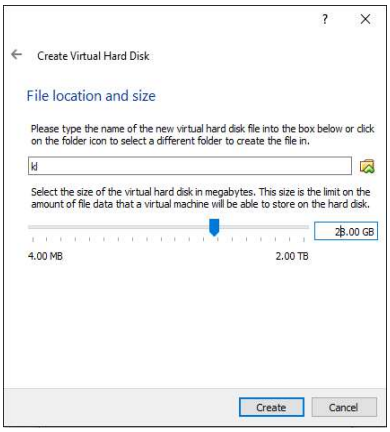
Select VDI as Hard disk Type and Click Next



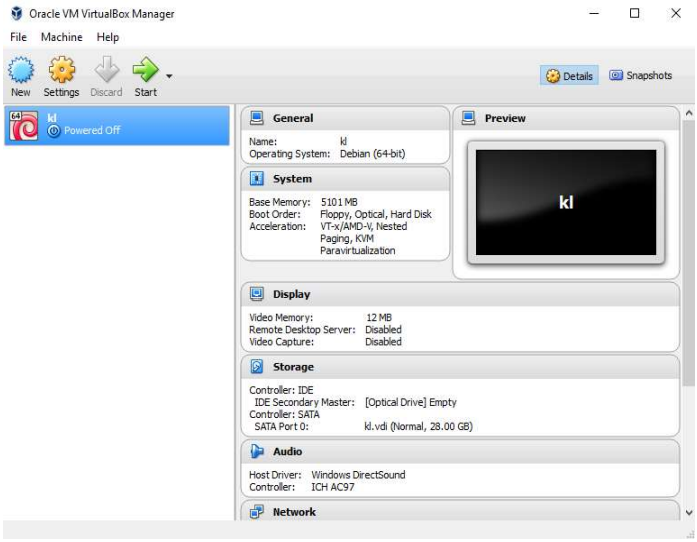
Select Dynamically Allocated As Storage and Click Next



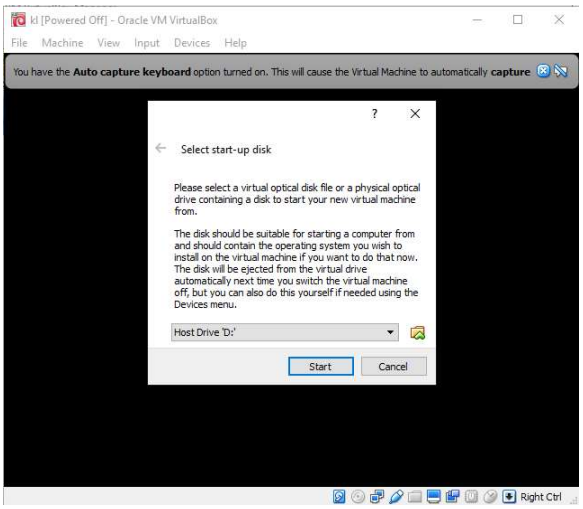
Change the file size to more than 20 GB for better performance and Click on Create Button.

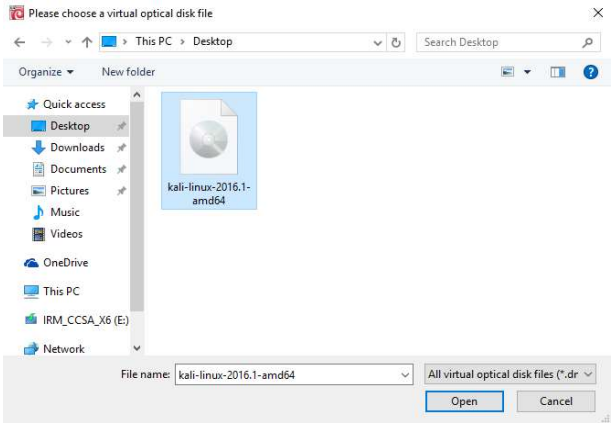


So Finally the OS will be created and listed like below diagram. Click on start button to start or double click the OS name to start.

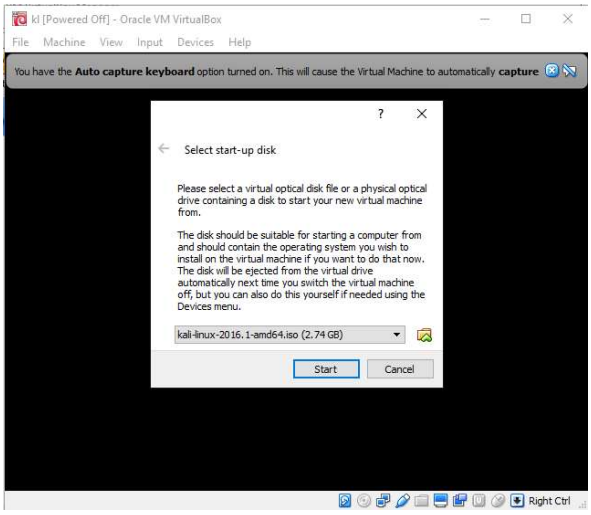


When it asks the Startup disk please select your downloaded kali Linux ISO file

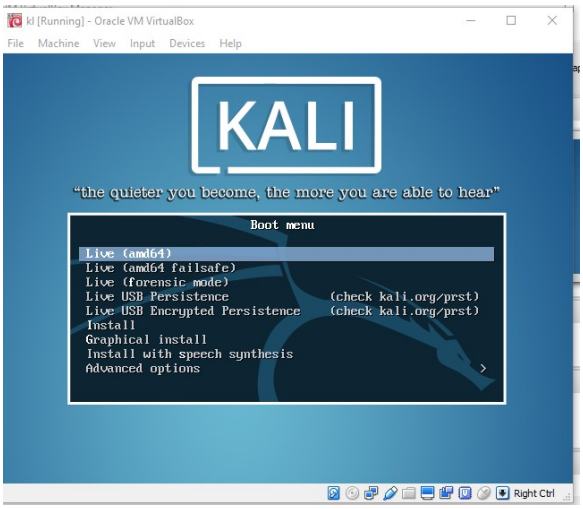




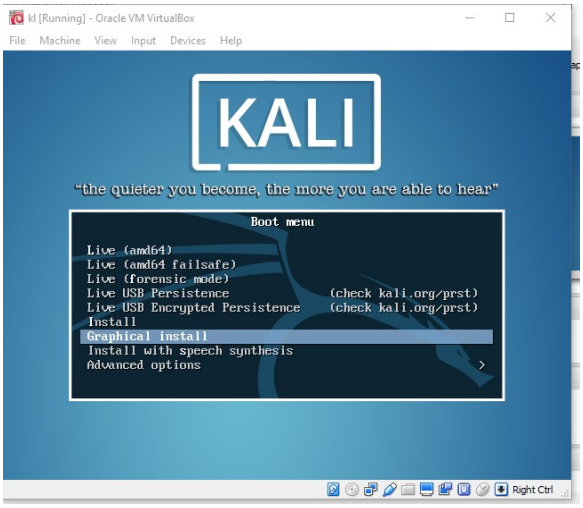
And Click On Start Button.



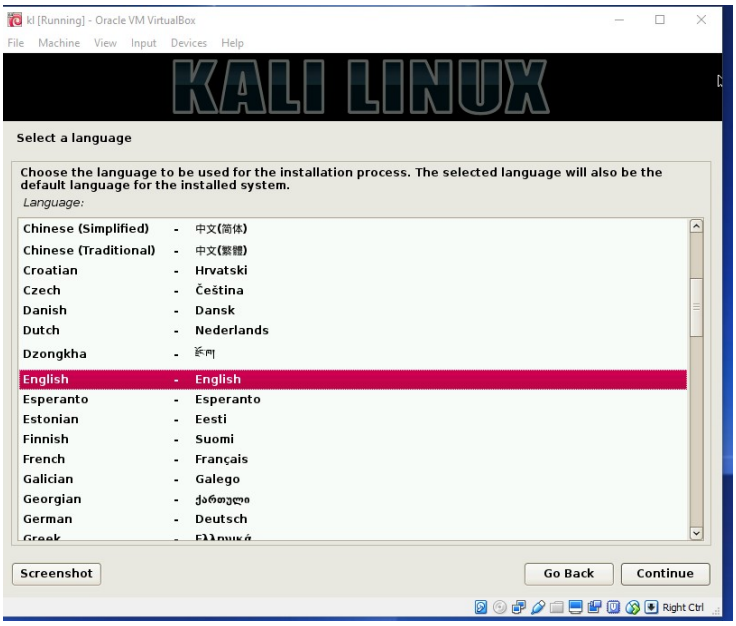
After few moments it will load like this



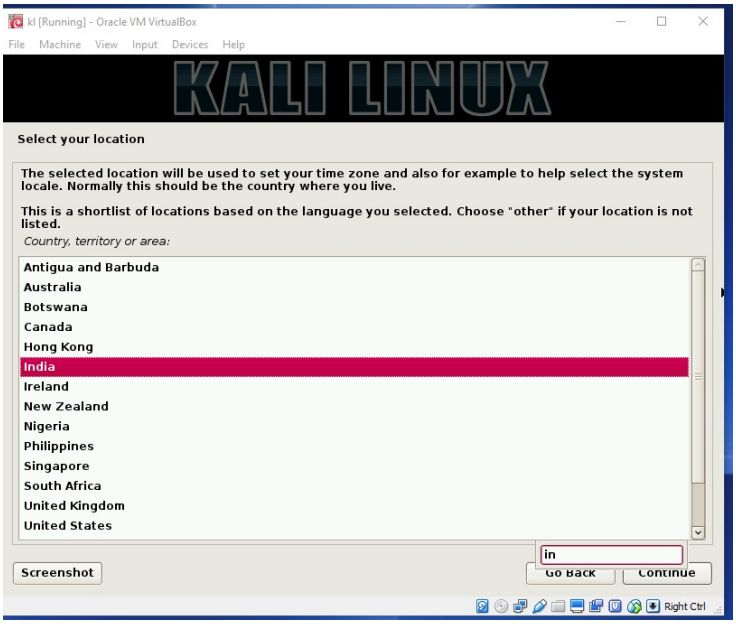
Select Graphical install with your keyboard down arrow keys and Press Enter.



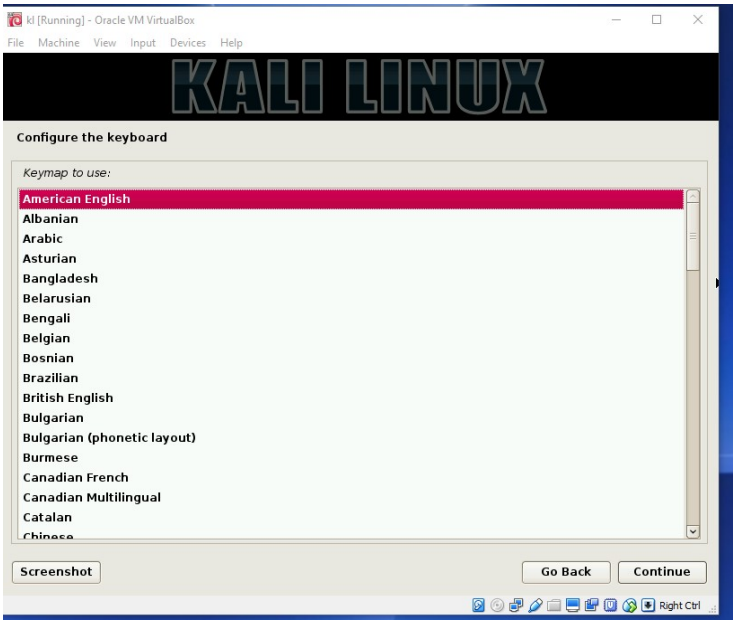
When it asks the Language select the Language you want (English Would be Good) and click on continue



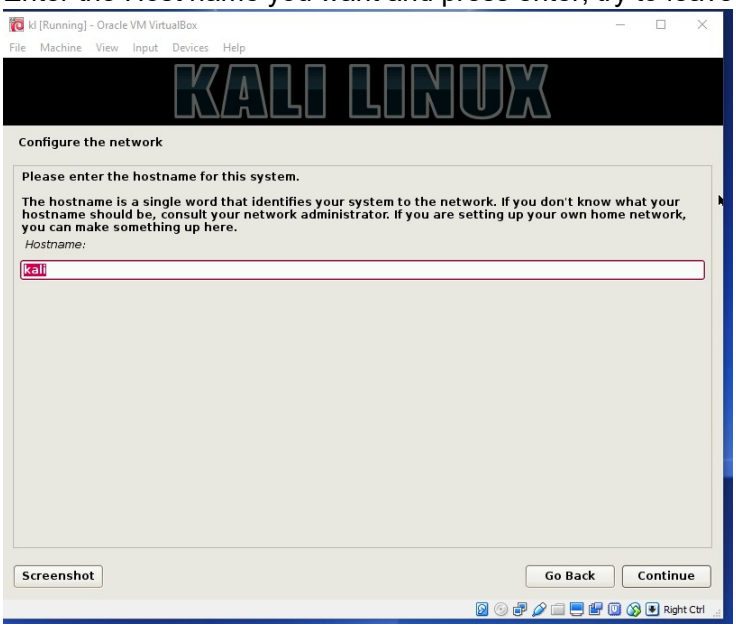
In the country section select your country (India here) and click continue



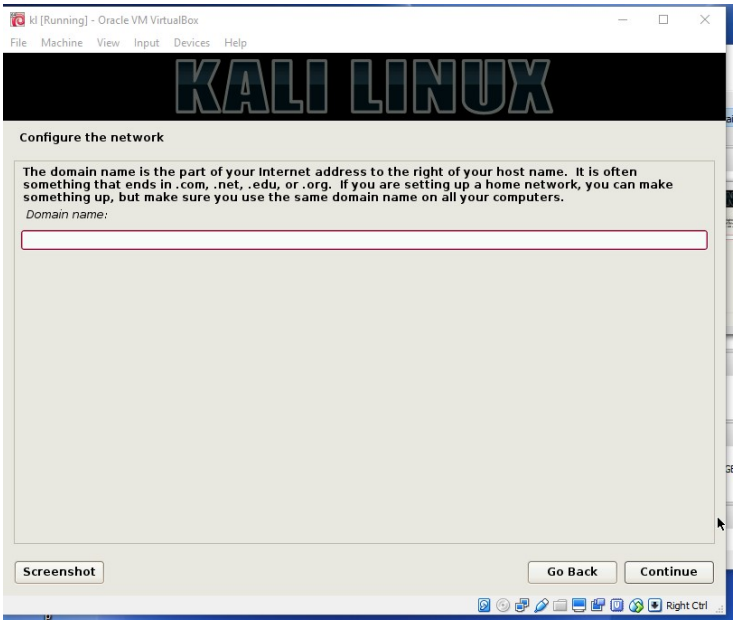
Select American English if you are using QWERTY keyboard select others if you use any other and Click continue



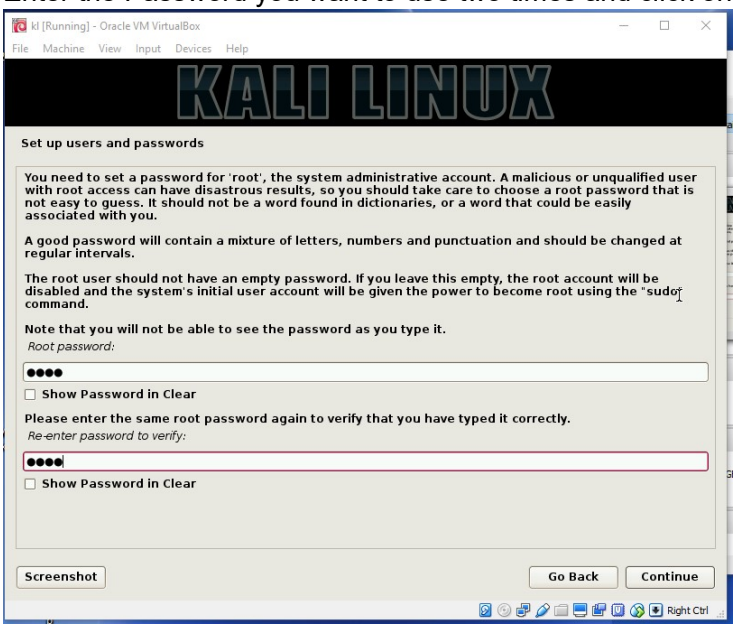
Enter the Host name you want and press enter, try to leave as it is if you don’t know.



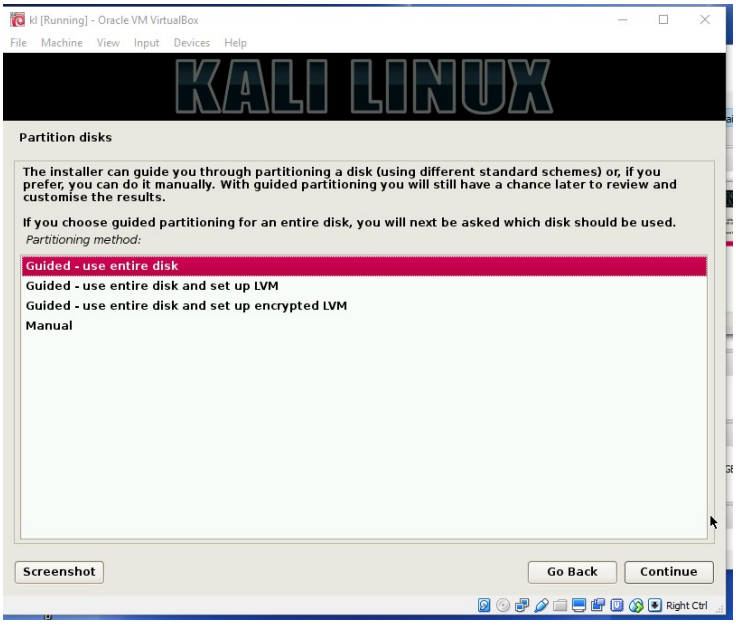
Leave the Domain name blank and Click on Continue



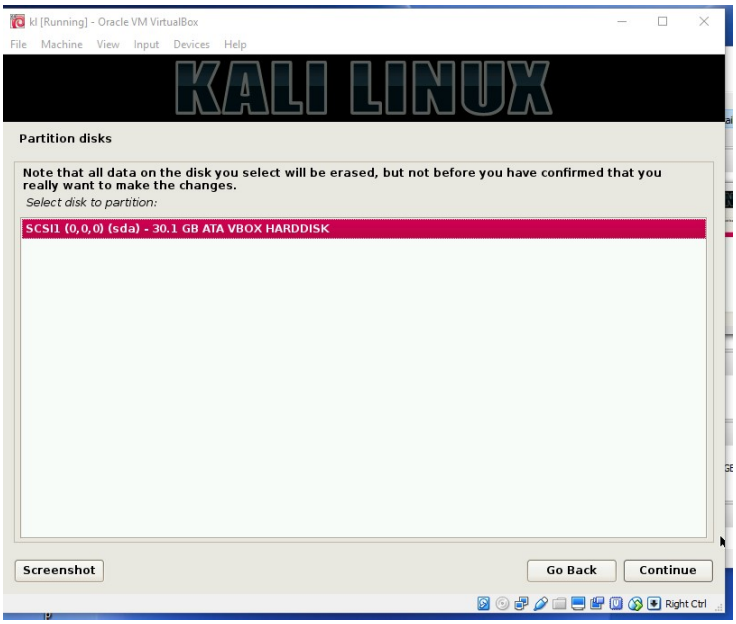
Enter the Password you want to use two times and click on continue (you can change later)



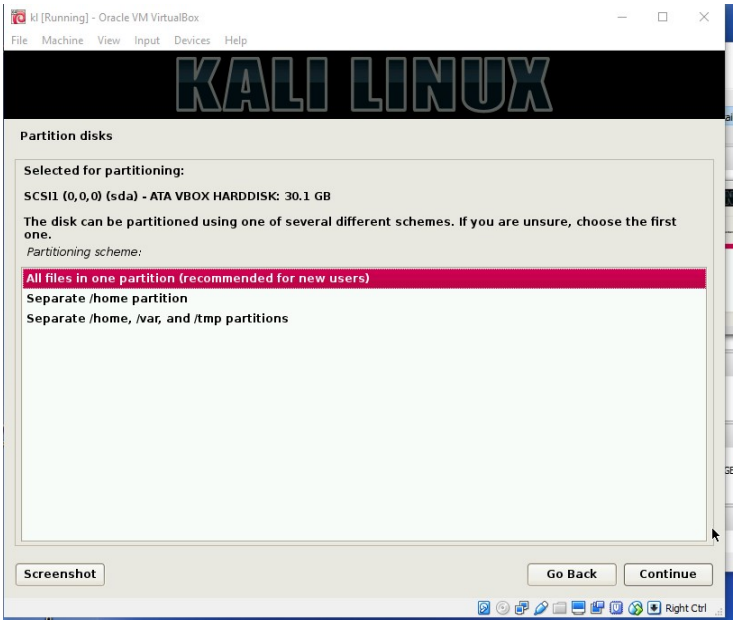
Select Guided-use Entire disk and Click on Continue



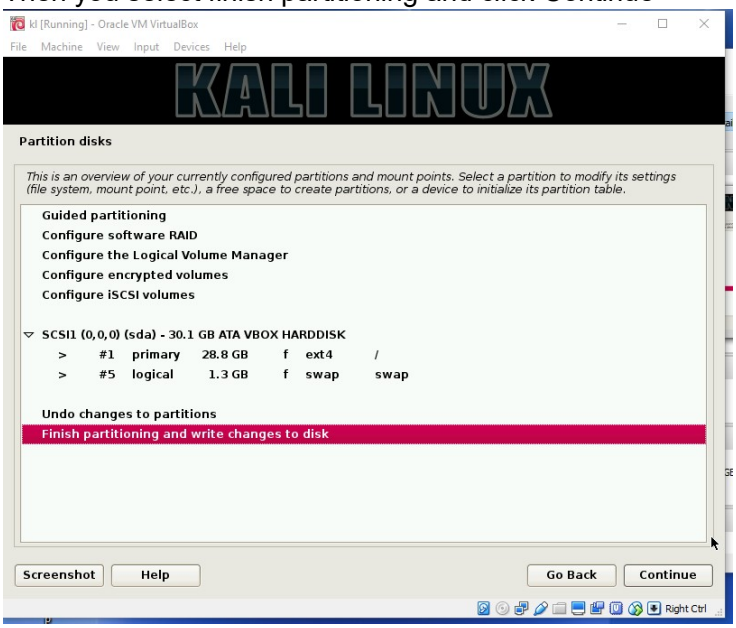
Select the Hard disk available there and Click On Continue.



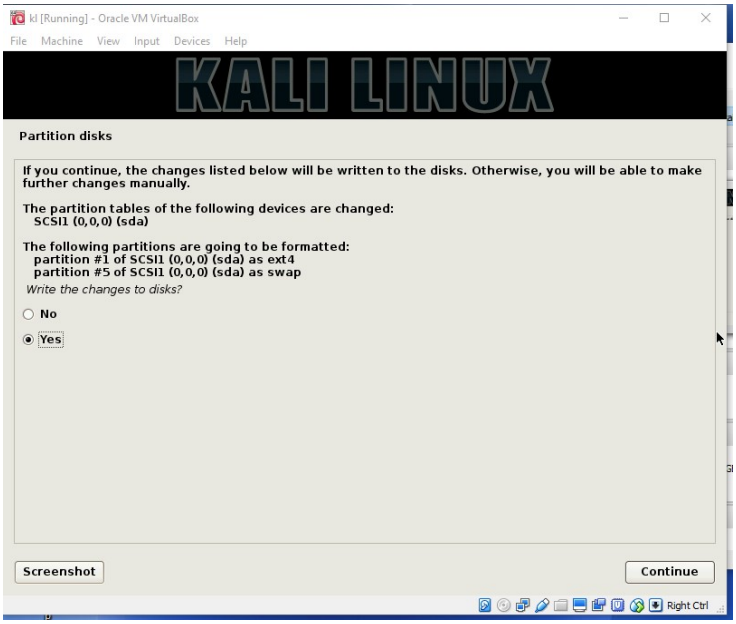
Select the First Option All Files in one partition and Click on continue.



Then you select finish partitioning and click Continue

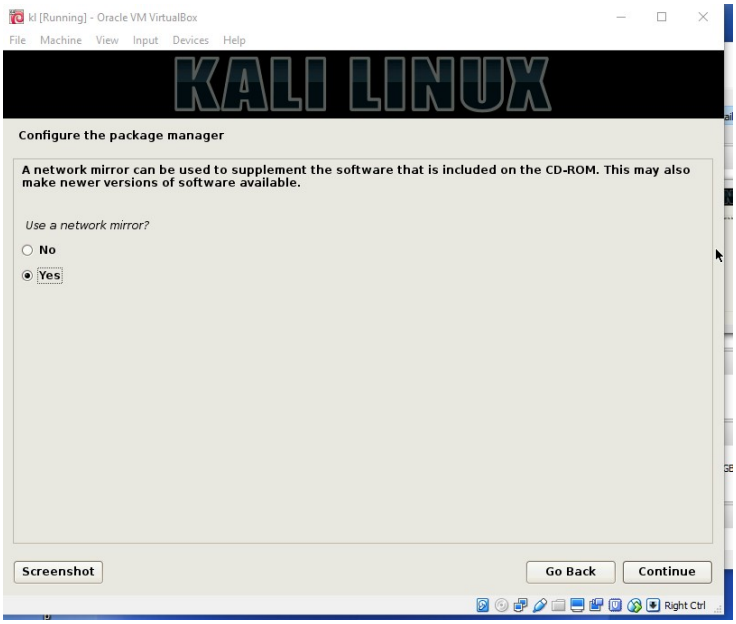


Select yes when prompting and continue.

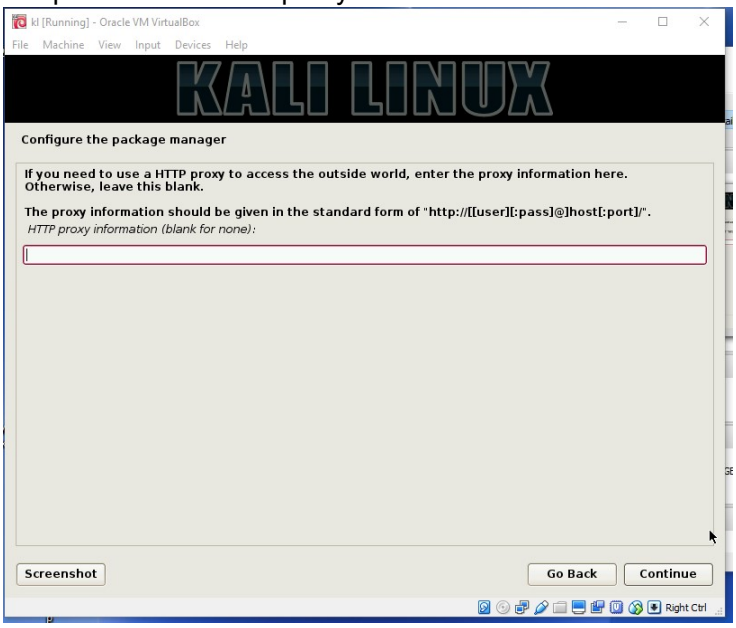


Wait till the process of copy completes.

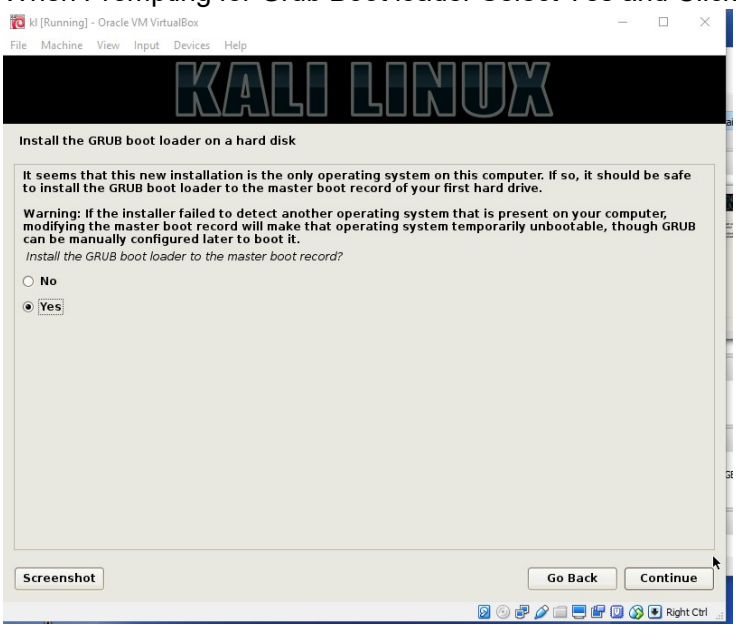
When prompting for Network mirror make sure you have working internet connection and Select YES and Continue



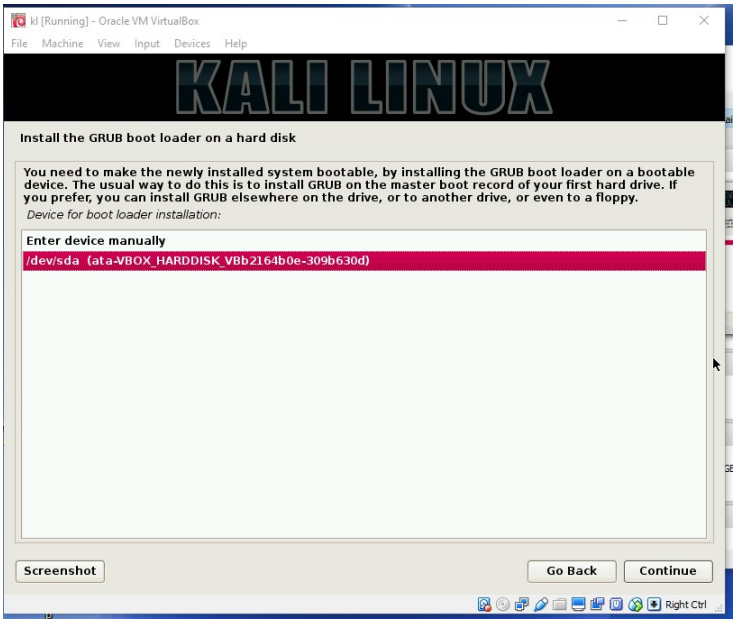
Keep Blank the HTTP proxy and Click Continue



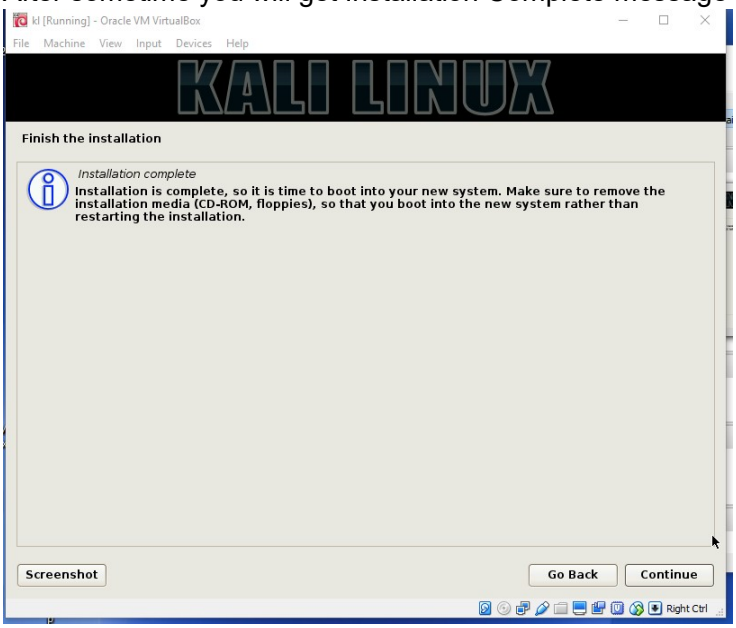
When Prompting for Grub Boot loader Select Yes and Click Continue



Select the Device from the list and Click Continue



After sometime you will get Installation Complete message click continue to start your OS.



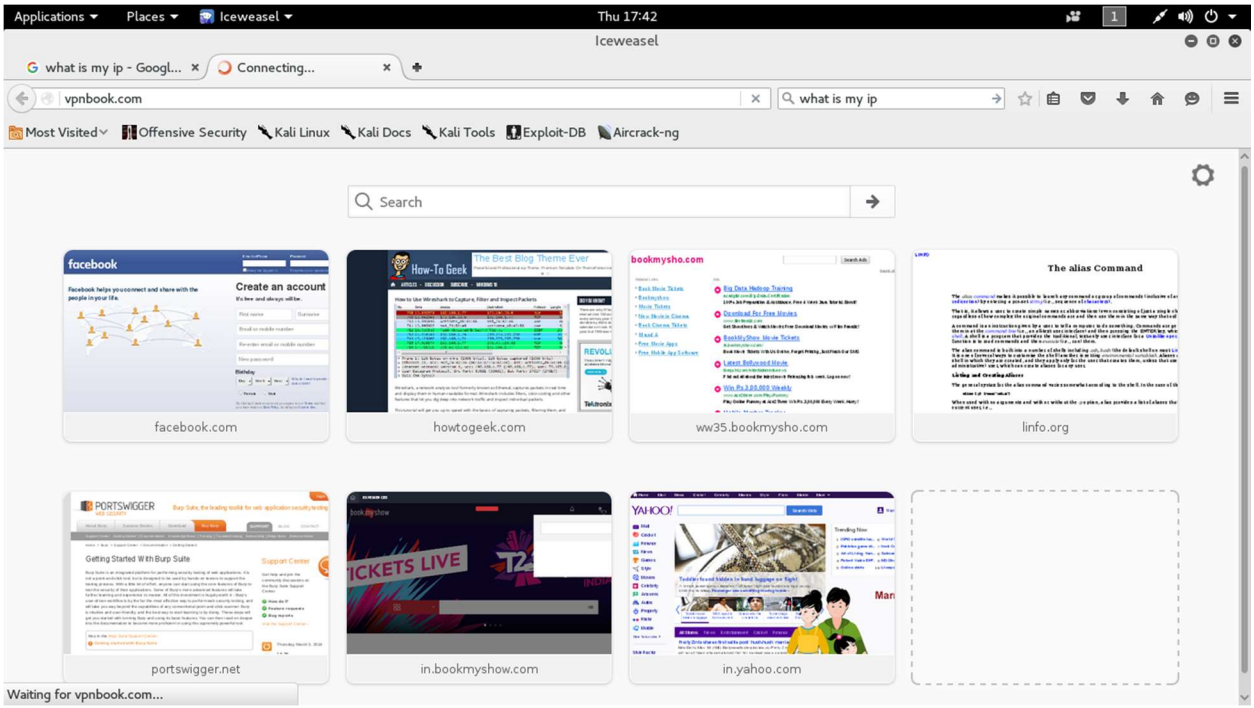
Practical No 2: IP address spoofing in kali Linux.

Requirements:

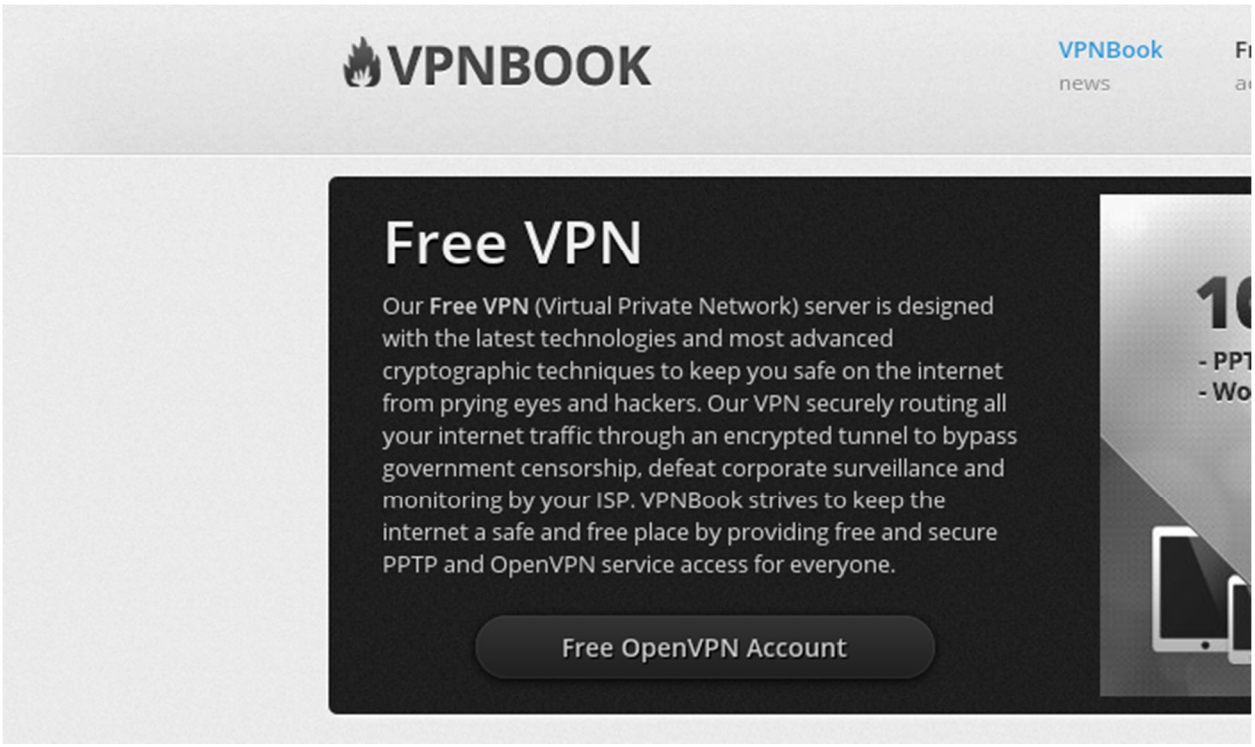
Good internet connection

Kali Linux installed (either host or guest)

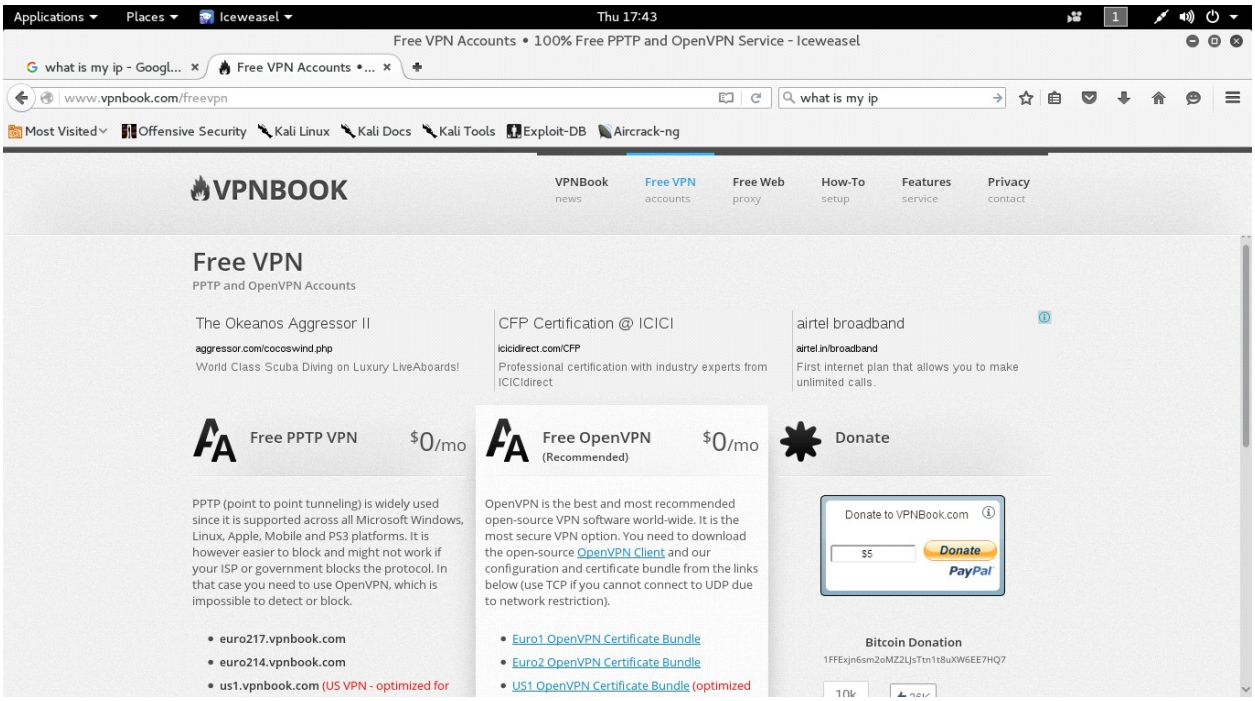
Step 1: Go to vpnbook.com and click on free VPN account.

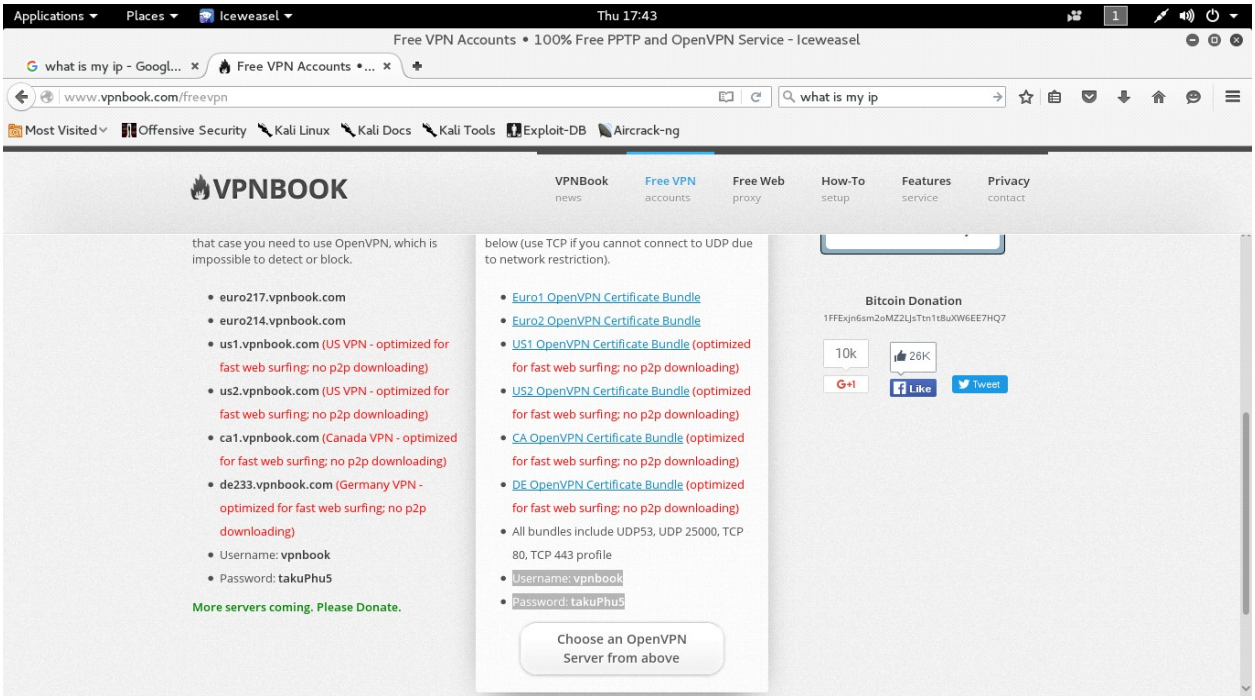

Applications
Places
Iceweasel
Thu 17:42
Iceweasel
what is my ip - Googl...
Connecting...
vpnbook.com
what is my ip
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Search
facebook.com
howtogeek.com
ww35.bookmysho.com
linfo.org
portswigger.net
in.bookmyshow.com
in.yahoo.com
Waiting for vpnbook.com...


Applications
Places
Iceweasel
Thu 17:42
Free VPN • 100% Free PPTP and OpenVPN Service - Iceweasel
what is my ip - Googl...
Free VPN • 100% Fr...
www.vpnbook.com
what is my ip
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
VPNBOOK
VPNBook
news
Free VPN
accounts
Free Web
proxy
How-To
setup
Features
service
Privacy
contact
Free VPN
Our Free VPN (Virtual Private Network) server is designed with the latest technologies and most advanced cryptographic techniques to keep you safe on the internet from prying eyes and hackers. Our VPN securely routing all your internet traffic through an encrypted tunnel to bypass government censorship, defeat corporate surveillance and monitoring by your ISP. VPNBook strives to keep the internet a safe and free place by providing free and secure PPTP and OpenVPN service access for everyone.
Free OpenVPN Account
100% Free VPN Service
- PPTP and OpenVPN Protocols Supported
- Works on All Mobile Devices and Operating Systems.
bankbazaar.com
LOOKING FOR A
MORE REWARDING
CREDIT CARD?
PPTP and OpenVPN
Unblock Websites
Surf the Web anonymously
100% Free
Why Pay For VPN Service Again?
Waiting for googleads.g.doubleclick.net...

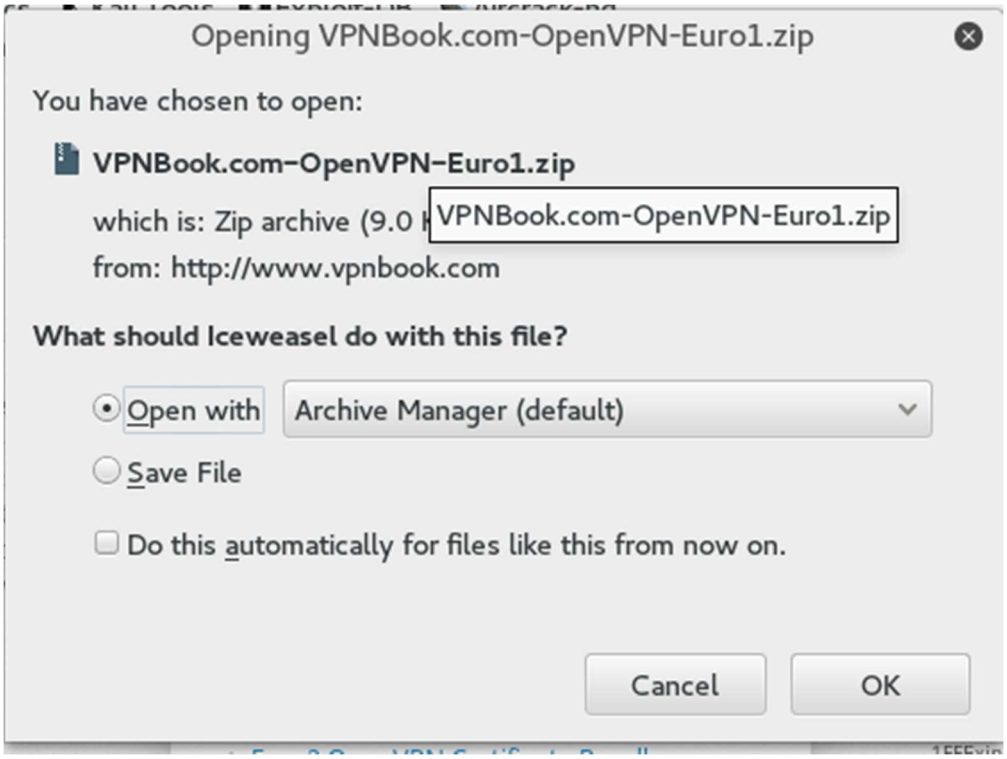


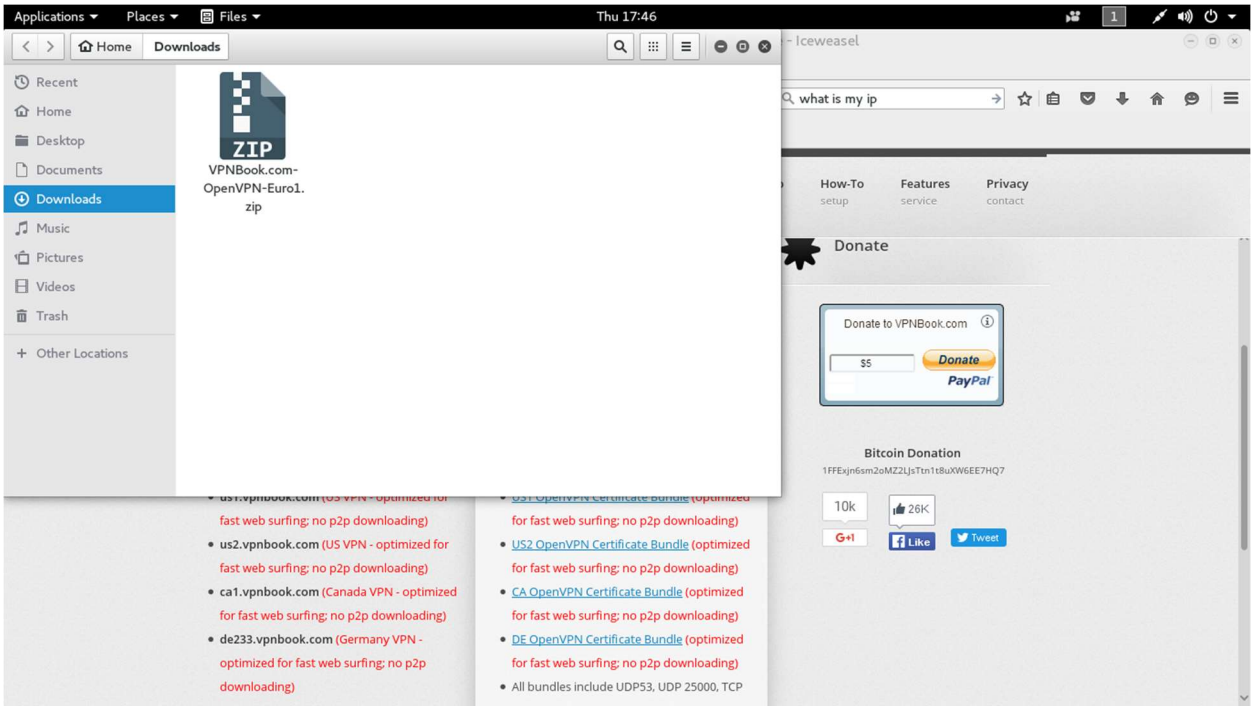
On the next screen under free openvpn account credentials will be there just note down them in a separate place.





Step 2: download any one of the file (the file will be downloaded to /root/Downloads by default)





Step 3: go to the download location with the command

cd /root/Downloads

```
root@kali:~# cd /root/Downloads
root@kali:~/Downloads#
```

```
root@kali:~# cd /root/Downloads
root@kali:~/Downloads# ls
VPNBook.com-OpenVPN-Euro1.zip
root@kali:~/Downloads#
```

Step 4: extract the file contents with the following command

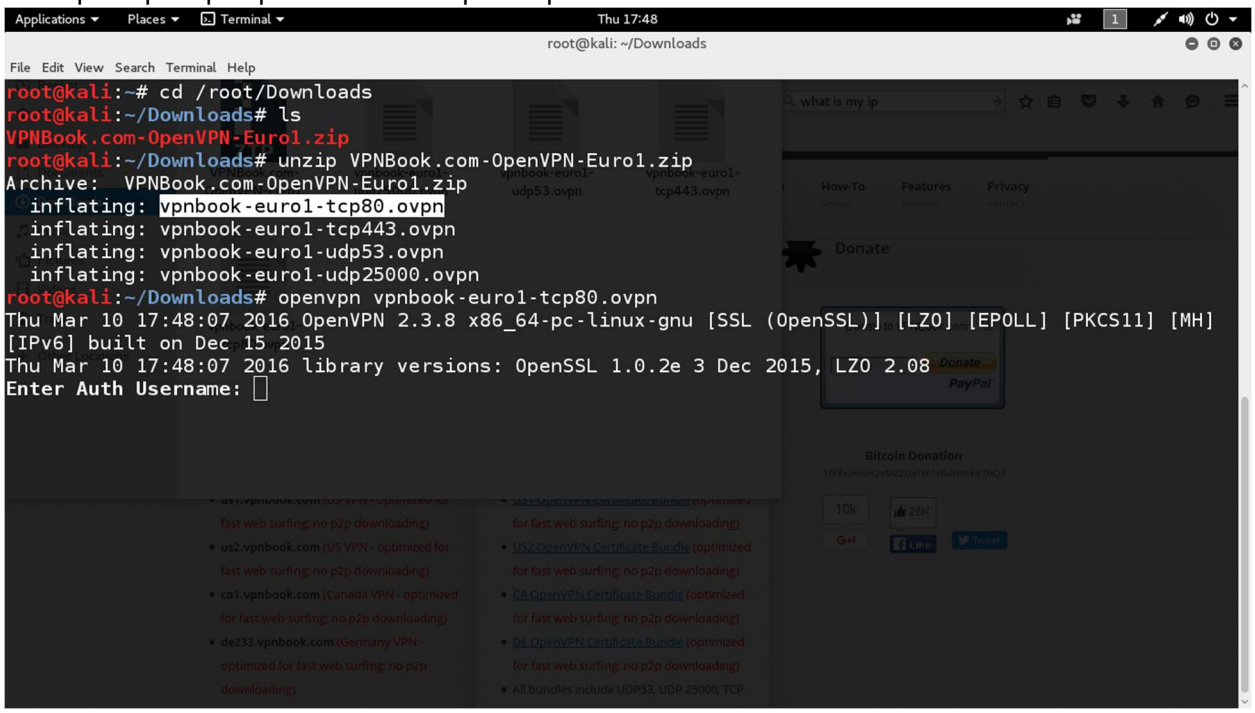
Syntax: unzip filename

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

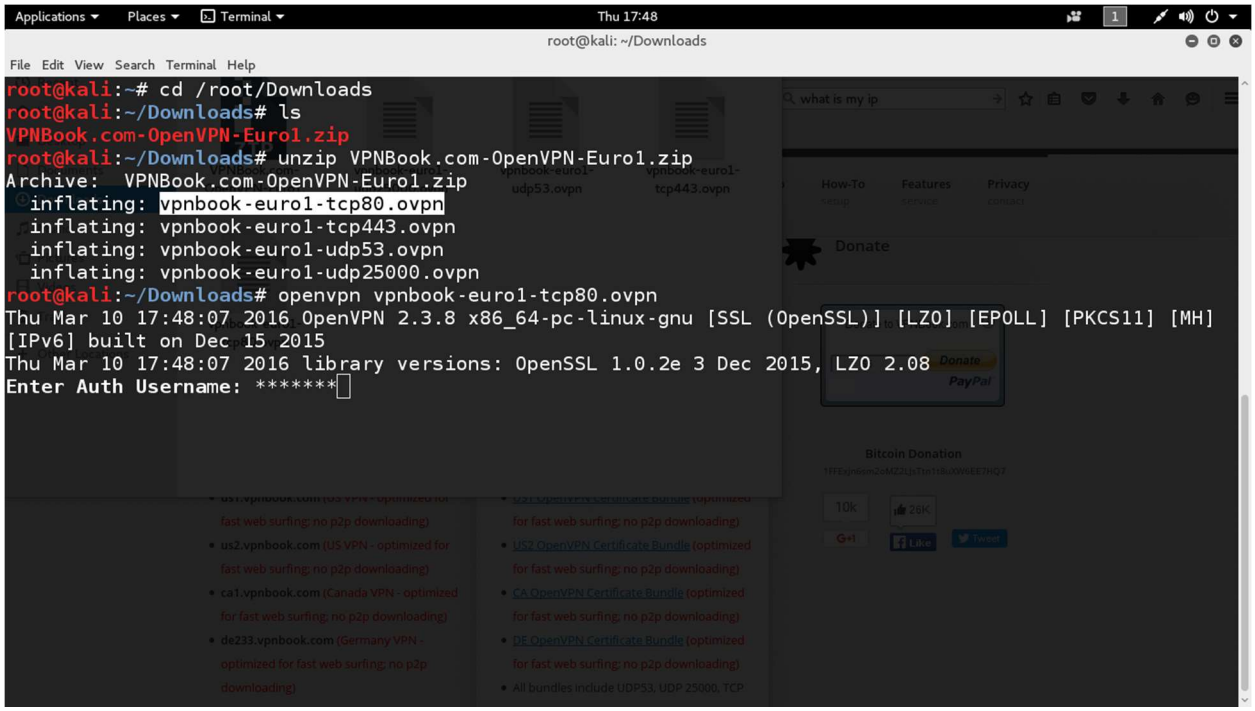
Step 5: after extraction execute the following command to change your IP

Syntax: openvpn <extracted file name>

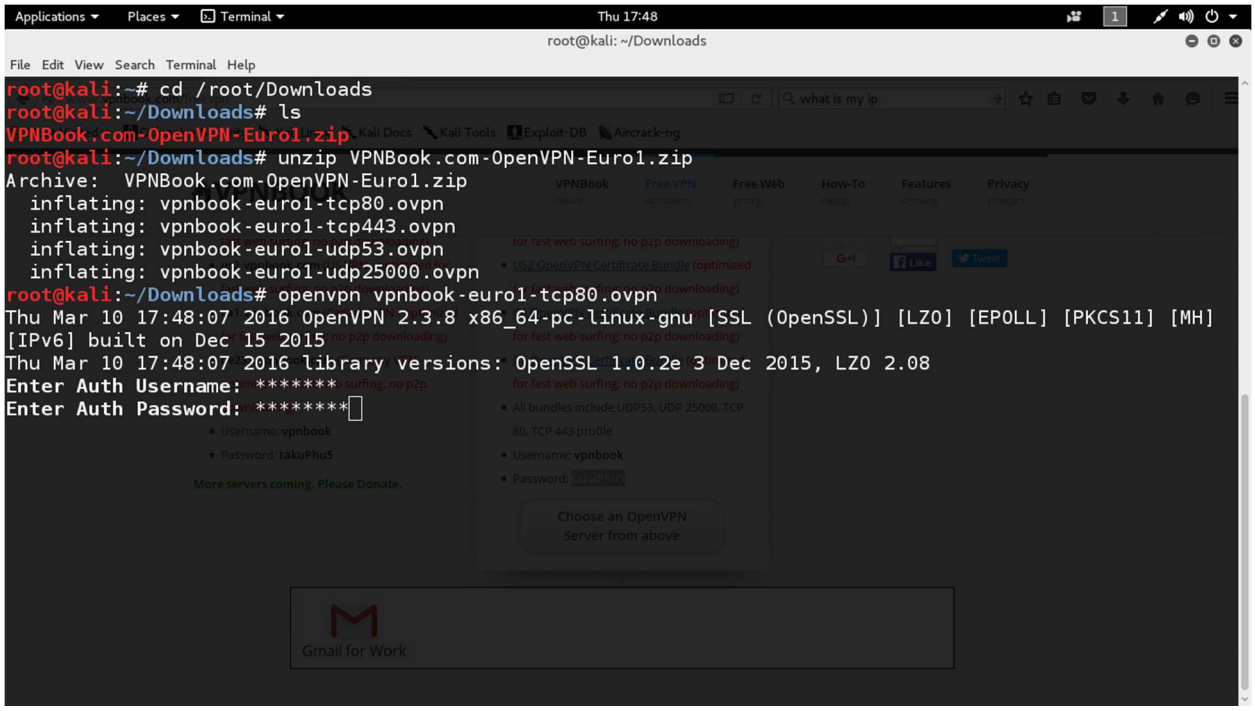
Example: openvpn vpnbook-euro1-tcp80.ovpn



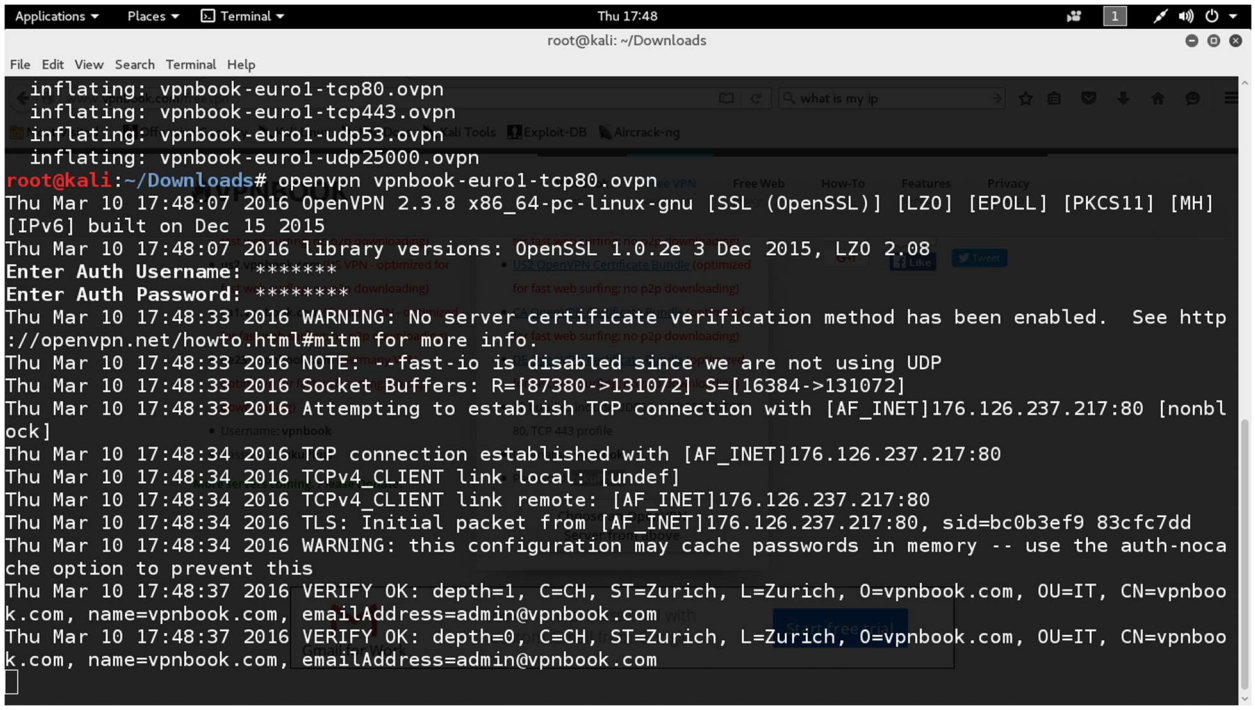
It will ask you enter your name just enter the username you seen from the vpnbook website



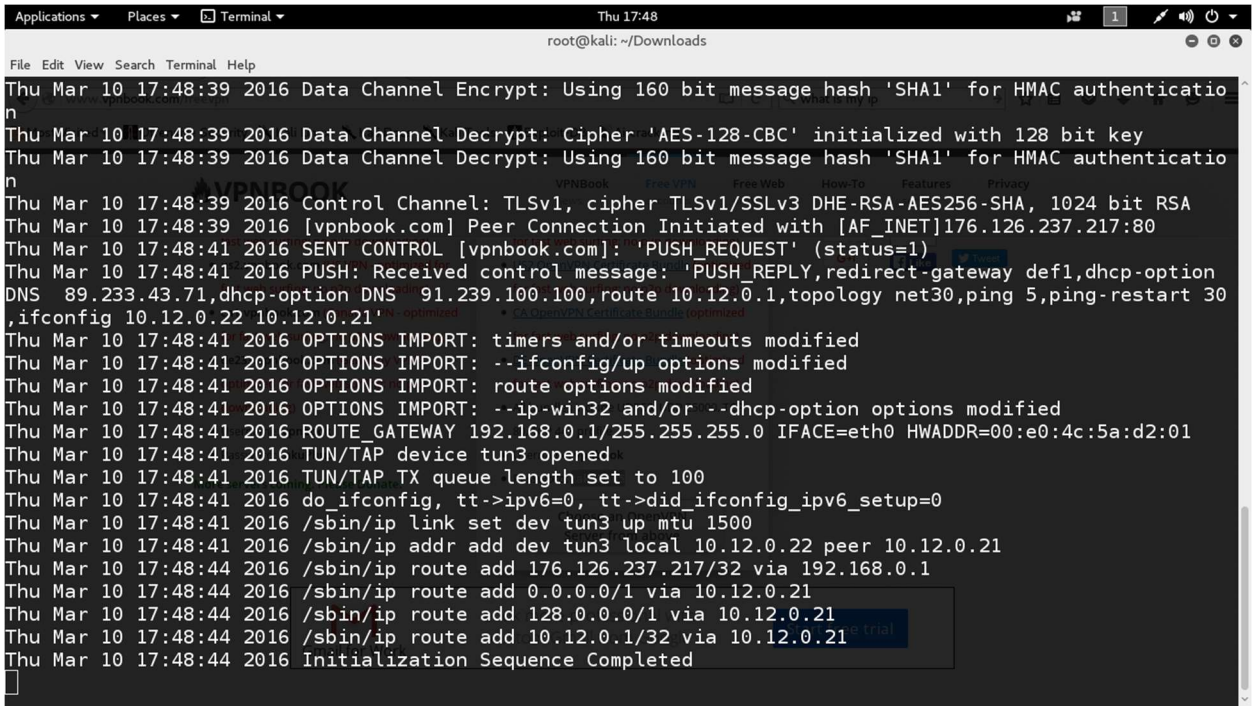
After entering username hit enter so it will ask you to input password enter the password also



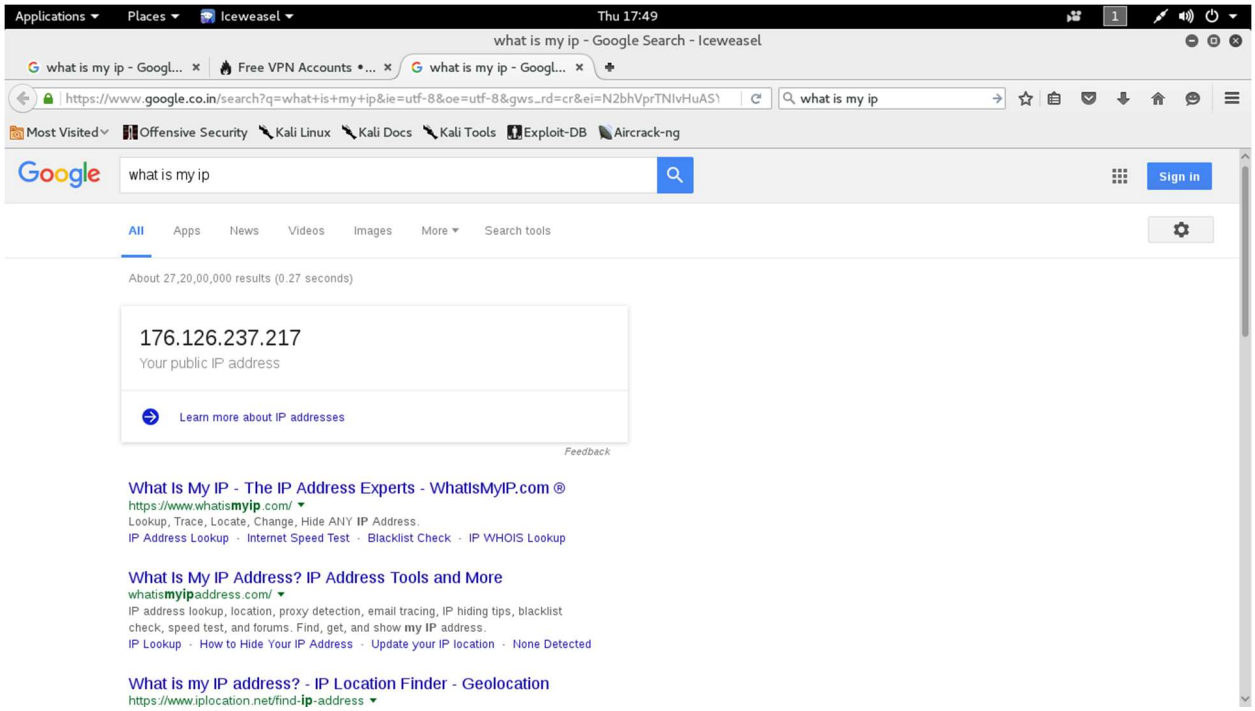
After that hit enter it will do some processing.



After you see “Initialization Sequence Completed” Message you can check your ip by typing “ifconfig” in your terminal you can observe a new ip, and also you can google for “what is my ip” you can see the new spoofed ip.

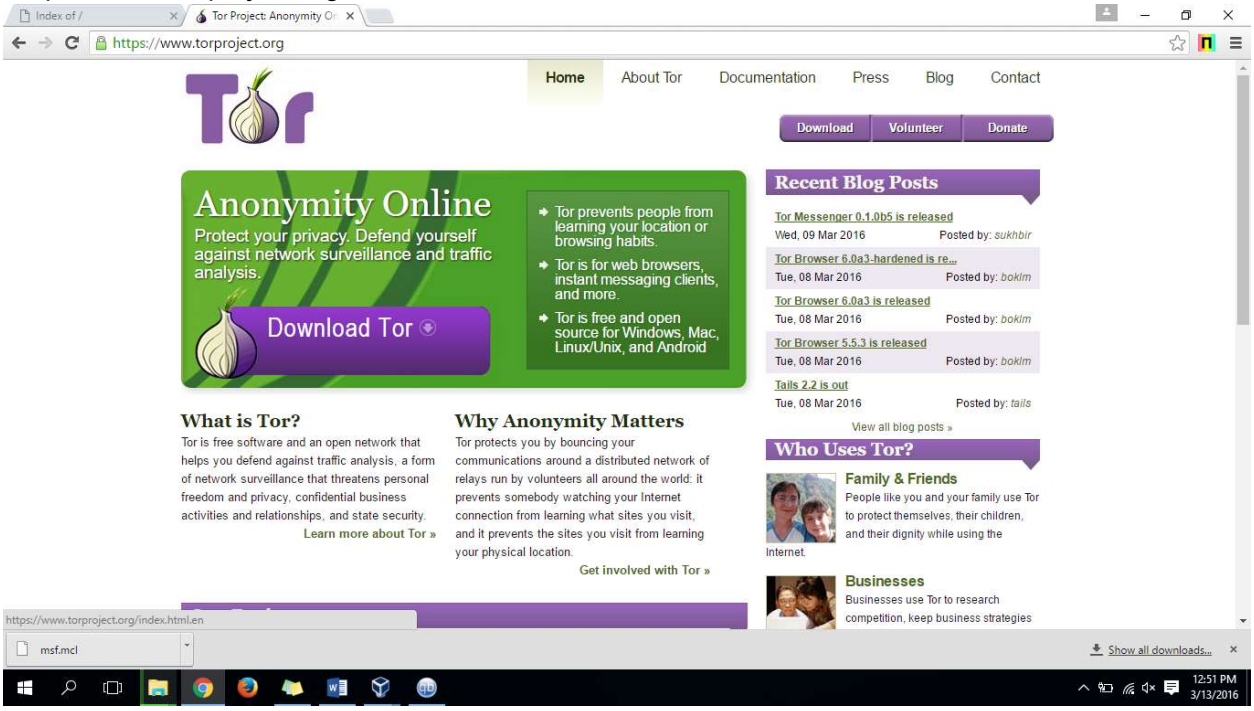



```
tun3: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
      inet 10.12.0.22  netmask 255.255.255.255  destination 10.12.0.21
      unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
      RX packets 183  bytes 93589 (91.3 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 215  bytes 19611 (19.1 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

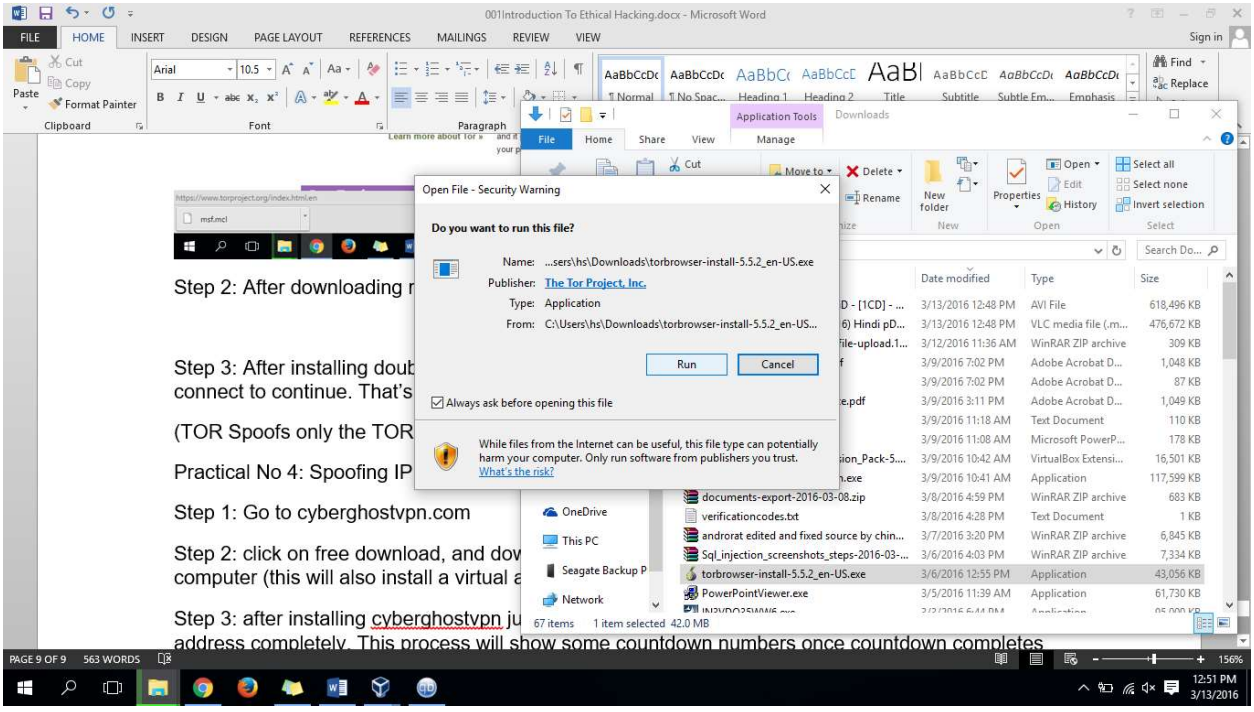


Practical No 3: Spoofing IP address any operating system.

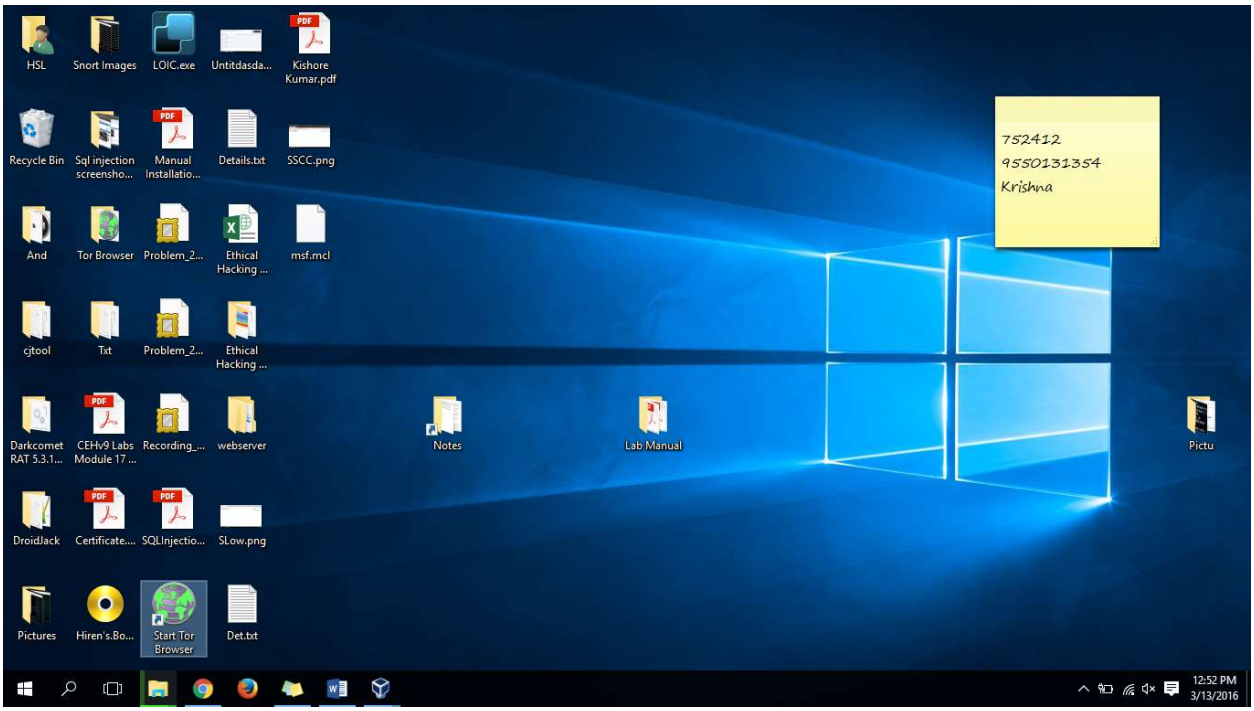
Step 1: Go to torproject.org and download the TOR browser



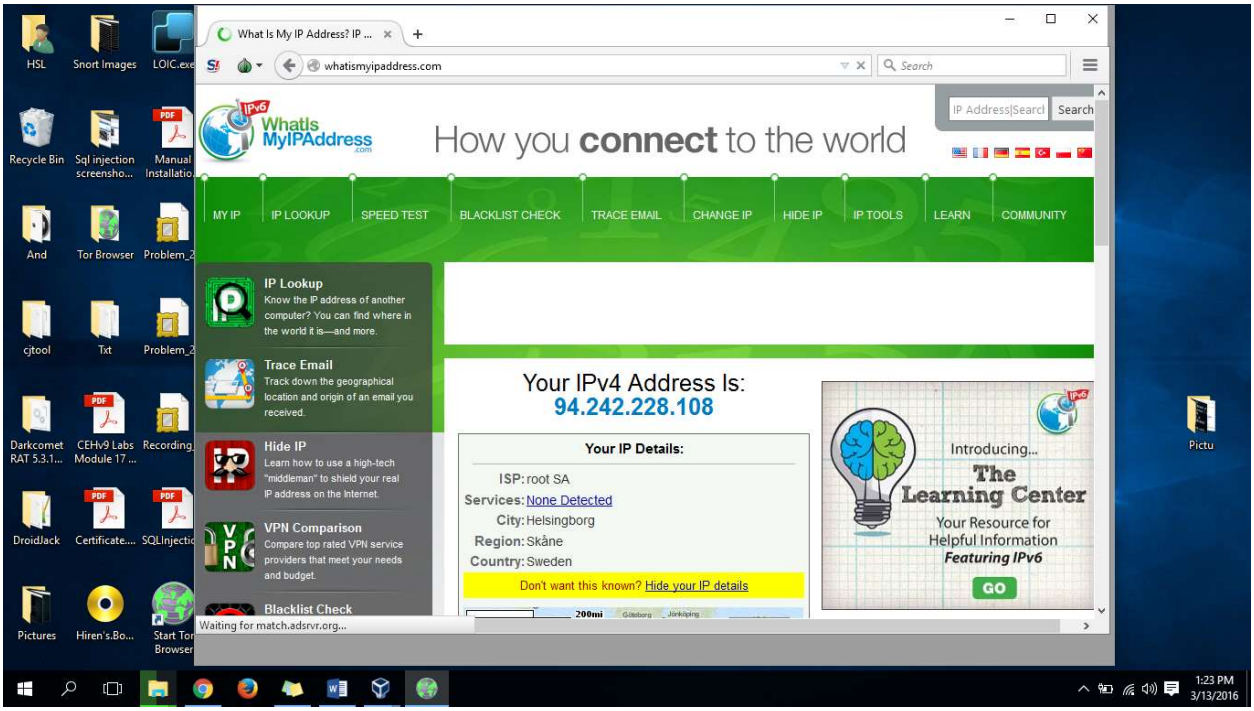
Step 2: After downloading run the Tor bundle to extract the browser package.



Step 3: After installing double click on the Start TOR link to start TOR browser,



If asking click on connect to continue. That's it you are spoofed your browser automatically.



(TOR Spoofs only the TOR browser, anything you do outside of TOR browser cannot be spoofed.)

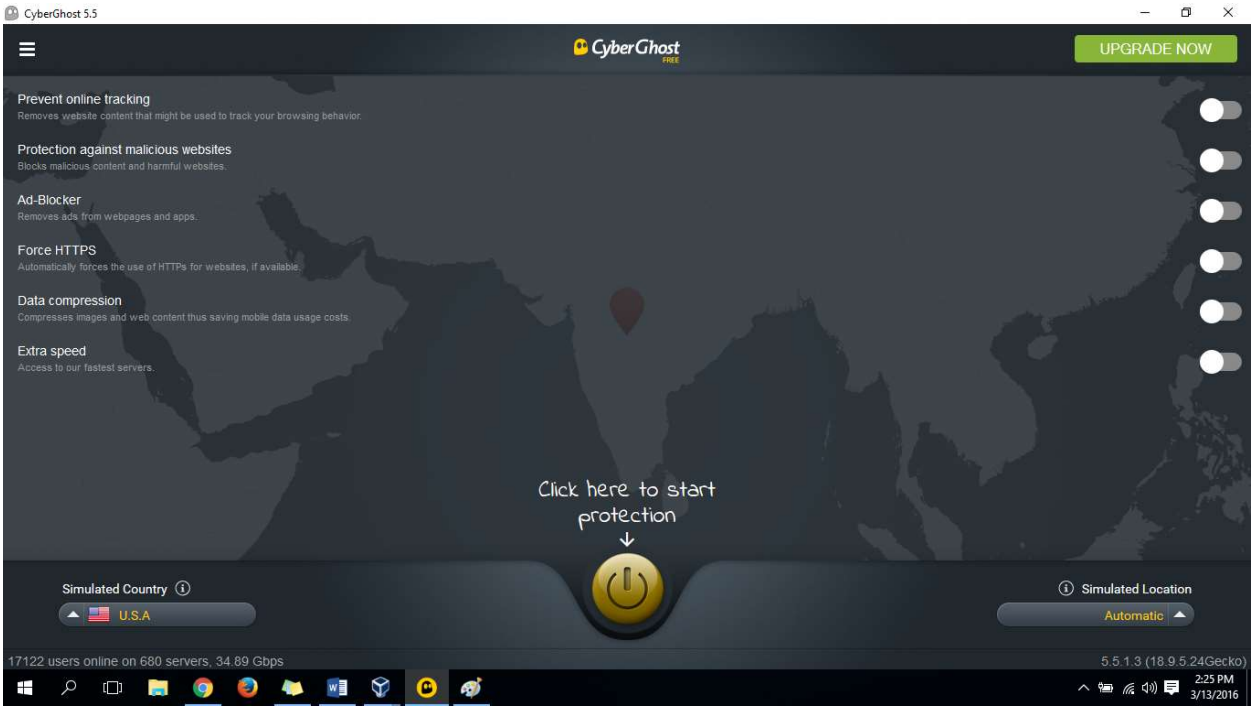
Practical No 4: Spoofing IP address in any machine completely

Step 1: Go to cyberghostvpn.com

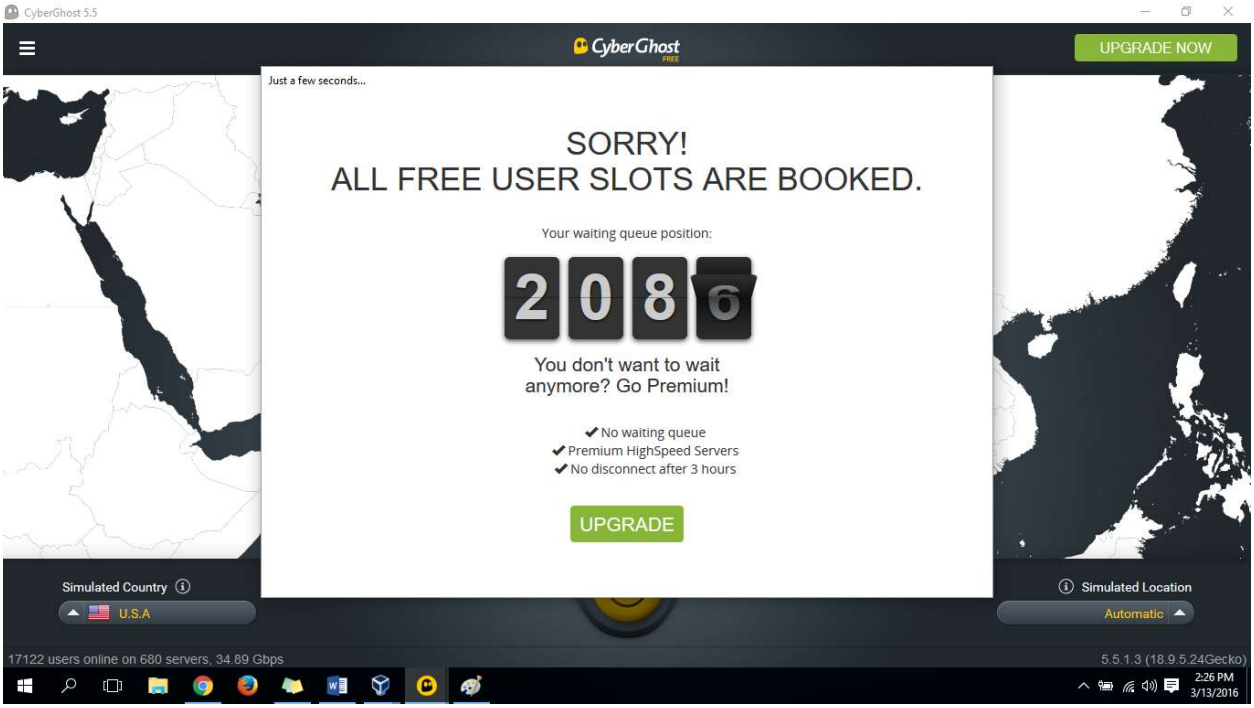
Step 2: click on free download, and download the cyberghostvpn setup and install it on your computer (this will also install a virtual adapter if it asking a prompt to install select “YES”)

Step 3: after installing cyberghostvpn

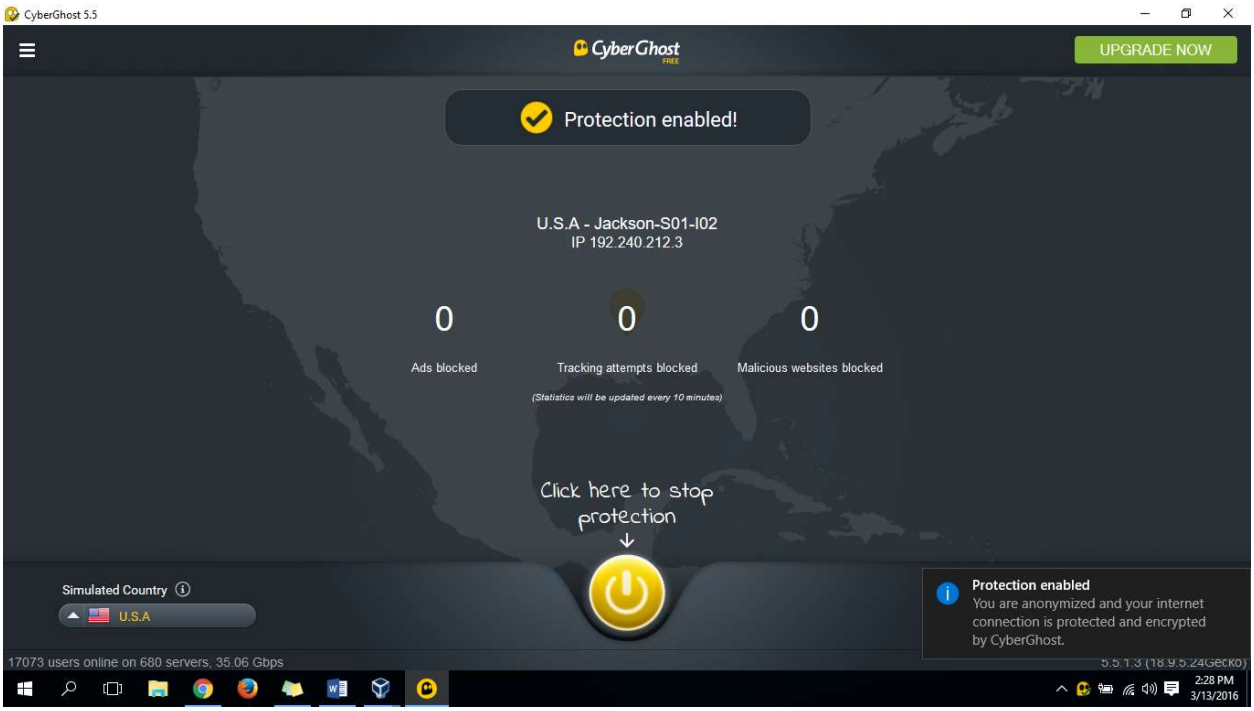
Just click on the power button on the interface to spoof your IP address completely.



This process will show some countdown numbers



Once countdown completes your IP will be spoofed, you have to wait till then.

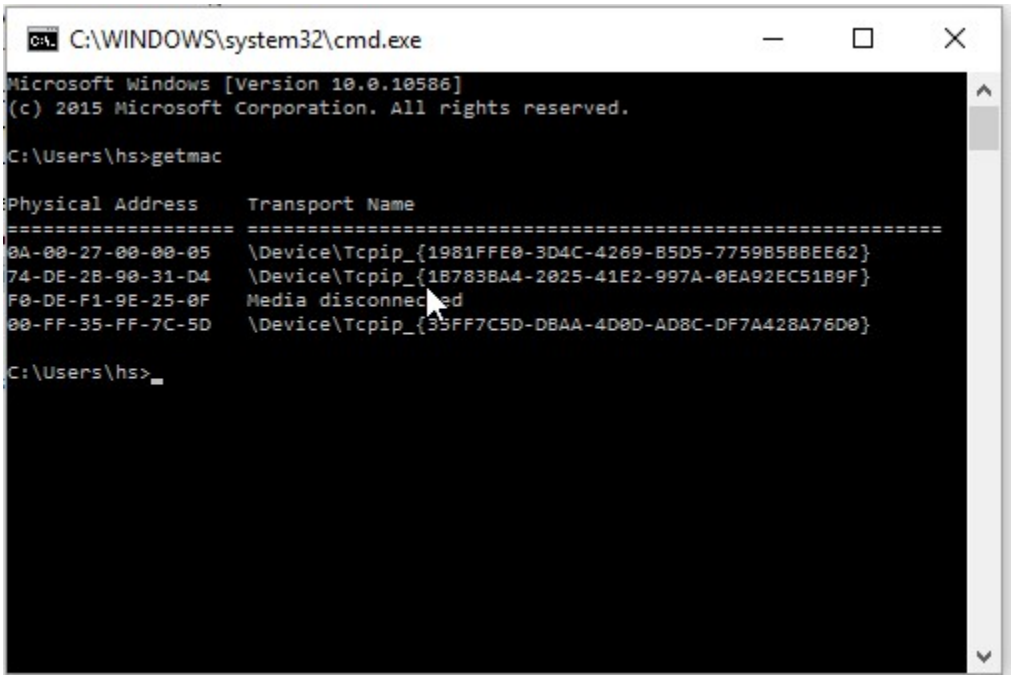


If you want you can select some other countries also and some other IPs also from the left and right menus.

If you want to disconnect from the spoofed ip just click on the same button again.

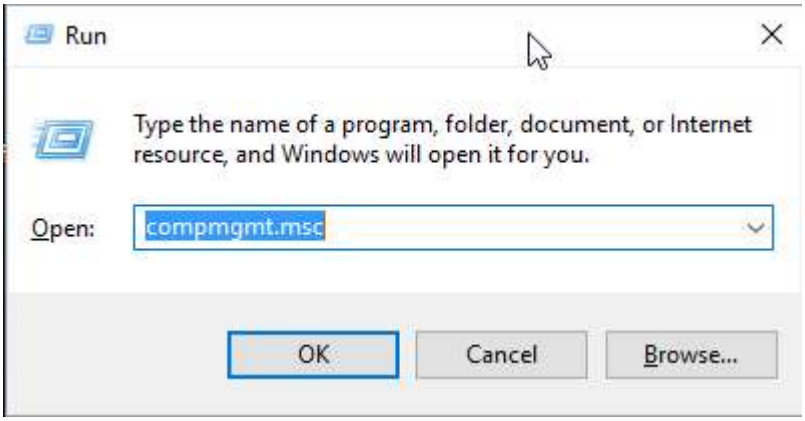
Practical No 5: MAC Address Spoofing in Windows Machines:

First of all check out your real mac address in the command prompt by executing getmac command

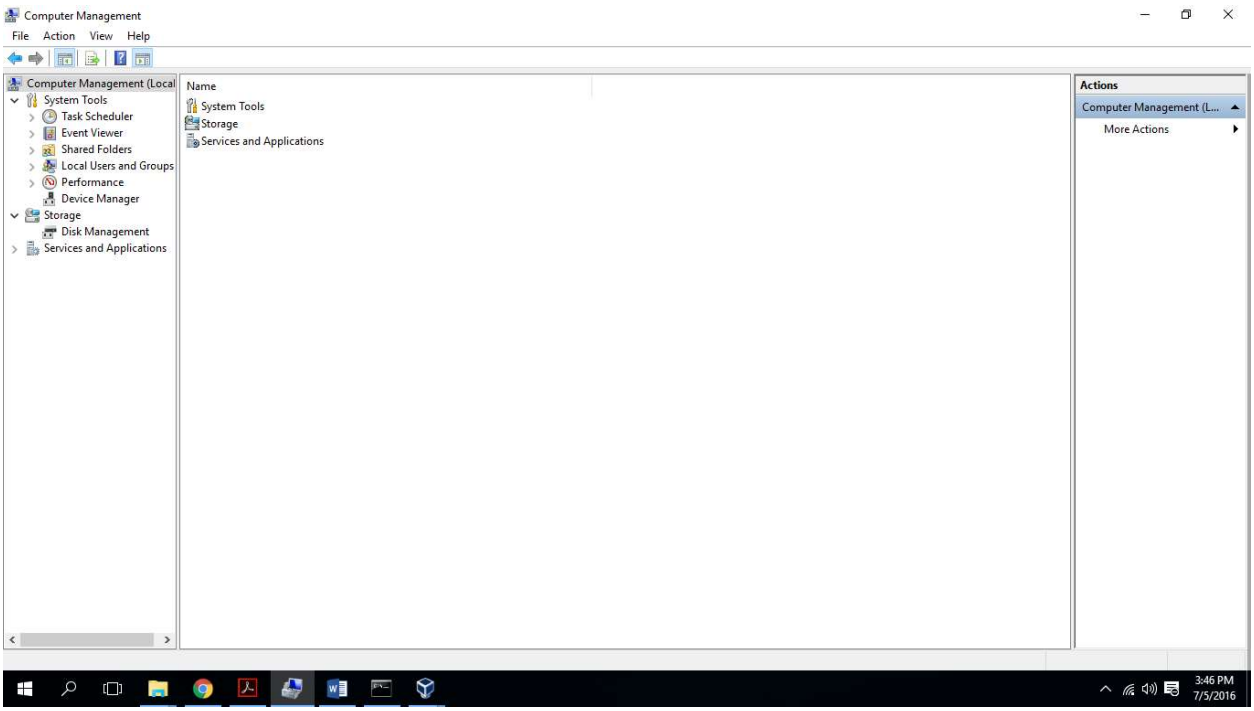


In the above list iam going to spoof my 3rd MAC address for this practical, you have to choose which ever one you want to spoof while you are spoofing.

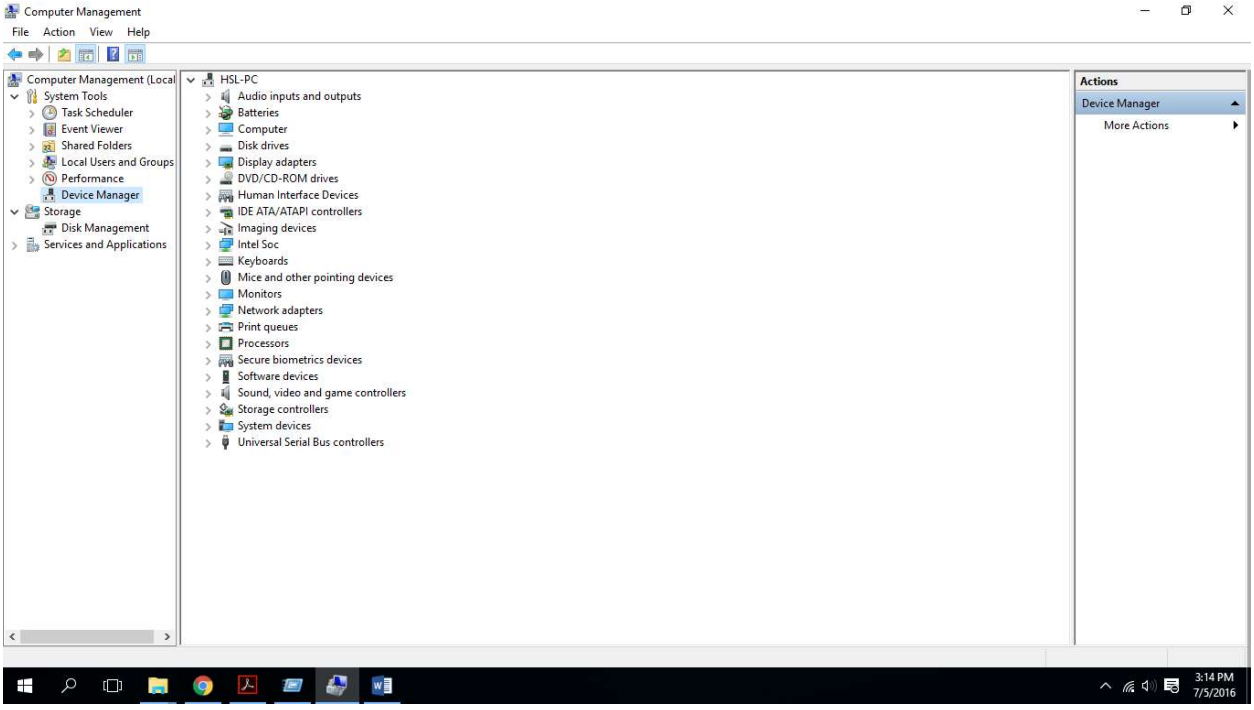
Then open computer management console by executing the below command in run dialog box.



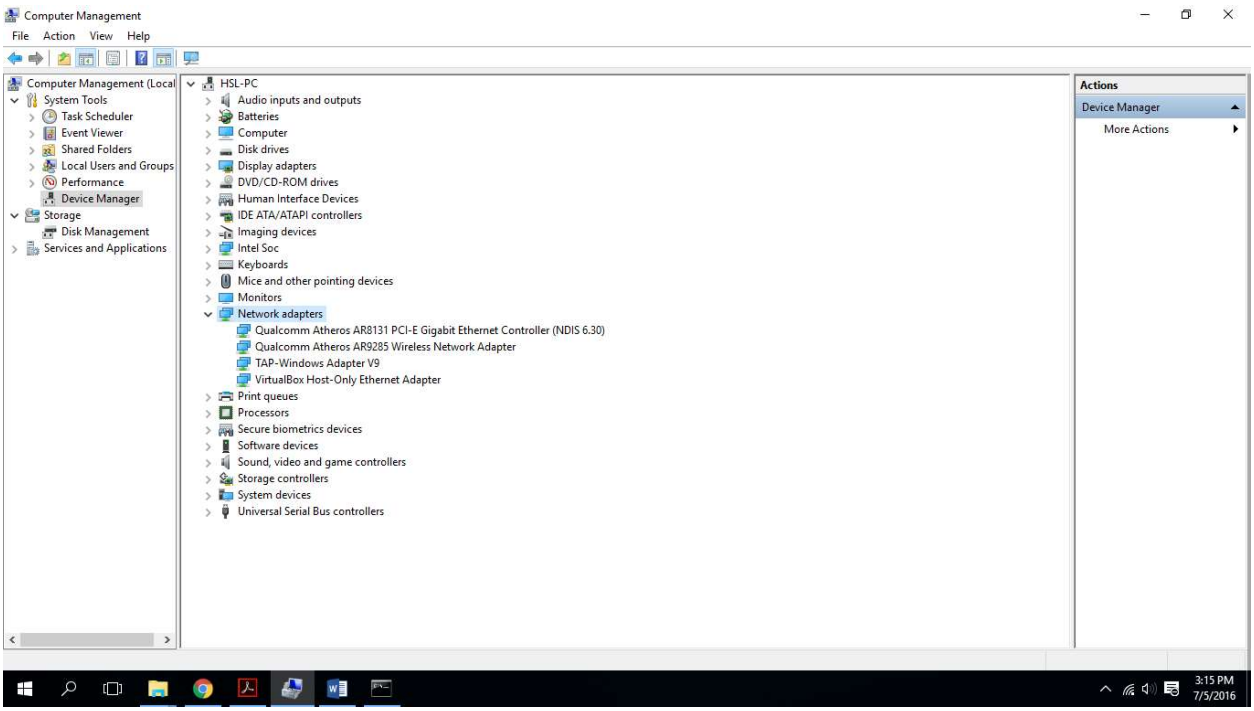
This is how the computer management windows will look like



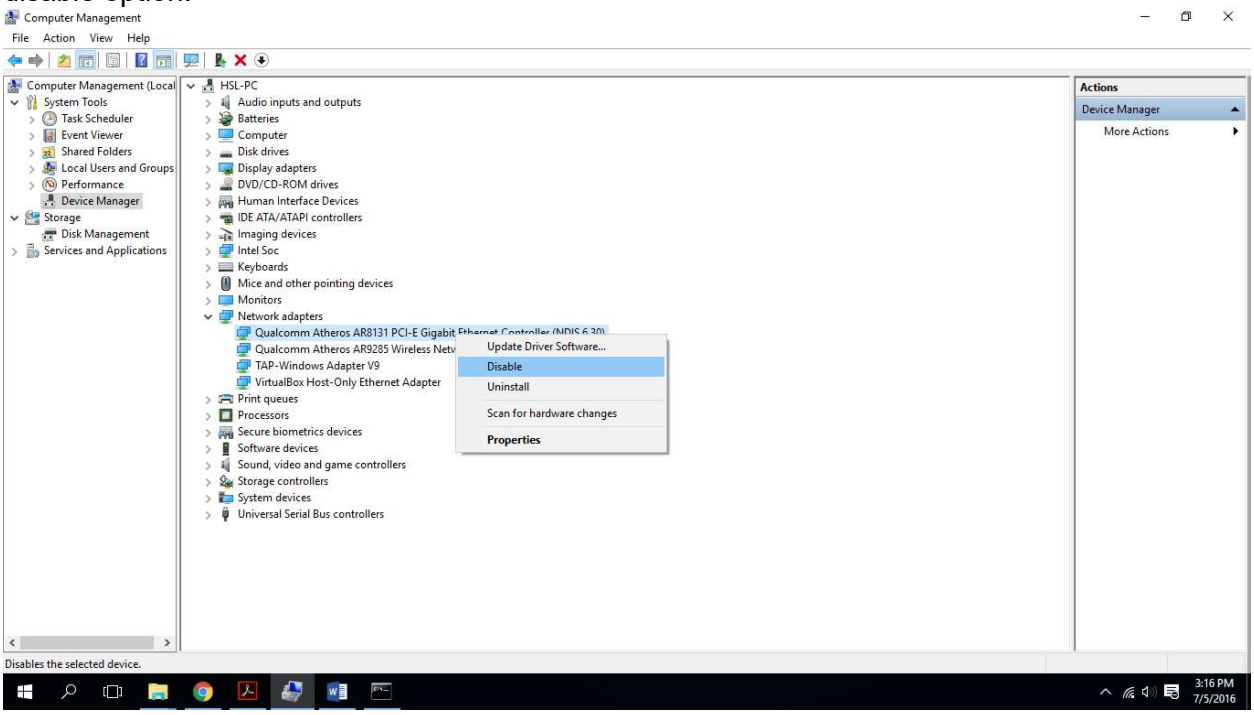
In this computer management window Please select device manager so that you can see right side a list of devices which you have in your machine



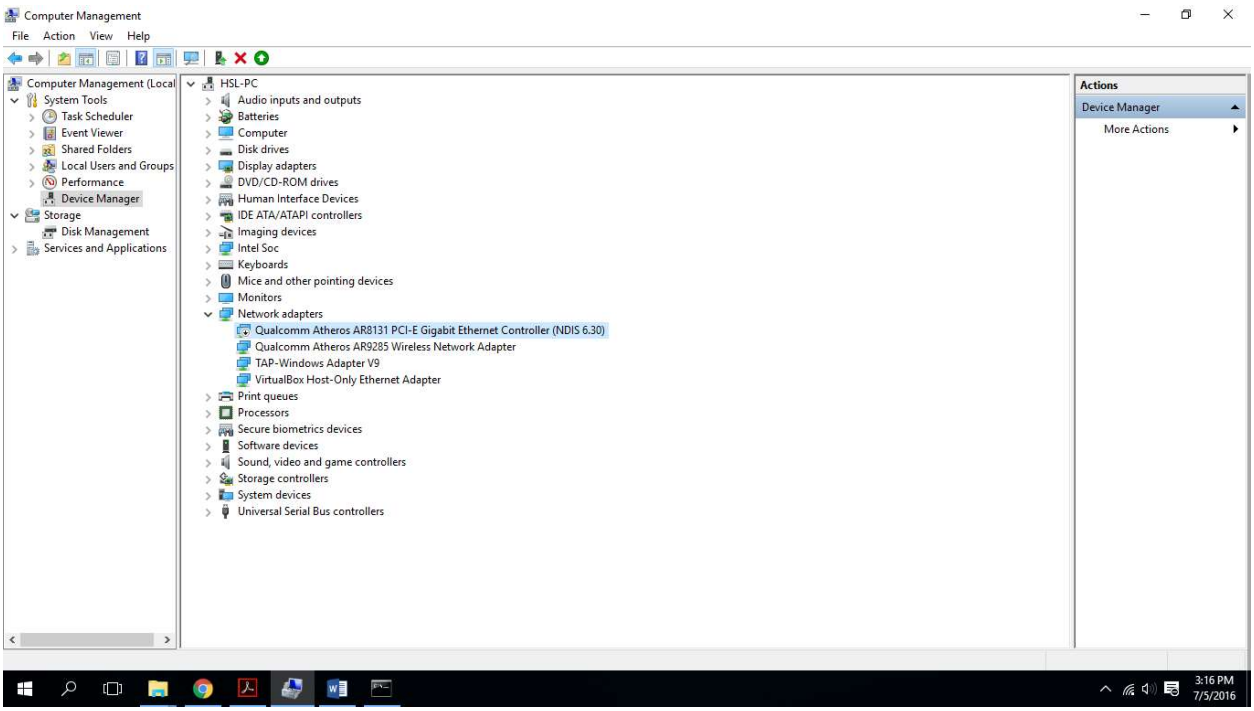
From the list you need to find out network adaptors section and expand the section so you can see whatever NIC cards you have in your machine will be listed out there



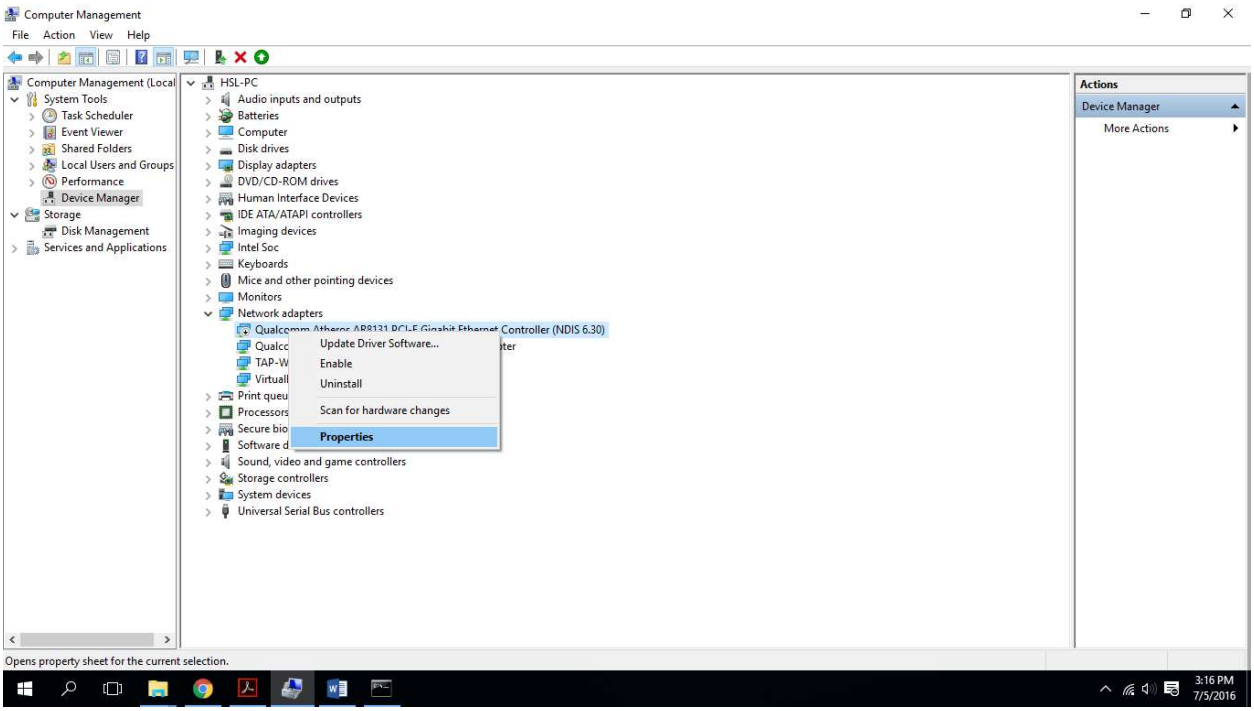
To spoof MAC address to spoof MAC address first you need to disable the NIC card to do that all you have to do is simply right click on it so you can see a Button called Disable select that disable option.



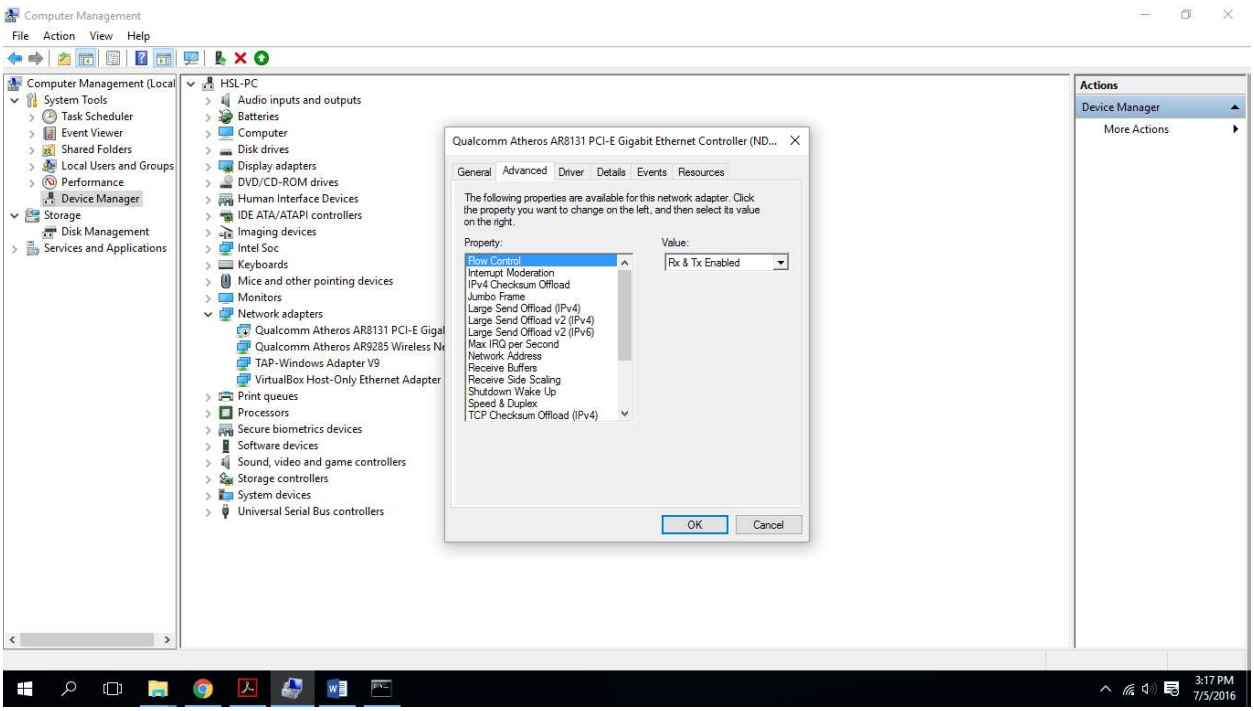
So that your NIC card will be disabled.



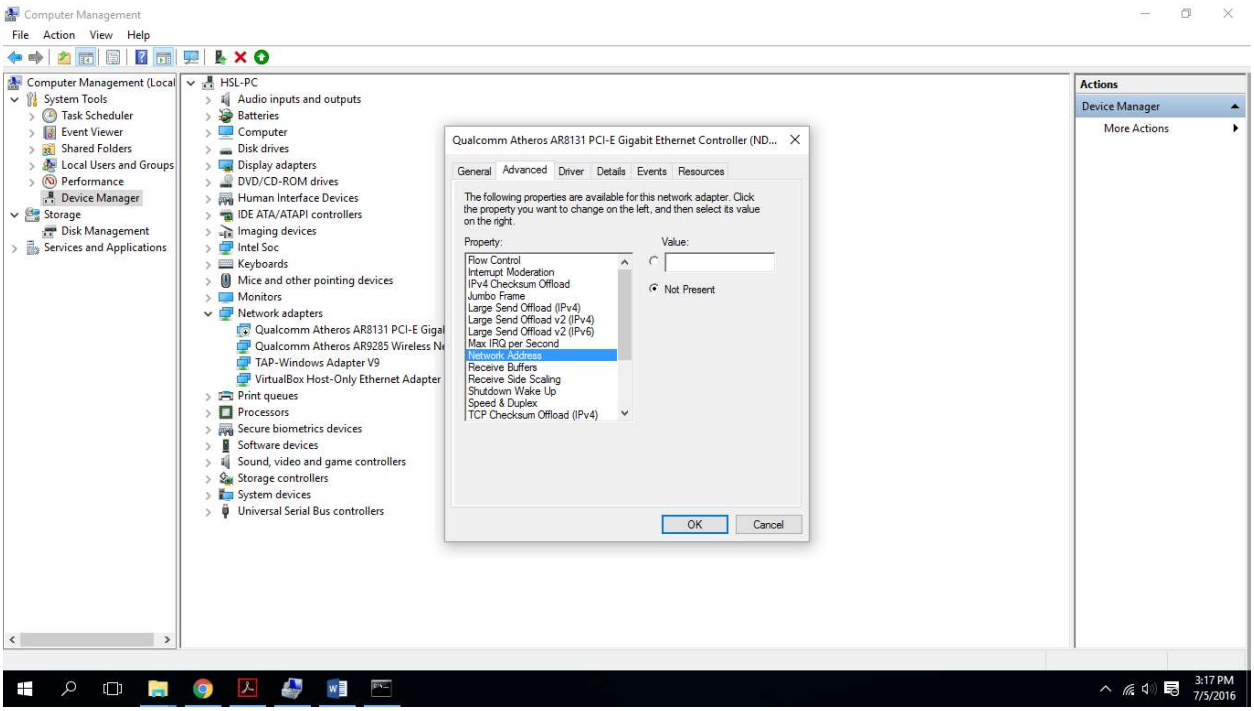
Once its disabled right click on the NIC card and select properties so that you can see a dialogue box



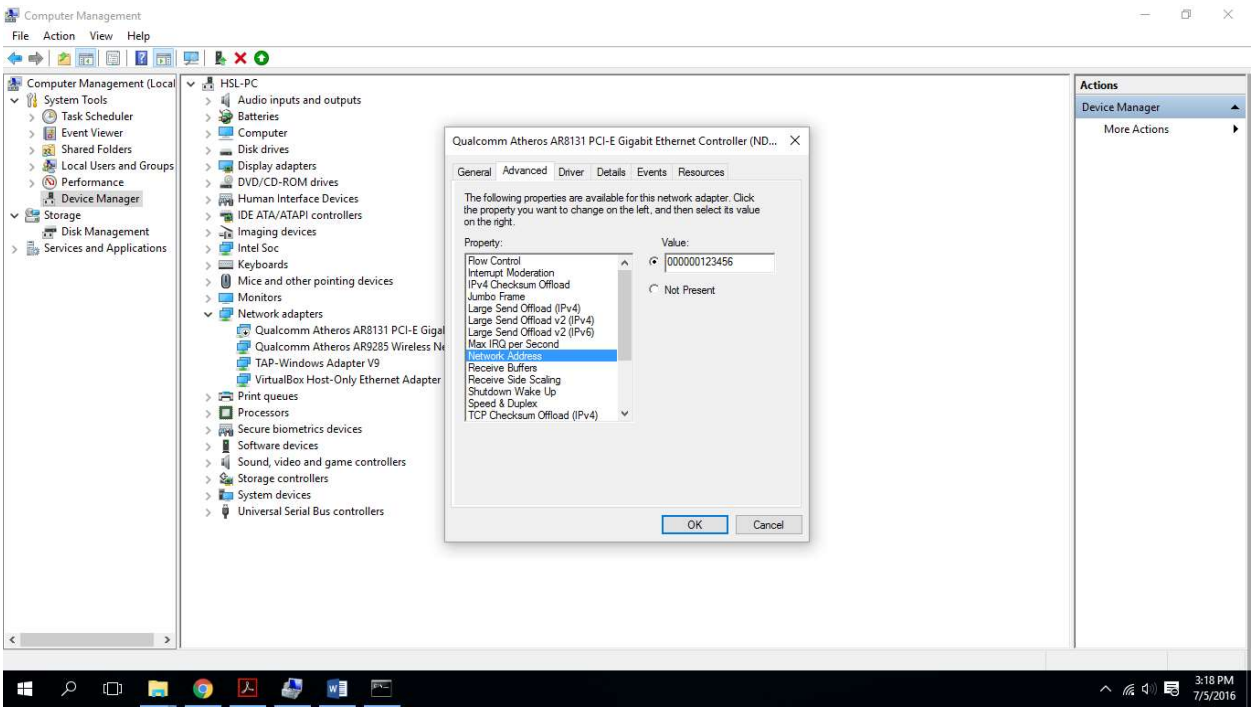
In that dialogue box go to advanced section in the advanced section



so please find out an option with the name network address Select that once you find it So you can see right side two options with the name not present and value

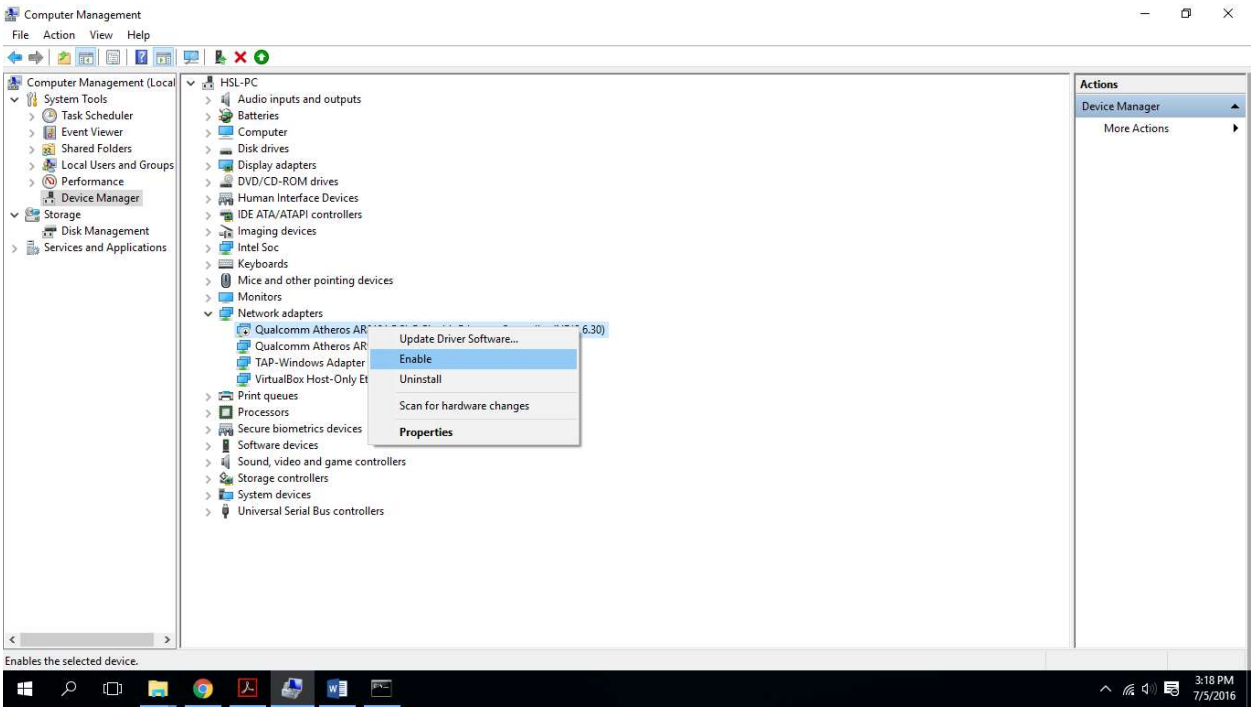


here the not present represents the default MAC address whereas the value represents your custom MAC address by default it will select the not present what you have to do is Select the value and give whatever MAC address you want to use.

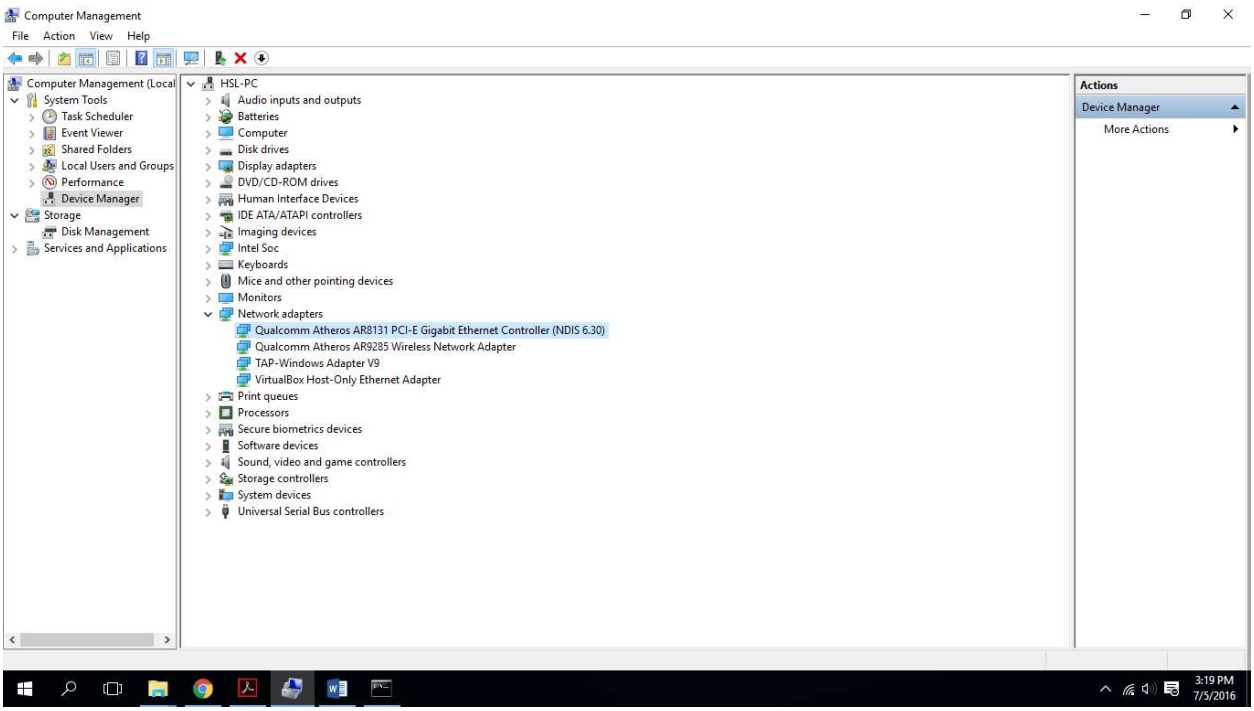


Once you are custom MAC address is given click on Ok so that the settings will be saved.

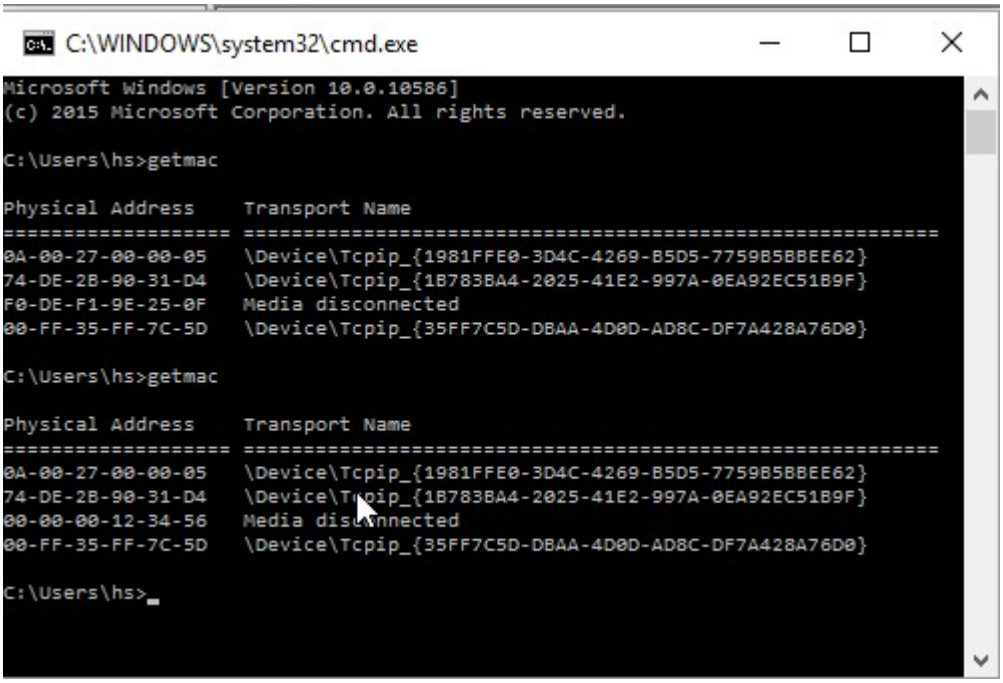
Now all you have to do is enable the NIC card which you have disabled earlier.



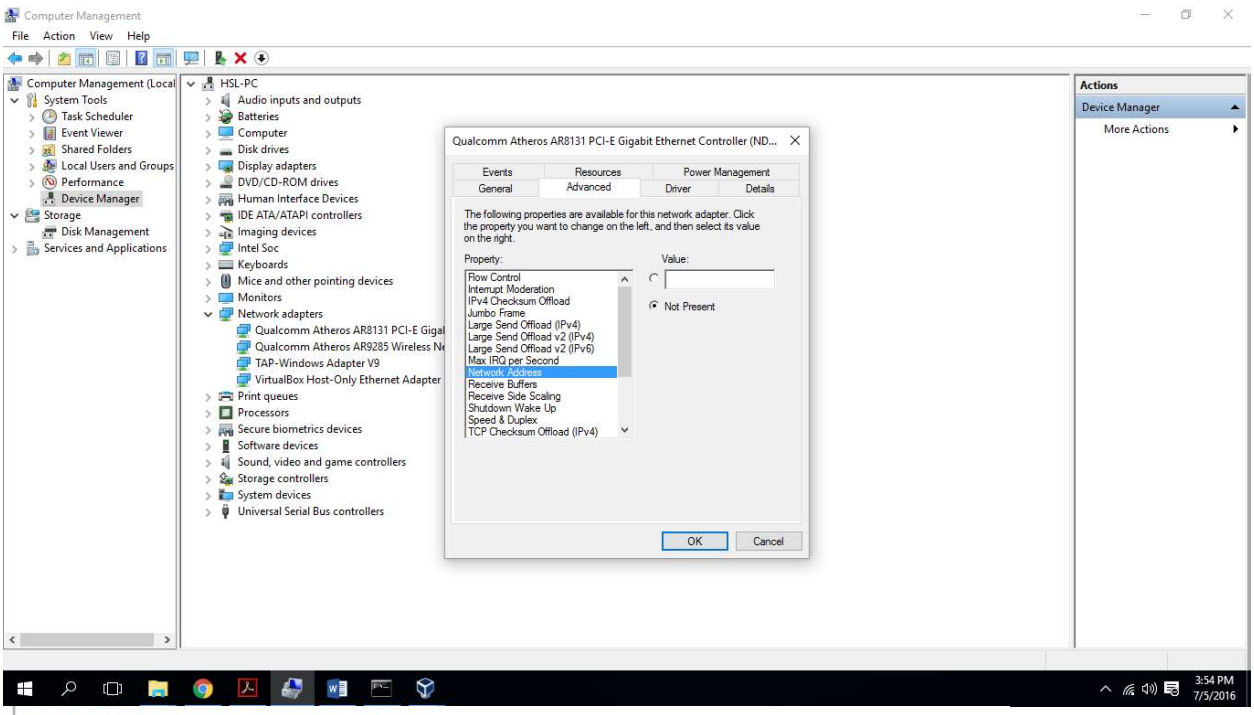
Right click on the NIC card and select enable option.

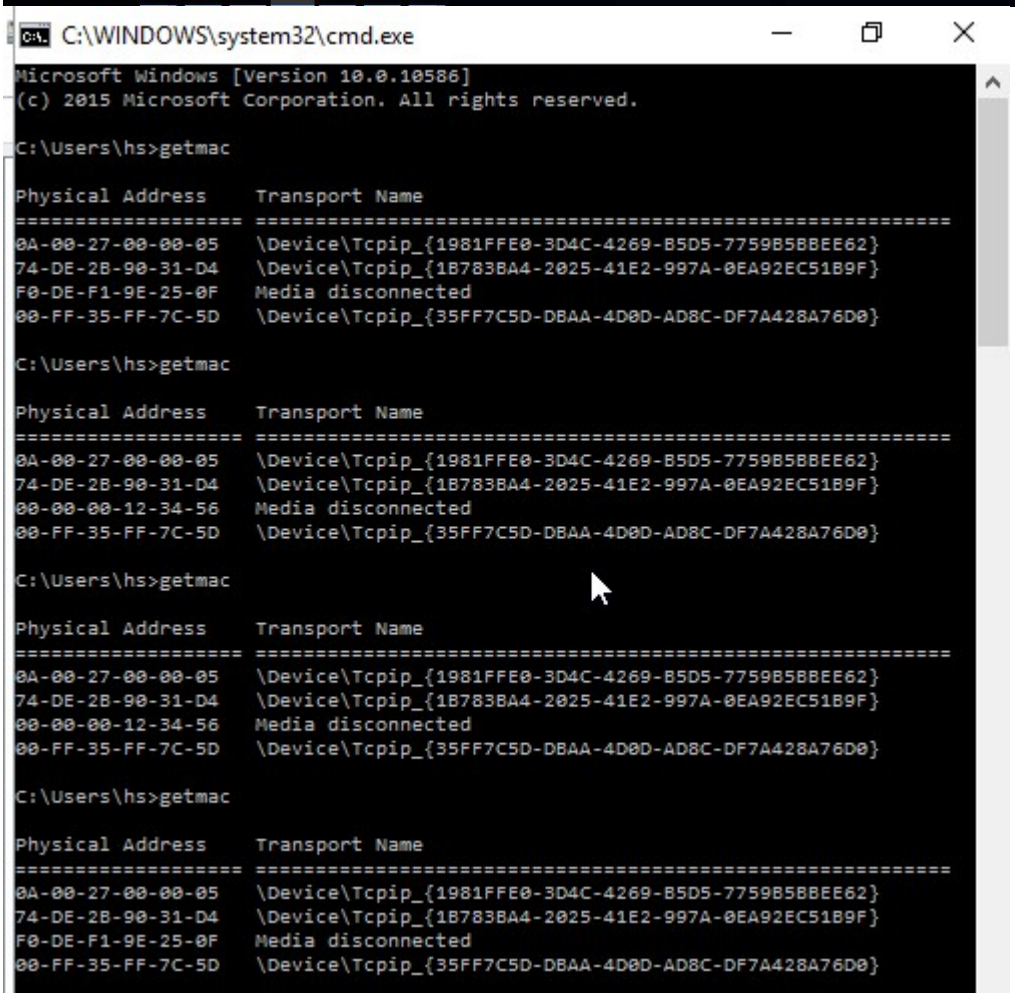


As soon as you enable check out your MAC address with the get MAC command, you can observe the changed MAC address in the command prompt window. Now any connections you made with this spoofed NIC card will show your custom given MAC address



Once your work is finished if you want to get back your original MAC address all you have to do is disable the NIC card again and open the properties and switch back to not present if you check out your MAC address again it will be your original MAC Address just like the picture shown below.

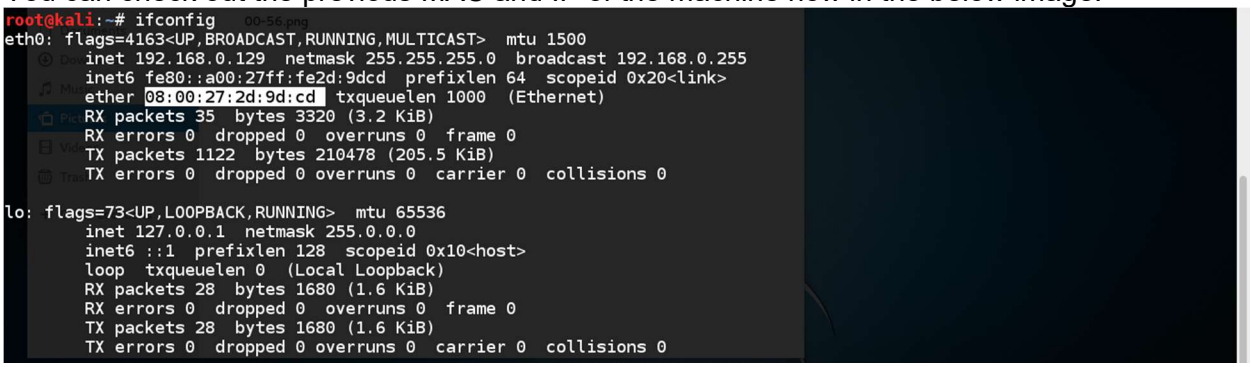

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
HSL-PC
Audio inputs and outputs
Batteries
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Human Interface Devices
IDE ATA/ATAPI controllers
Imaging devices
Intel Soc
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Qualcomm Atheros AR8131 PCI-E Gigal
Qualcomm Atheros AR9285 Wireless Ne
TAP-Windows Adapter V9
VirtualBox Host-Only Ethernet Adapter
Print queues
Processors
Secure biometrics devices
Software devices
Sound, video and game controllers
Storage controllers
System devices
Universal Serial Bus controllers
Qualcomm Atheros AR8131 PCI-E Gigabit Ethernet Controller (ND...
Events
Resources
Power Management
General
Advanced
Driver
Details
The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.
Property:
Value:
Flow Control
Interrupt Moderation
IPv4 Checksum Offload
Jumbo Frame
Large Send Offload (IPv4)
Large Send Offload v2 (IPv4)
Large Send Offload v2 (IPv6)
Max IRQ per Second
Network Address
Receive Buffers
Receive Side Scaling
Shutdown Wake Up
Speed & Duplex
TCP Checksum Offload (IPv4)
Not Present
OK
Cancel
Actions
Device Manager
More Actions
3:54 PM
7/5/2016


C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\hs>getmac
Physical Address Transport Name
0A-00-27-00-00-05 \Device\Tcpip_{1981FFE0-3D4C-4269-B5D5-7759B5BBEE62}
74-DE-2B-90-31-D4 \Device\Tcpip_{1B783BA4-2025-41E2-997A-0EA92EC51B9F}
F0-DE-F1-9E-25-0F Media disconnected
00-FF-35-FF-7C-5D \Device\Tcpip_{35FF7C5D-DBAA-4D0D-AD8C-DF7A428A76D0}
C:\Users\hs>getmac
Physical Address Transport Name
0A-00-27-00-00-05 \Device\Tcpip_{1981FFE0-3D4C-4269-B5D5-7759B5BBEE62}
74-DE-2B-90-31-D4 \Device\Tcpip_{1B783BA4-2025-41E2-997A-0EA92EC51B9F}
00-00-00-12-34-56 Media disconnected
00-FF-35-FF-7C-5D \Device\Tcpip_{35FF7C5D-DBAA-4D0D-AD8C-DF7A428A76D0}
C:\Users\hs>getmac
Physical Address Transport Name
0A-00-27-00-00-05 \Device\Tcpip_{1981FFE0-3D4C-4269-B5D5-7759B5BBEE62}
74-DE-2B-90-31-D4 \Device\Tcpip_{1B783BA4-2025-41E2-997A-0EA92EC51B9F}
00-00-00-12-34-56 Media disconnected
00-FF-35-FF-7C-5D \Device\Tcpip_{35FF7C5D-DBAA-4D0D-AD8C-DF7A428A76D0}
C:\Users\hs>getmac
Physical Address Transport Name
0A-00-27-00-00-05 \Device\Tcpip_{1981FFE0-3D4C-4269-B5D5-7759B5BBEE62}
74-DE-2B-90-31-D4 \Device\Tcpip_{1B783BA4-2025-41E2-997A-0EA92EC51B9F}
F0-DE-F1-9E-25-0F Media disconnected
00-FF-35-FF-7C-5D \Device\Tcpip_{35FF7C5D-DBAA-4D0D-AD8C-DF7A428A76D0}

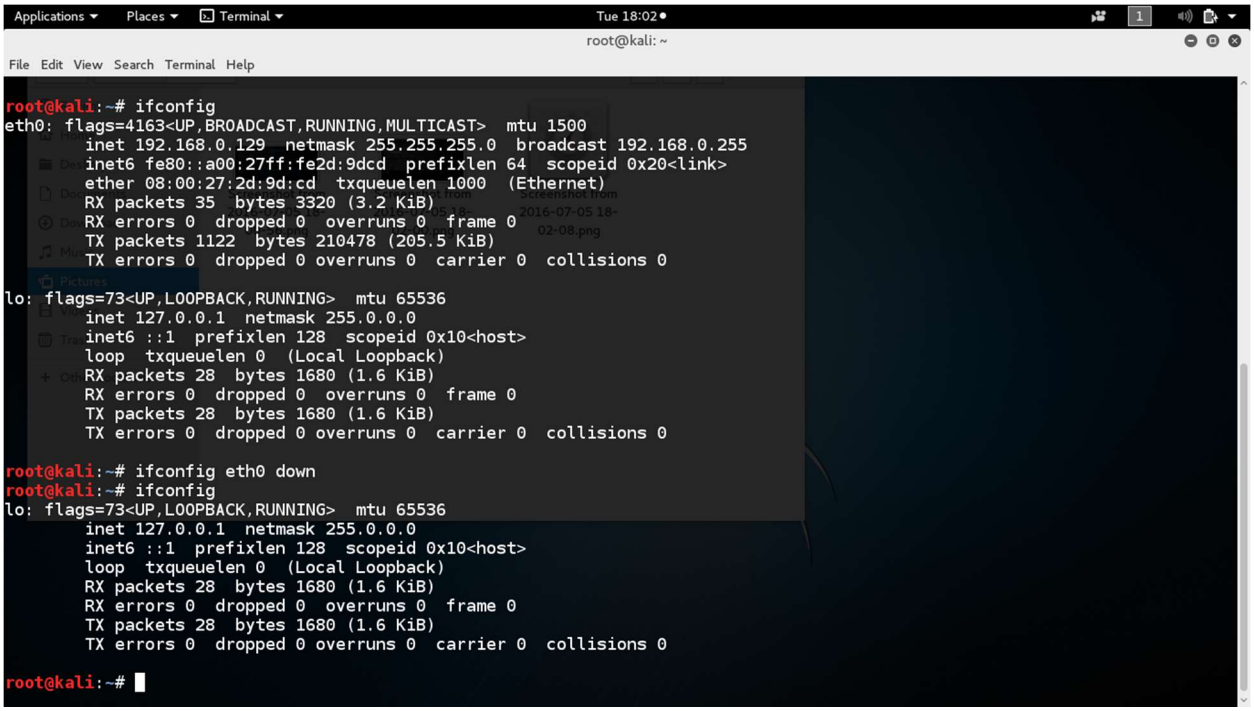
Practical 6: MAC Spoofing in Linux

Just like in Windows even in Linux also the processes disable the NIC card change the Mac address and enable the NIC card.

So to first disabled NIC card we will proceed with a command in the console
You can check out the previous MAC and IP of the machine now in the below image.

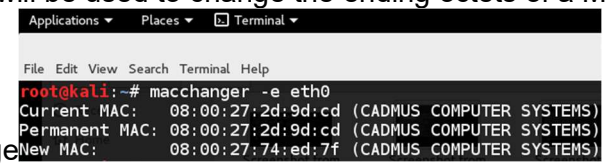


The command given above will disable the NIC card
As you can see after execution of the command ifconfig command will only show lo, where eth0 is disappeared

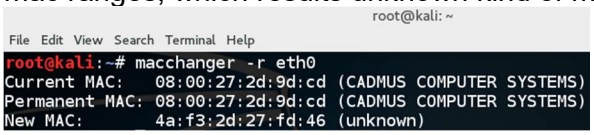


now in Kali Linux we have a tool called Mac changer which will be helpful in spoofing Mac addresses We have a wide range of options in Mac changer so that we can use in specific scenarios now I am going to show you different usages of those options so that you can decide while you are using which one will be suitable for you.

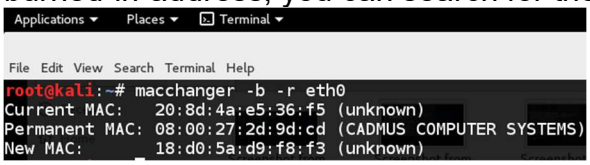
Option ‘-e’ will be used to change the ending octets of a Mac address which will look like the below image



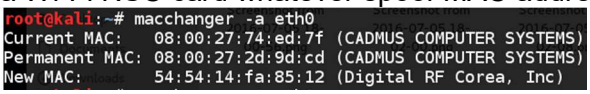
Option “-r” will give me the complete random MAC address which will not come in any of the mac ranges, which results unknown kind of mac



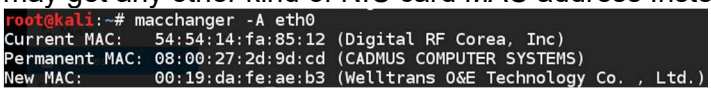
While the option “–r” giving complete random mac “–b –r” combo will try to give some burned-in-address, you can search for the “burned-in-address” in wiki to get more info



Option “-a” will be used to have a random address of the same kind here same kind refers to if you have a LAN NIC card whatever spoofed Mac you will get also will be a LAN one, If you have a Wi-Fi NSC card whatever spoof MAC address you will get will also will be a Wi-Fi one.



Option “-A” will be used to have a random NIC card of the any kind. Which means you may have a LAN NIC card but you may not get a LAN NIC MAC, you may have a Wi-Fi NIC card you may get any other kind of NIC card MAC address Instead.



Option l will be used to list out different MAC address ranges of different companies, so that you can choose any of the starting bits as your custom MAC address

```
root@kali:~# macchanger -l
Applications  Places  Terminal  Tue 18:03
root@kali: ~
File  Edit  View  Search  Terminal  Help
0009 - 00:04:5a - Linksys WPC11, WUSB11
0010 - 00:04:75 - 3Com 3CRWE62092B
0011 - 00:04:e2 - SMC SMC2632W
0012 - 00:05:5d - D-Link DWL-650, DWL-650H
0013 - 00:06:25 - Linksys WPC11 v2.5, D-Link DCF-650W, Linksys WPC11 v3
0014 - 00:07:0e - Cisco AIR-PCM352
0015 - 00:07:50 - Cisco AIR-LMC352
0016 - 00:08:21 - Cisco AIR-PCM352
0017 - 00:09:43 - Cisco AIR-LMC352
0018 - 00:09:5b - Netgear MA701, MA401RA
0019 - 00:09:7c - Cisco AIR-LMC352
0020 - 00:09:e8 - Cisco AIR-LMC352
0021 - 00:0a:41 - Cisco AIR-PCM352
0022 - 00:0a:8a - Cisco AIR-PCM352
0023 - 00:30:65 - Apple Airport Card 2002
0024 - 00:30:ab - Netgear MA401
0025 - 00:30:bd - Belkin F5D6020
0026 - 00:40:96 - Cisco AIR-PC4800, 350, AIR-PCM340, AIR-PCM352
0027 - 00:50:08 - Compaq WL100
0028 - 00:50:da - 3Com 3CRWE73796B
0029 - 00:60:01 - Lucent WaveLAN Silver
0030 - 00:60:1d - Lucent WaveLAN Bronze, WaveLAN Gold, Silver, Orinoco Gold
0031 - 00:60:6d - Cabletron CSIBB-AA
0032 - 00:60:b3 - SMC SMC2642W
0033 - 00:80:c7 - Netwave (Xircom Netwave/Netwave Airsurfer)
0034 - 00:90:d1 - LeArtery SyncByAir LN101
0035 - 00:a0:f8 - Symbol Spectrum24
0036 - 00:0c:f1 - Intel Pro 2100
0037 - 00:e0:29 - OEM OEM
0038 - 08:00:0e - Old Lucent Wavelan
0039 - 08:00:46 - Sony PCWA-C10
root@kali:~#
```

Option “–m” or “--mac=” using this option we can choose our own custom MAC address you can use the help of “-l” option, I have chosen 00:00:00 which belongs to Xerox.

```
Applications  Places  Terminal
File  Edit  View  Search  Terminal  Help
root@kali:~# macchanger --mac=00:00:00:11:22:33 eth0
Current MAC:   8e:83:3c:e1:cc:1a (unknown)
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)
New MAC:       00:00:00:11:22:33 (XEROX CORPORATION)
```

Once you choose any of the above options you have to enable your NIC card so that your NIC card will work.

The command to enable your NIC is

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ifconfig eth0 up
root@kali:~#
```

You can see the result like this below image. Where MAC changed and ip assigned to the new MAC.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.130  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::200:ff:fe11:2233  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:11:22:33  txqueuelen 1000  (Ethernet)
        RX packets 236  bytes 18920 (18.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1155  bytes 214186 (209.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 44  bytes 2784 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 2784 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

If you want to get your real MAC.

Disable the NIC, (Command is right up in the starting of the practical)

Option “-p” will be used to Restore our original MAC address back

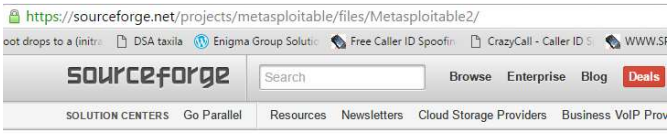
```
root@kali:~# macchanger -p eth0
Current MAC:   00:00:00:11:22:33 (XEROX CORPORATION)
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)
New MAC:       08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)
```

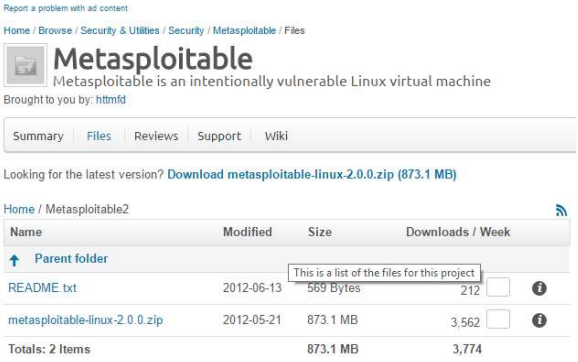
Enable the NIC, (Command is right up in the ending of the practical)

Practical No 7: Installing Vulnerable Machine to Practice:

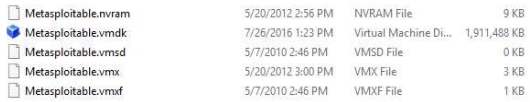
Download and Install Virtual Machine In Your PC. (Steps are provided in the first practical)

Go to http://sourceforge.net/projects/metasploitable/files/Metasploitable2/ and download the metasploitable Virtual image file and save it to your machine and extract it.





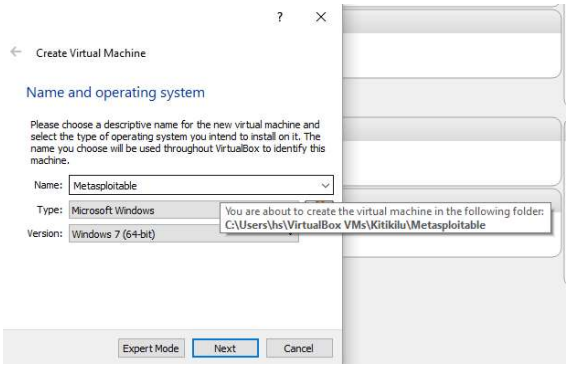
After extracting you can see a VMDK file like this



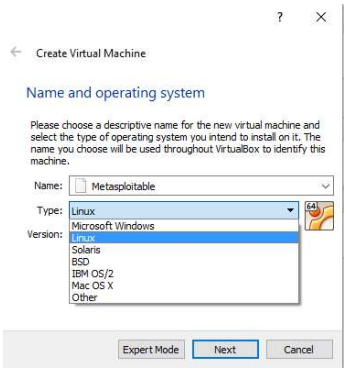
Now start you Virtual Box

Click On New Button 

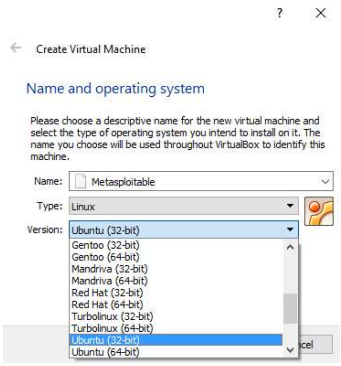
Give a name



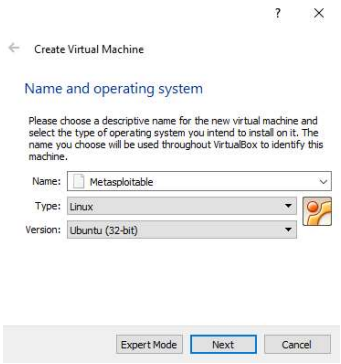
Select Type as Linux



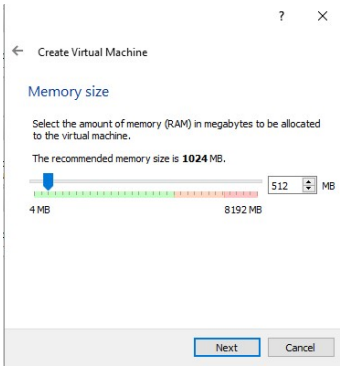
Select Version as Ubuntu 32 Bit.



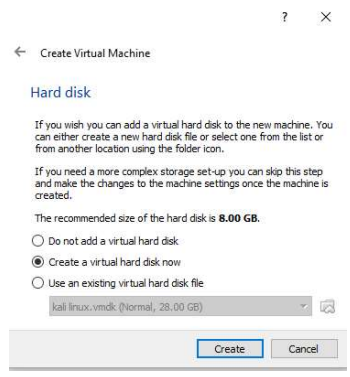
Click On Next



Give RAM(you can choose upto Green Area In The BAR) then Click on next

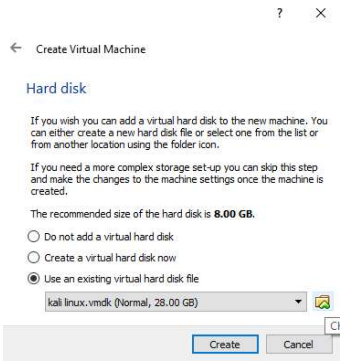


In this screen

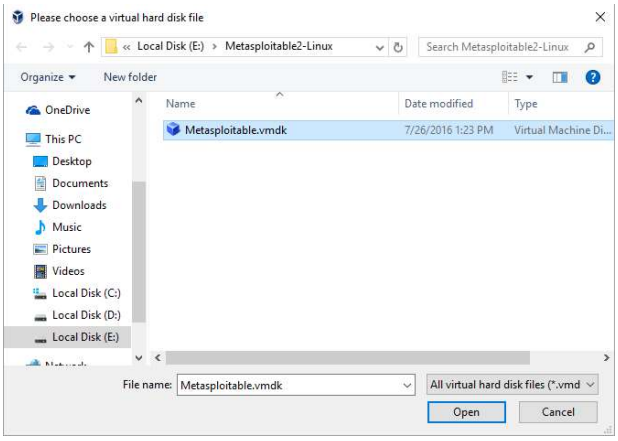


Select third option that is “Use an existing virtual harddisk file”

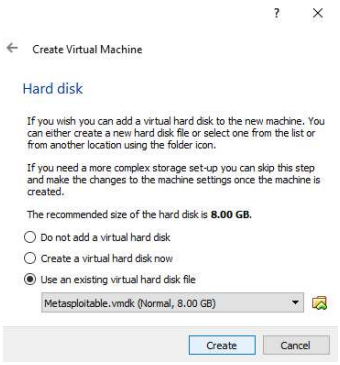
Click on the folder icon to select a file



Locate the file in PC and select and click on “Open”



Finally Click on create button to create a machine.



You can find your new VM in VMS list.

Default username and password for this metasploitable in

Username:msfadmin

Password:msfadmin

Practical No 8 Network Settings in VMs:

By default in any new VM you will have ip address that is 10.0.2.15

The above kind of IP can get internet but will not be able to communicate in the LAN as it has some class A series of IP.

```
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8a:36:b5
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:36b5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5487 (5.3 KB)  TX bytes:12027 (11.7 KB)
          Base address:0xd010 Memory:f0000000-f0020000

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:16436  Metric:1
          RX packets:174 errors:0 dropped:0 overruns:0 frame:0
          TX packets:174 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58781 (57.4 KB)  TX bytes:58781 (57.4 KB)
```

But as Your HOST and other machines in your LAN may have some class C series of IP, so it would be difficult to perform practicals in the LAN.

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9de7:4f80:206e:51d7%2
   IPv4 Address. . . . . . . . . . . : 192.168.0.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

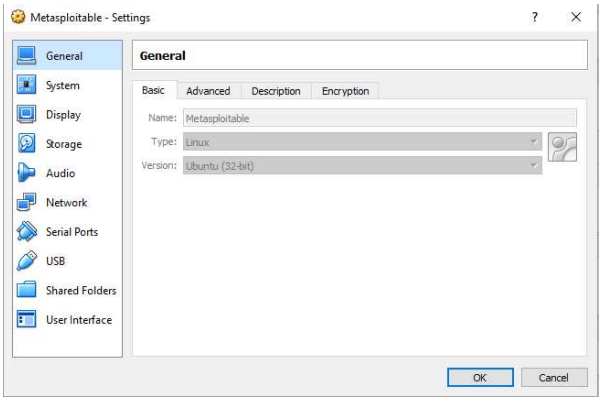
At the point you can change your network settings of VM to make it available in the regular LAN.

Follow the below given steps

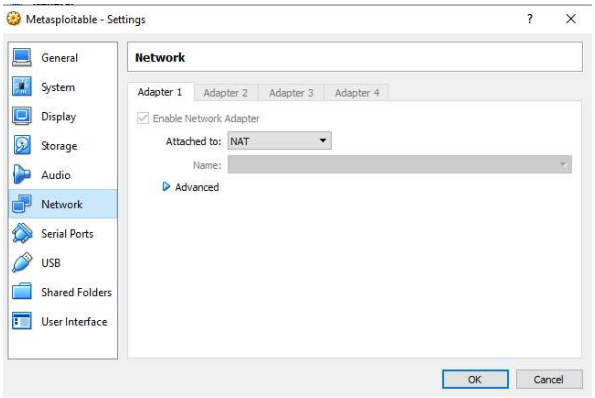
Select the VM you want to change the settings

Then click on settings button on the TOP

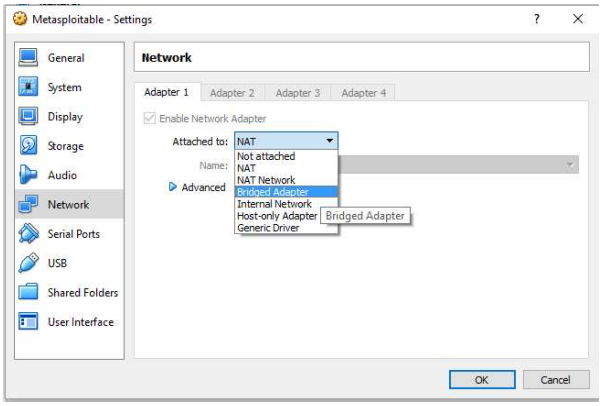
Then you should see the following box on screen.



Click on network tab to switch towards network related settings.

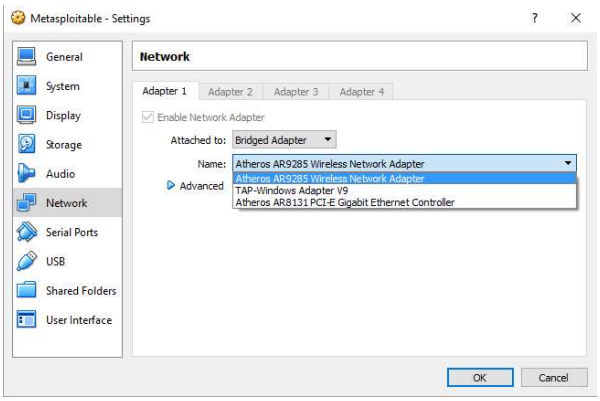


There by default “attached to” is selected as NAT, which results your VM getting Class A IP change it to “Bridged adapter” from the Drop-Down Menu.



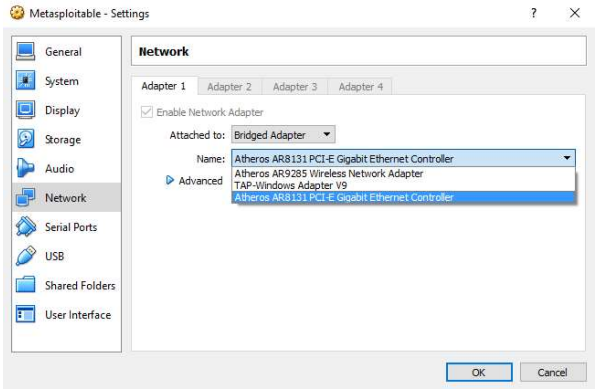
Then if you are using a wifi like this

Select WIFI adapter from the “Name” Drop-Down Menu. (Adapter Name will not be same as mine)

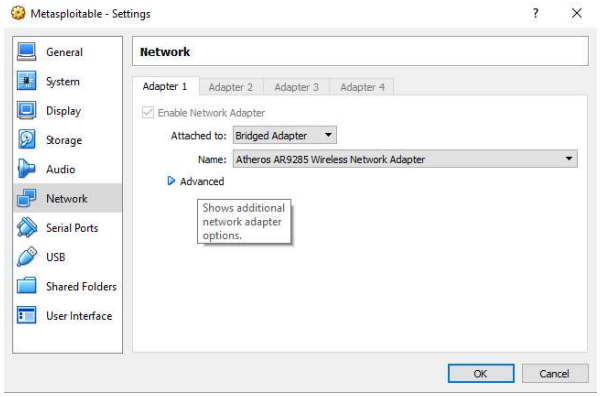


Or if you are using LAN like this

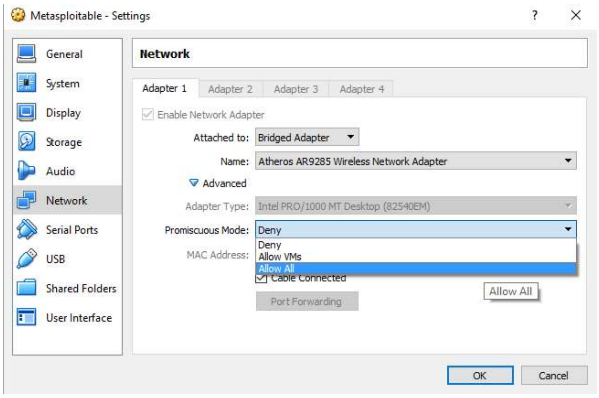
Select Ethernet adapter from the “Name” Drop-Down Menu. (Adapter Name will not be same as mine)

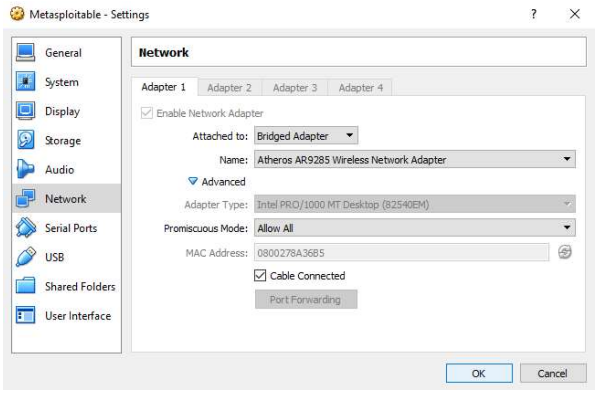


Next click on “Advanced” to expand advanced options.



In the “Advanced” under “Promicuous Mode” change that “Deny” to “Allow All” to make the VM available to all machines in the network. And make sure “cable connected” check box is CHECKED.





Finally Click on OK button

Restart your network if you know how to, if you don't know, try restarting your PC(HOST and VM Both) to avoid issues.

After a while you can see your VM also having IP that belongs to your host network(if your network is good enough ☺)

```
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8a:36:b5
          inet addr:192.168.0.156  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8a:36b5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:908 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85116 (83.1 KB)  TX bytes:13596 (13.2 KB)
          Base address:0xd010 Memory:f0000000-f0020000

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:16436  Metric:1
          RX packets:200 errors:0 dropped:0 overruns:0 frame:0
          TX packets:200 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:71229 (69.5 KB)  TX bytes:71229 (69.5 KB)
```