

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

First download virtual box and also Download Kali Linux ISO File

The screenshot shows the official Kali Linux Downloads page. At the top, there's a navigation bar with links to Blog, Downloads, Training, Documentation, Community, and About Us. Below the navigation is a section for social media followers: 'Follow @offsectrainin' (82.5K followers) and 'Follow @exploitdb' (95.3K followers). A large table below lists Kali Linux releases from 2016.1, including Kali Linux 64 bit, Kali Linux 32 bit, Kali Linux 64 bit Light, Kali Linux 32 bit Light, and Kali Linux armhf. The 'Download Kali Linux 64 bit ISO' link is highlighted with a red box.

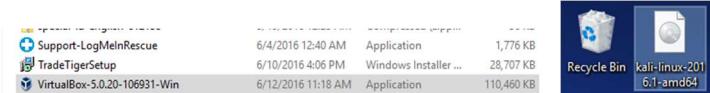
Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	2.6G	2016.1	deaa41c5c8f26b7854caf34b6ff1b567871c4875
Kali Linux 32 bit	ISO	Download Kali Linux 64 bit ISO torrent	2.6G	2016.1	23dadf9c6d3fc190e345ee070aa57155e93b745
Kali Linux 64 bit Light	ISO	Torrent	0.8G	2016.1	4132238042deba9e3bc1702afbdb1b4672b64bcb
Kali Linux 32 bit Light	ISO	Torrent	0.8G	2016.1	addd89b750e31030e96c6cbd5a3da4f0f17287a8
Kali Linux armhf	Image	Torrent	0.7G	2016.1	cd750dde538eaed9f8e4fea011a9b9dc1e75143

Download Kali Linux VMware, VirtualBox and ARM images

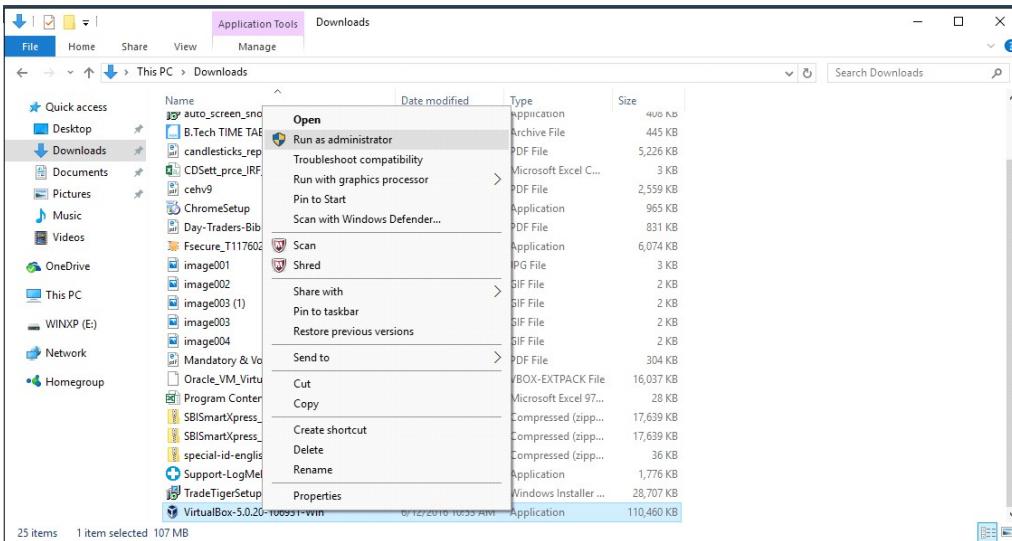
The screenshot shows the VirtualBox download page. At the top, there's a navigation bar with links to About, Screenshots, Downloads, Documentation, End-user docs, Technical docs, Contribute, and Community. The main content area features a large 'VirtualBox' logo and a 'Download VirtualBox' button. Below this, there's a section for 'VirtualBox binaries' with a list of available packages. A note at the bottom of this section says: 'See the changelog for what has changed. You might want to compare the SHA256 checksums or the MD5 checksums to verify the integrity of downloaded packages. The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!' A note at the bottom of the page says: 'Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.' The status bar at the bottom of the browser window shows the date as 6/12/2016 and the time as 11:26 AM.



Have the two files ready before you begin



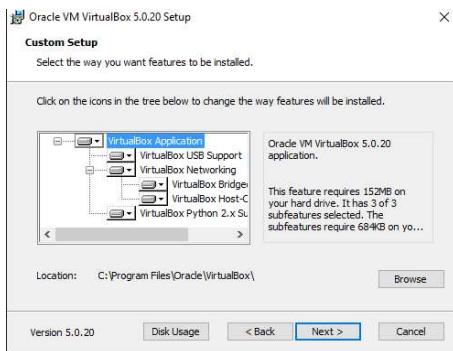
First install Virtual box by right clicking and selecting run as administrator



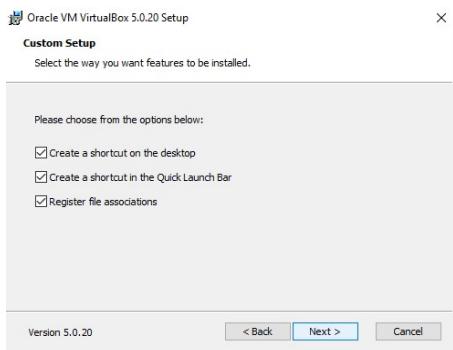
Click Next in the Below Image



Click Next



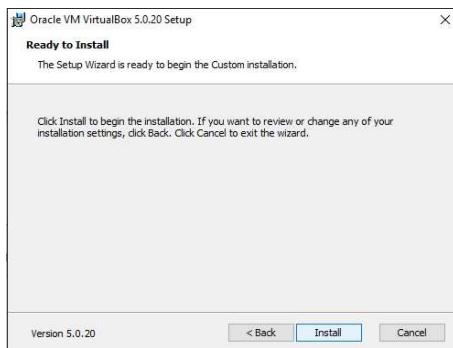
Click Next



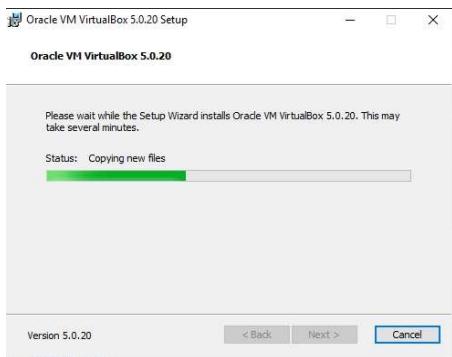
Click YES



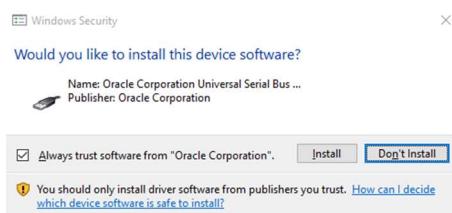
Click Install



Wait



Click Install Here

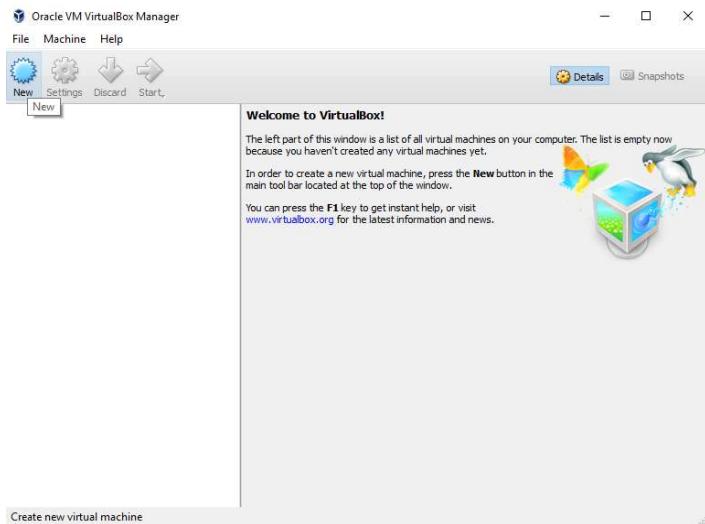


Click Finish



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

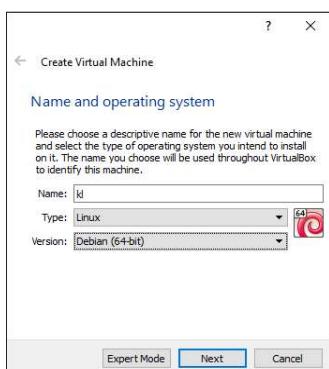
Click New Button Here



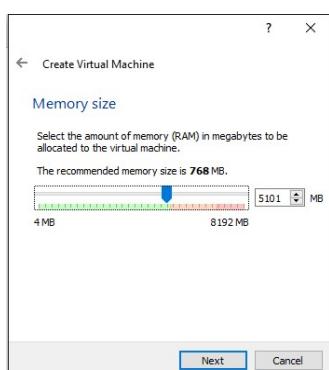
Give some name in the name box

Select Linux as Type

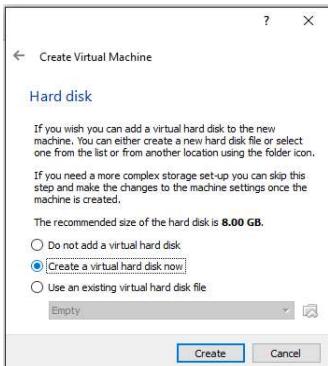
Select Debian 32 or 64 as Version Click Next



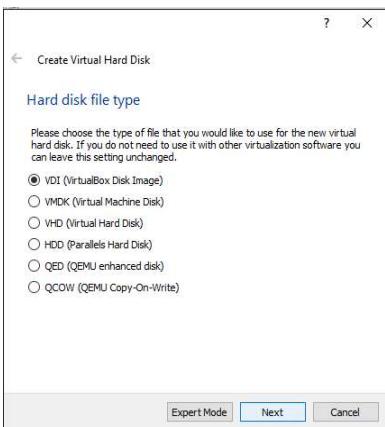
Give the amount of ram you want to allocate to your VM (it has to be in green limit) (minimum 3 GB recommended) and Click on Next



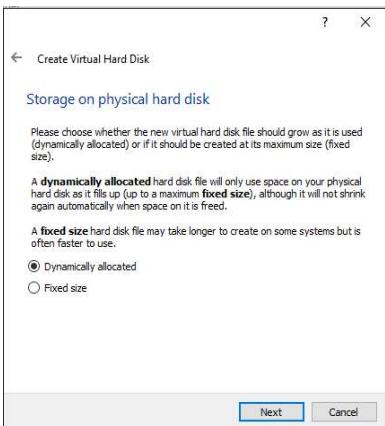
Select Create a virtual hard disk now option and click Create Button.



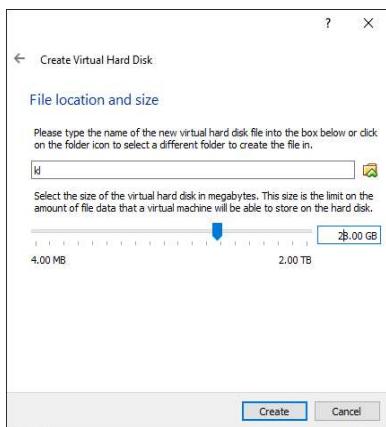
Select VDI as Hard disk Type and Click Next



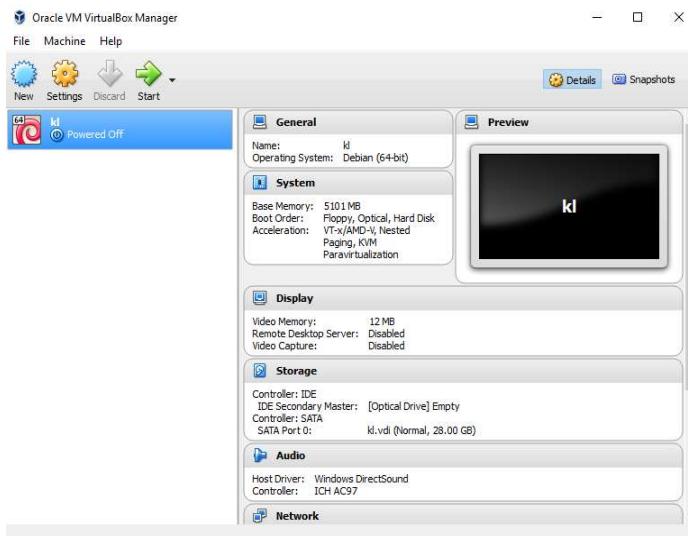
Select Dynamically Allocated As Storage and Click Next



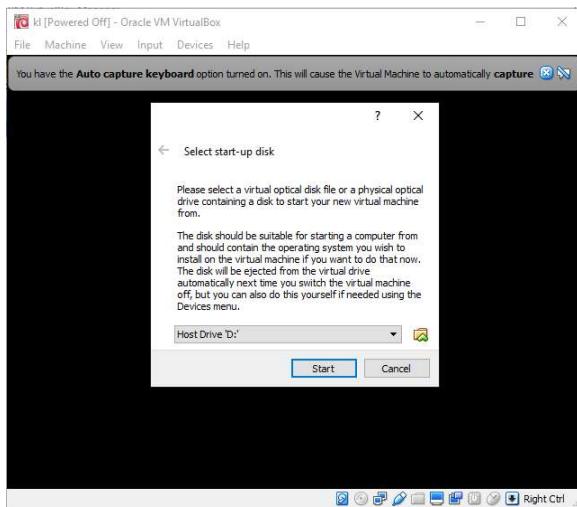
Change the file size to more than 20 GB for better performance and Click on Create Button.

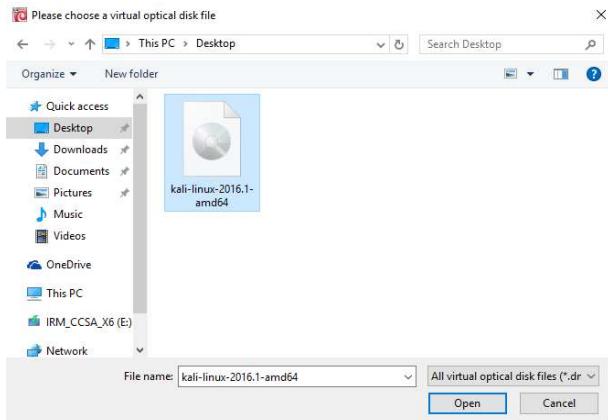


So Finally the OS will be created and listed like below diagram. Click on start button to start or double click the OS name to start.

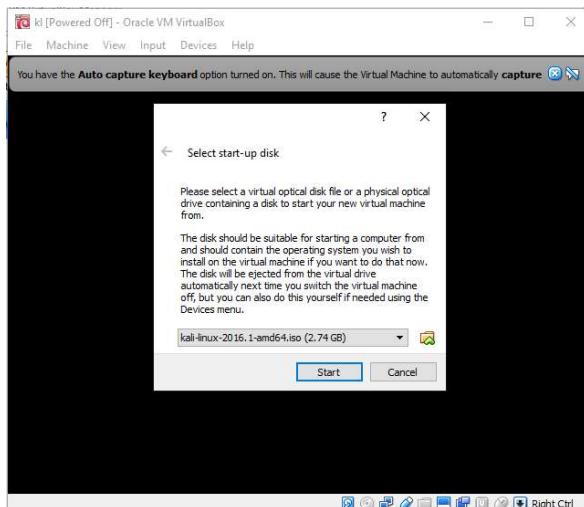


When it asks the Startup disk please select your downloaded kali Linux ISO file





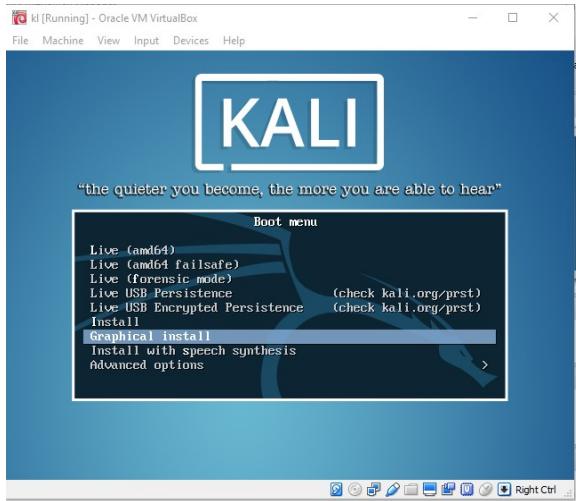
And Click On Start Button.



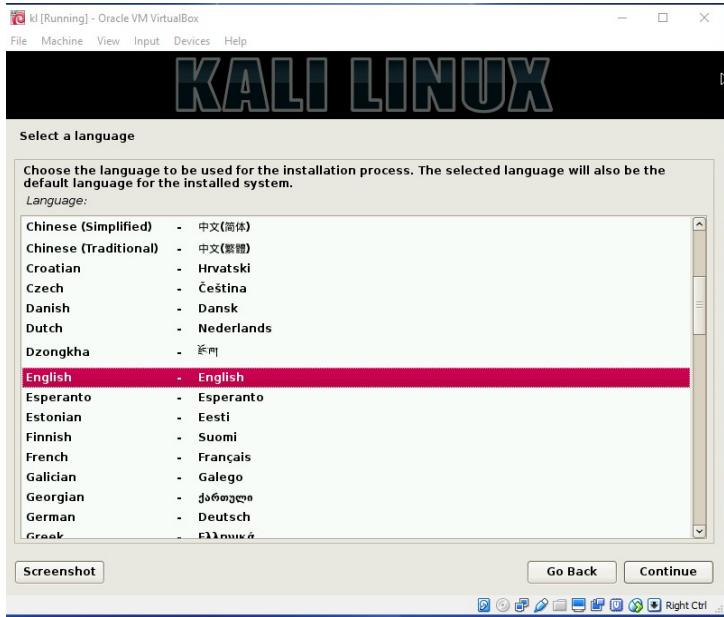
After few moments it will load like this



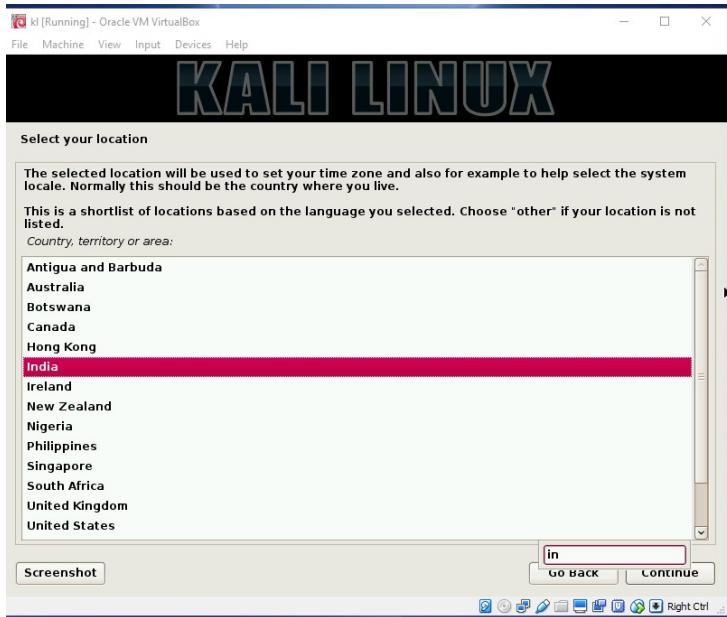
Select Graphical install with your keyboard down arrow keys and Press Enter.



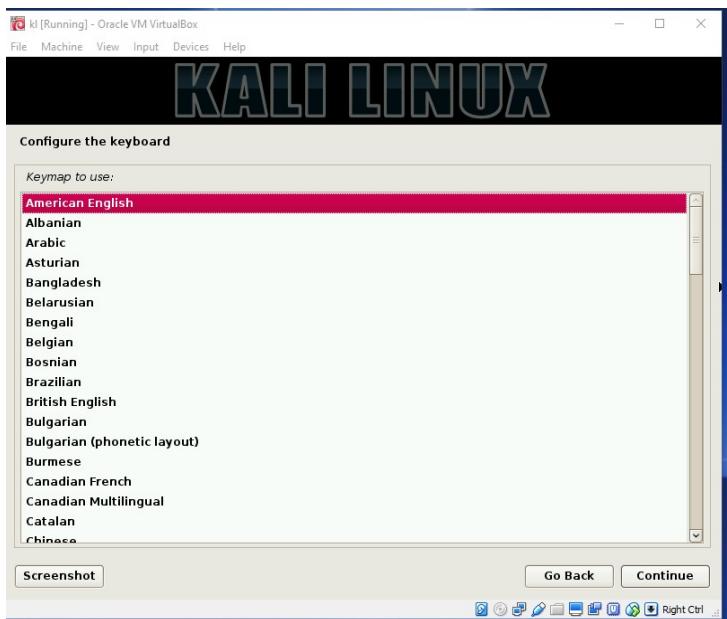
When it asks the Language select the Language you want (English Would be Good) and click on continue



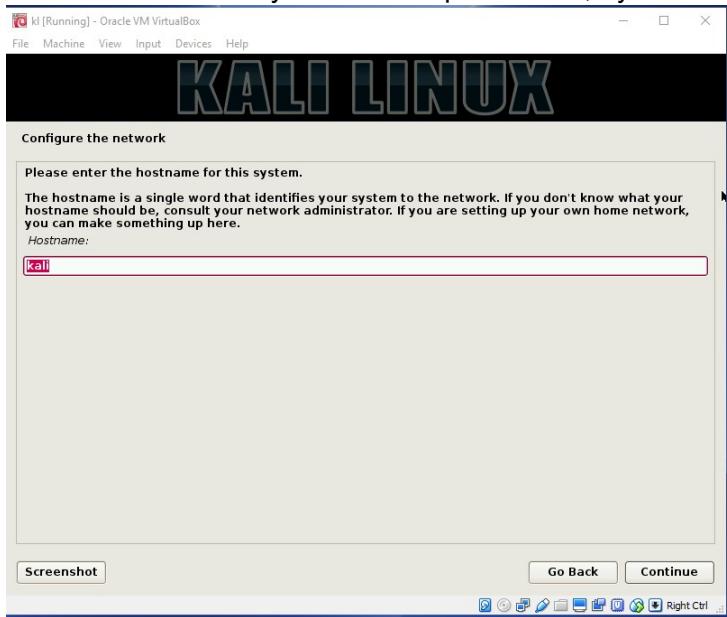
In the country section select your country (India here) and click continue



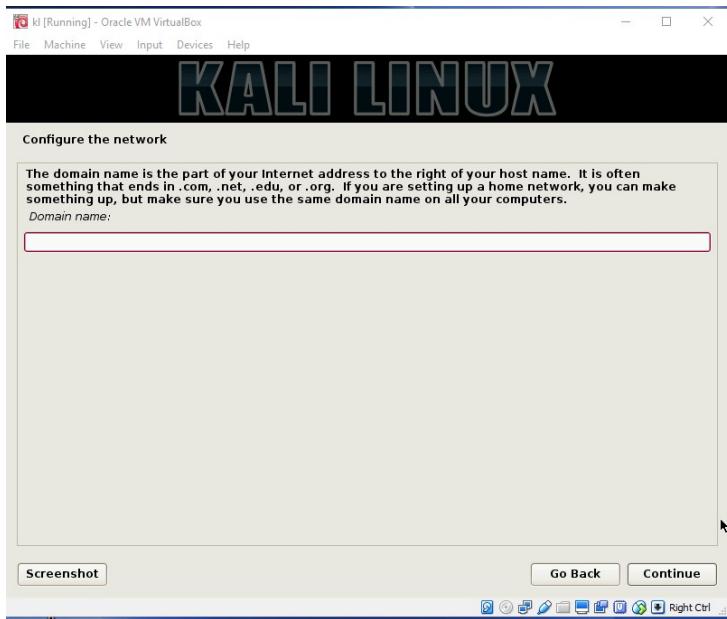
Select American English if you are using QWERTY keyboard select others if you use any other and Click continue



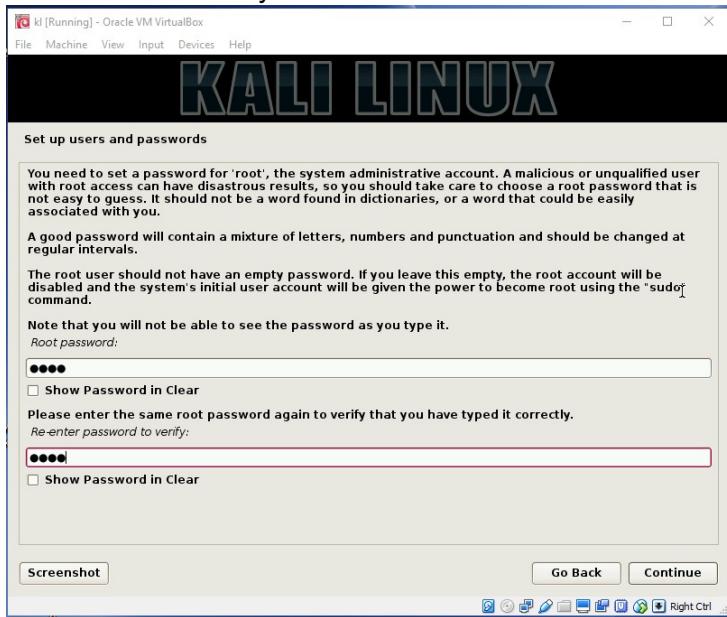
Enter the Host name you want and press enter, try to leave as it is if you don't know.



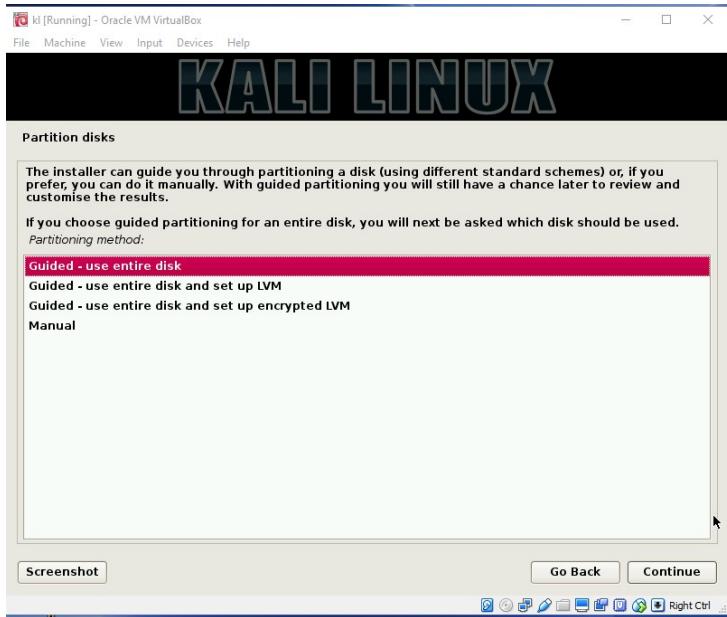
Leave the Domain name blank and Click on Continue



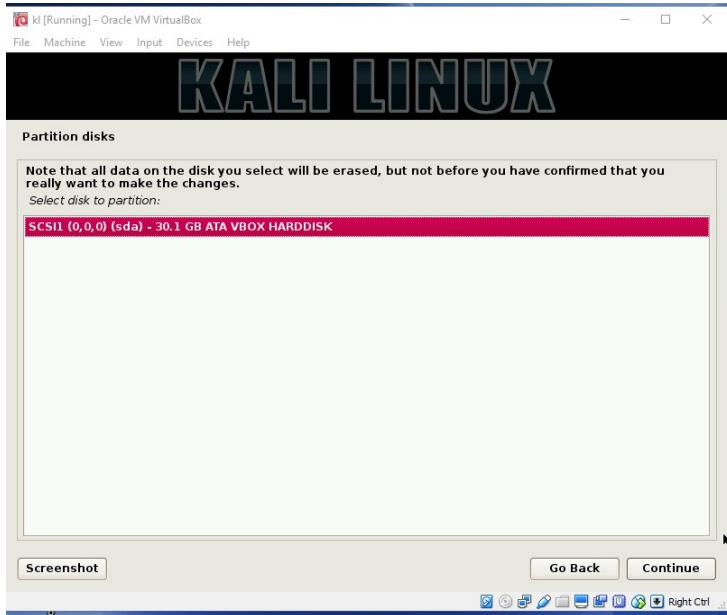
Enter the Password you want to use two times and click on continue (you can change later)



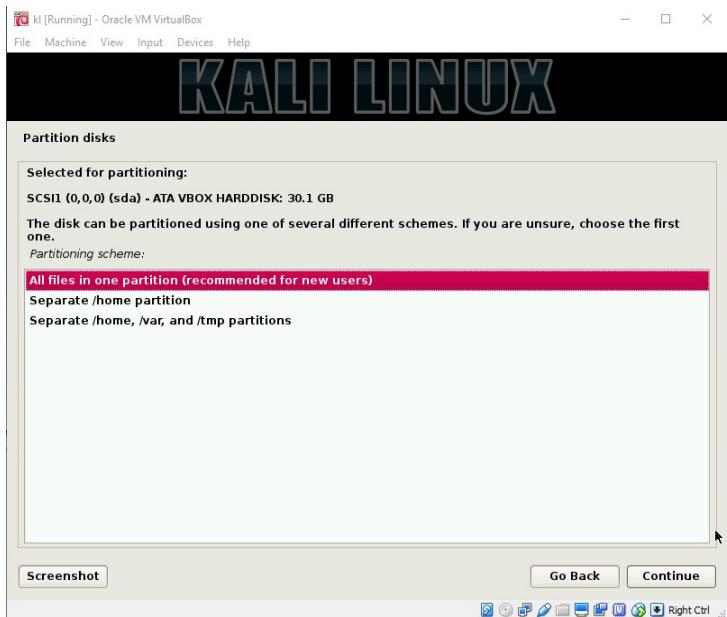
Select Guided-use Entire disk and Click on Continue



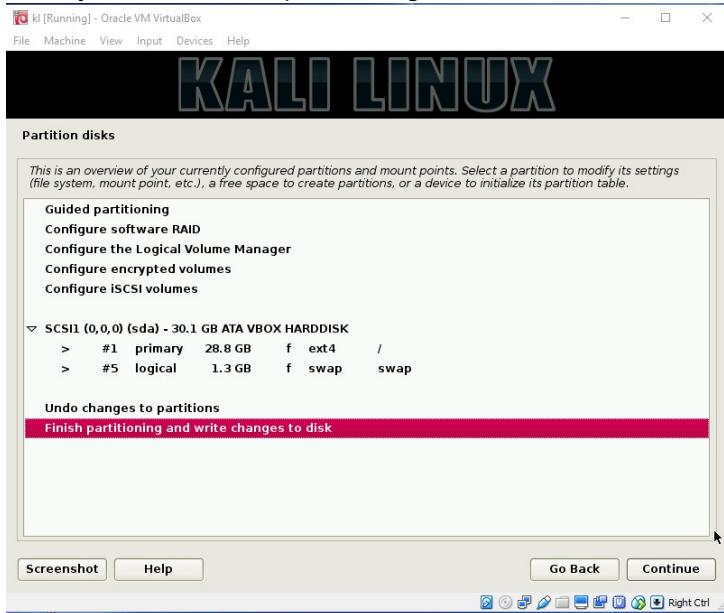
Select the Hard disk available there and Click On Continue.



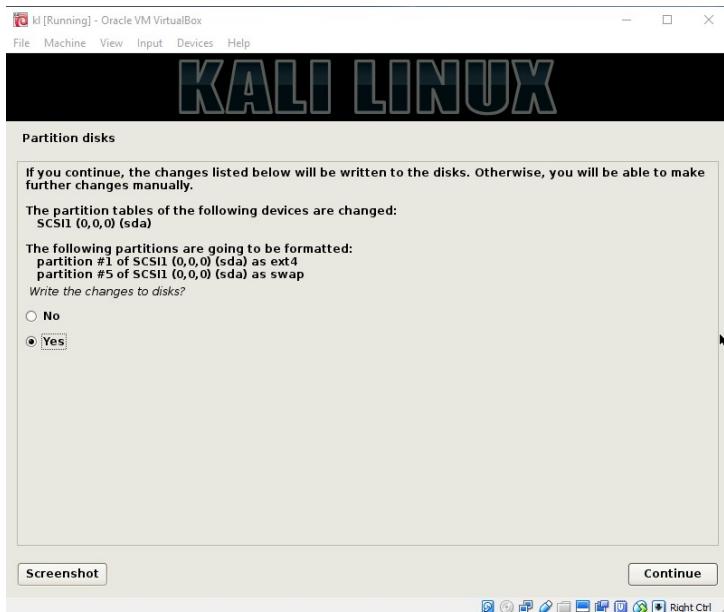
Select the First Option All Files in one partition and Click on continue.



Then you select finish partitioning and click Continue

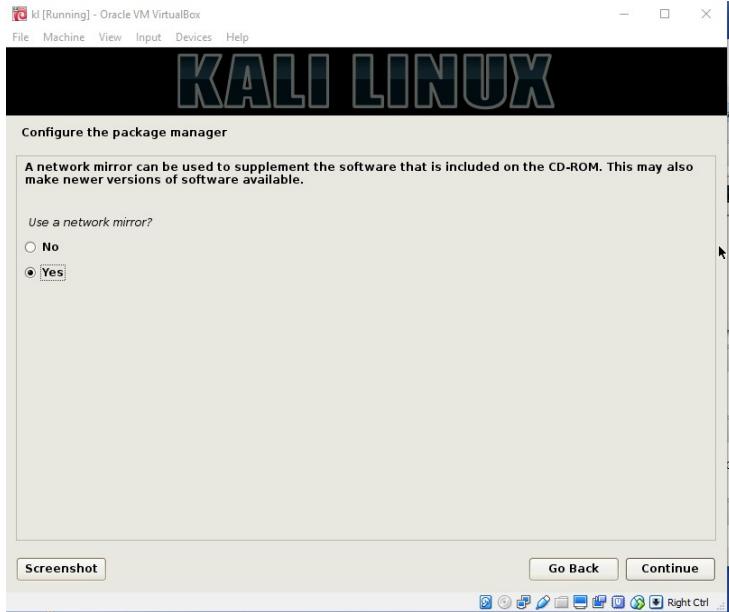


Select yes when prompting and continue.

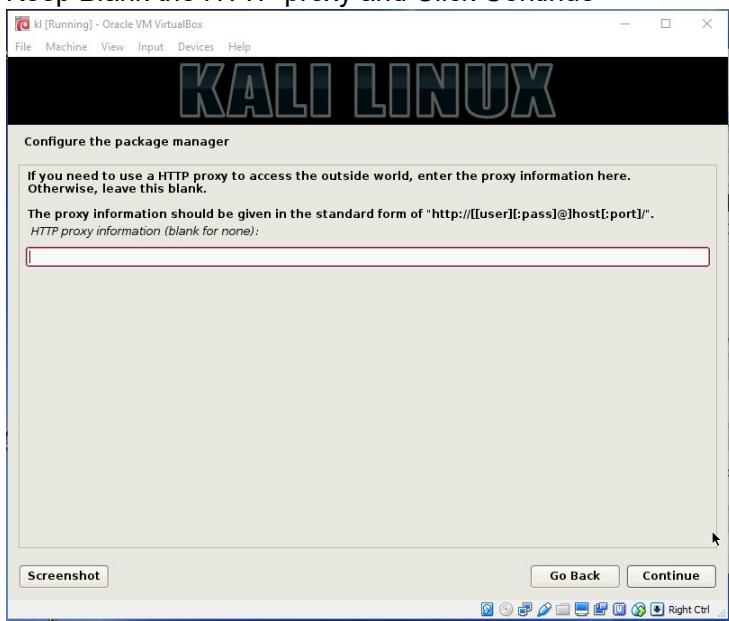


Wait till the process of copy completes.

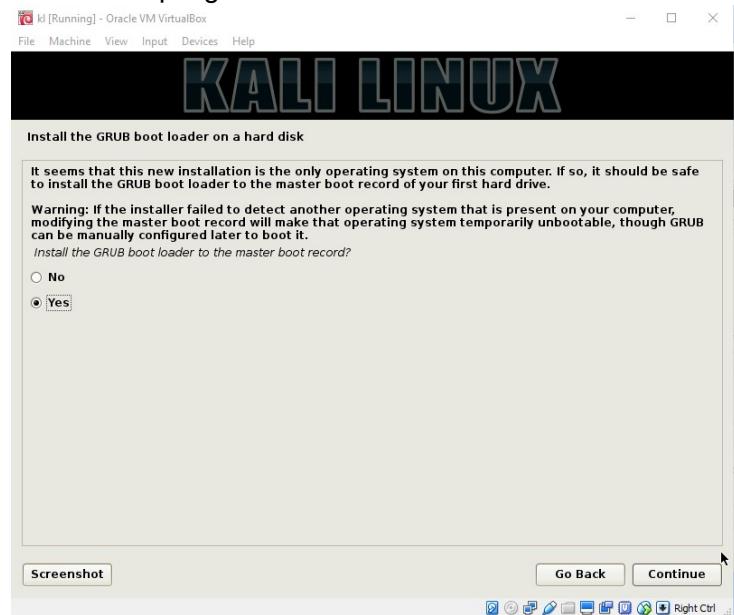
When prompting for Network mirror make sure you have working internet connection and Select YES and Continue



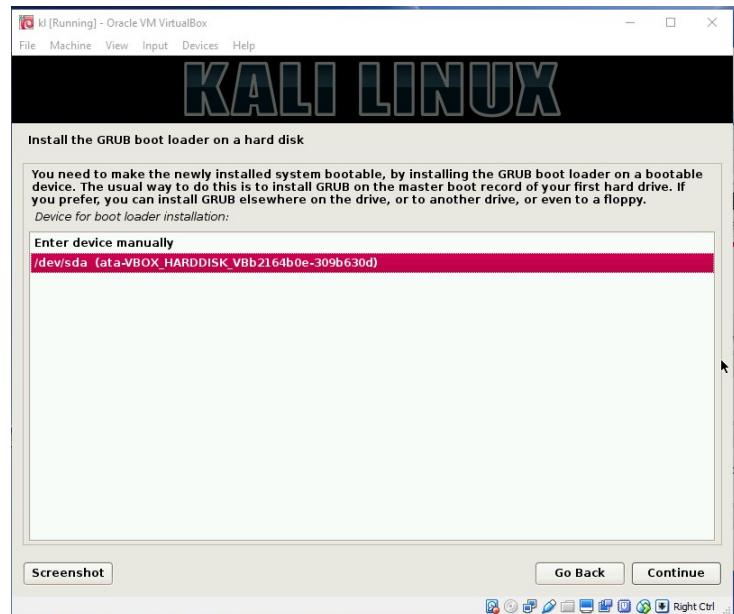
Keep Blank the HTTP proxy and Click Continue



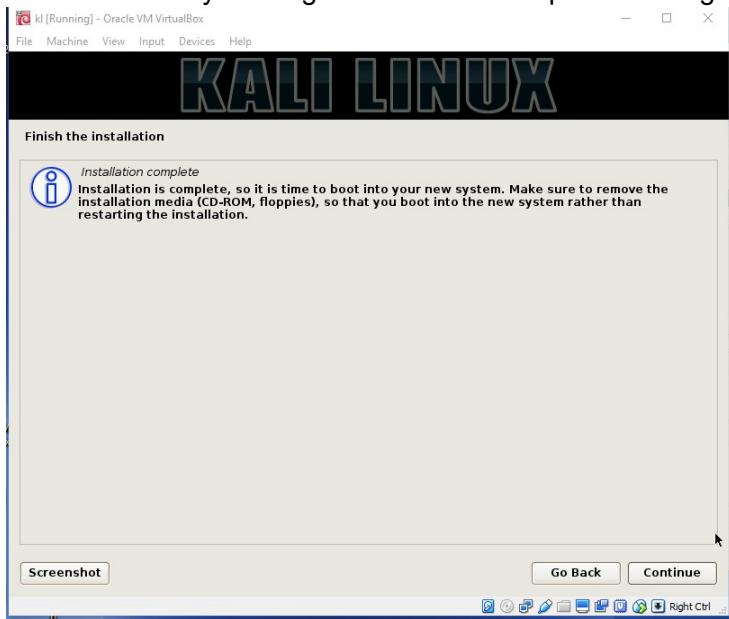
When Prompting for Grub Boot loader Select Yes and Click Continue



Select the Device from the list and Click Continue



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



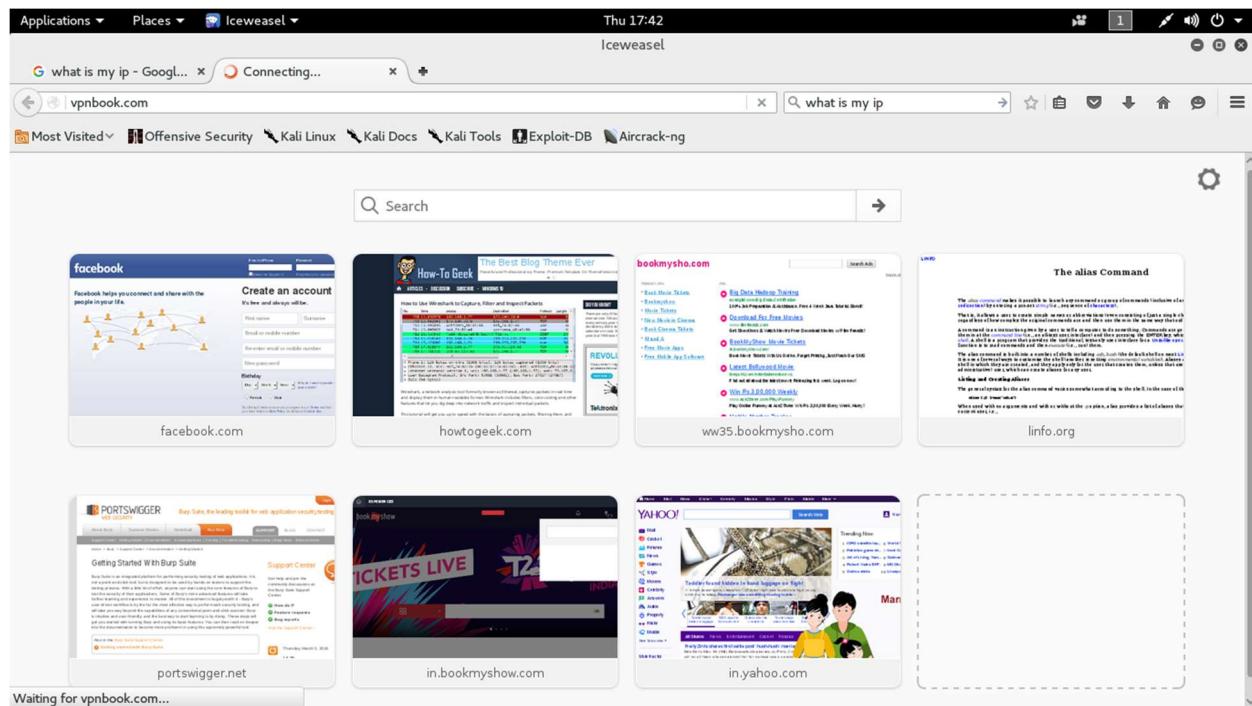
Practical No 2: IP address spoofing in kali Linux.

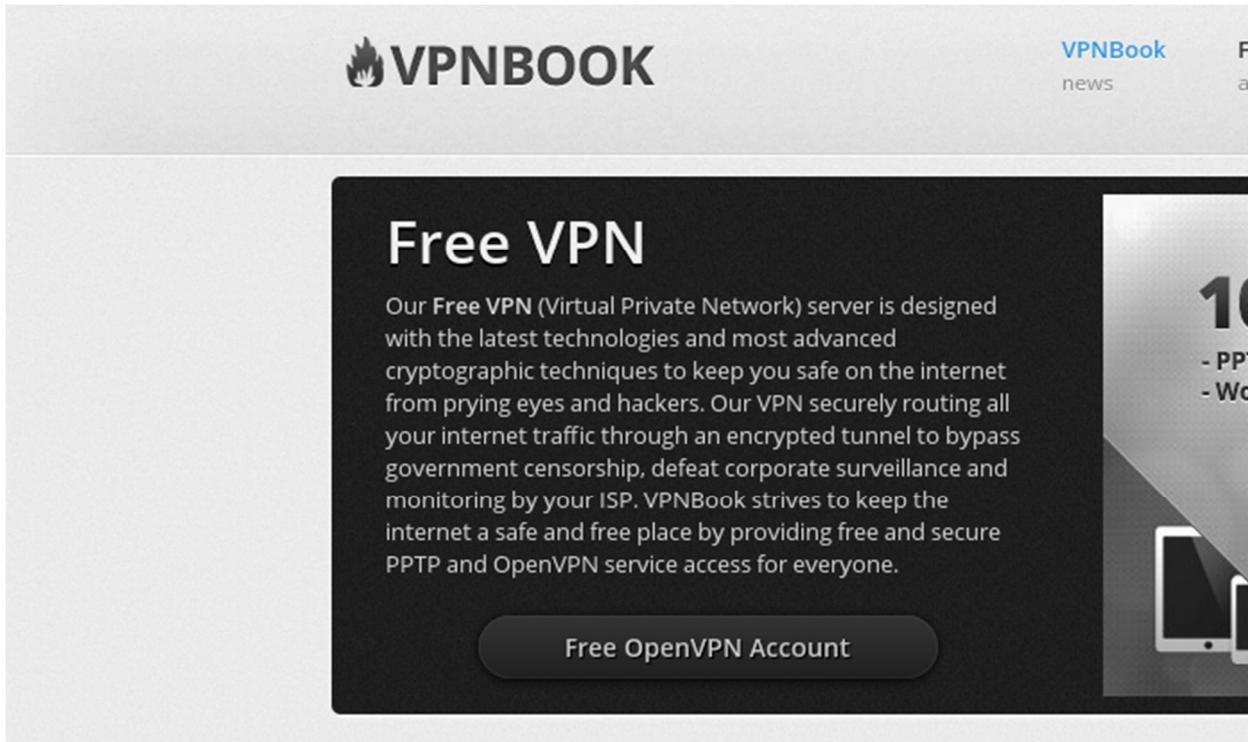
Requirements:

Good internet connection

Kali Linux installed (either host or guest)

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



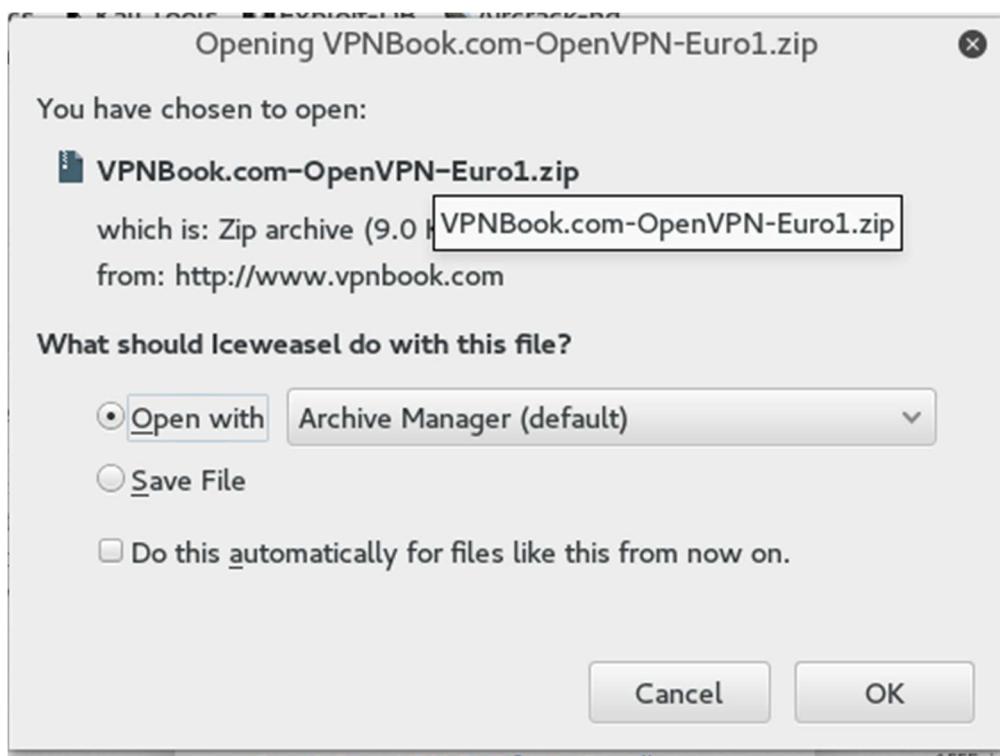


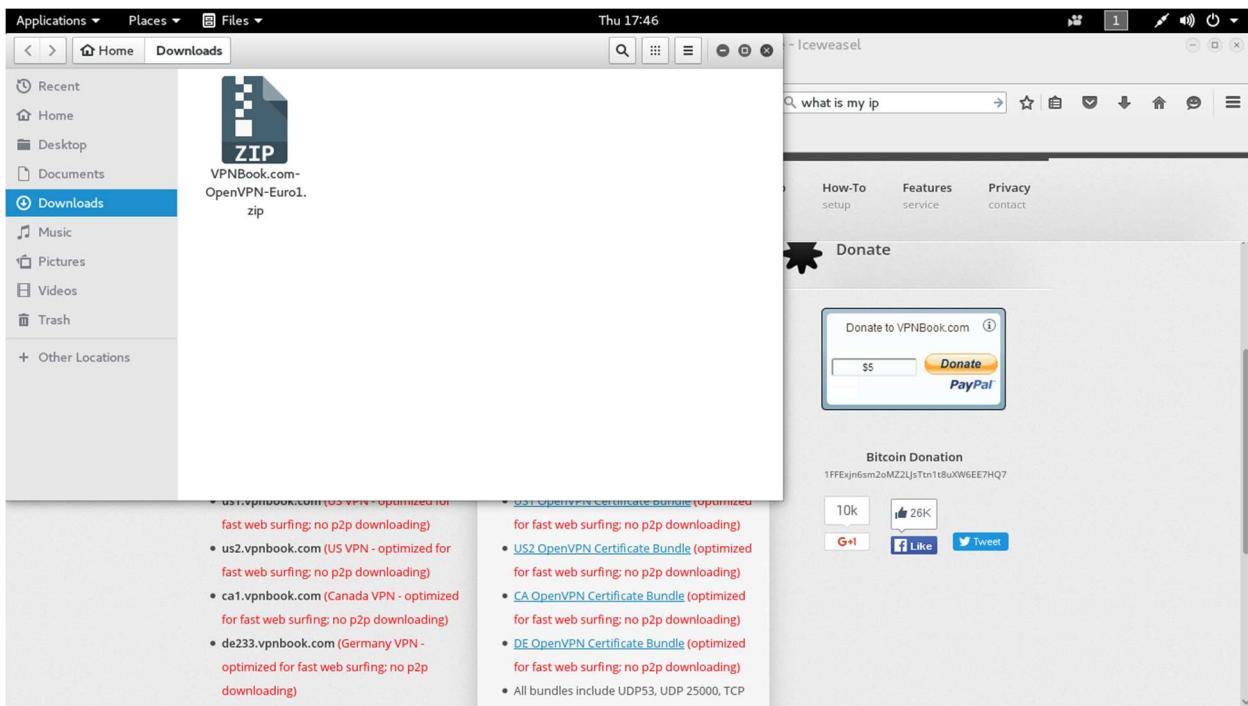
On the next screen under free openvpn account credentials will be there just note down them in a separate place.

This screenshot shows the "Free VPN" section of the VPNBook website. The top navigation bar includes links for "VPNBook news", "Free VPN accounts", "Free Web proxy", "How-To setup", "Features service", and "Privacy contact". The main content area has a heading "Free VPN" and sub-sections for "PPTP and OpenVPN Accounts". It lists two options: "The Okeanos Aggressor II" (Free PPTP VPN, \$0/mo) and "Free OpenVPN (Recommended)" (Free OpenVPN, \$0/mo). Below these, there's a brief description of OpenVPN and links to download certificate bundles. To the right, there's a "Donate" section with a PayPal button and a Bitcoin donation address: 1FFEjn6sm2oMZZLjsTn1t8uXW6EE7HQ7. The footer contains social media links and a "100% Free PPTP and OpenVPN Service - Iceweasel" link.

The screenshot shows a Linux desktop environment with a window titled "Iceweasel". The browser is displaying the website www.vpnbook.com/freevpn. The main content of the page is a list of VPN server options, each with a link to download its configuration file. Below this list, there is a note about using TCP instead of UDP if UDP is blocked. To the right of the list, there is a "Bitcoin Donation" section with a QR code and social sharing links for Google+, Facebook, and Twitter. A call-to-action button at the bottom right of the page says "Choose an OpenVPN Server from above".

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

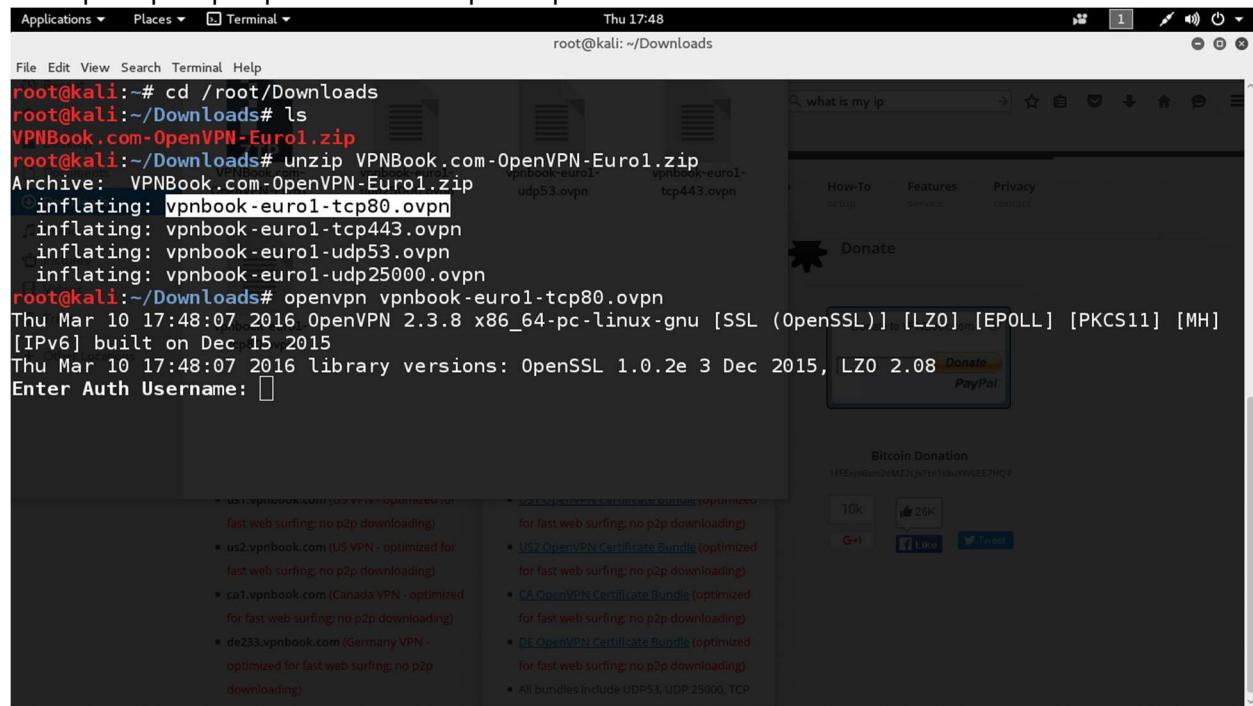
Syntax: unzip filename

```
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

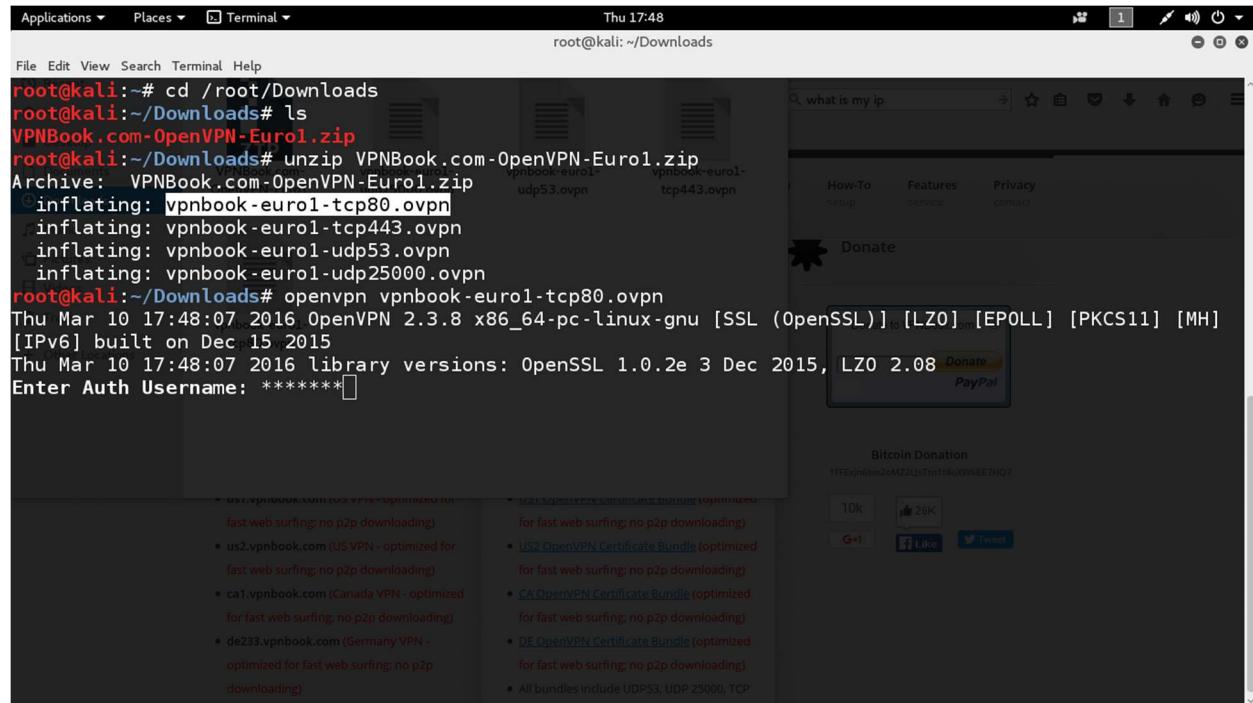
Syntax: openvpn <extracted file name>

Example: openvpn vpnbook-euro1-tcp80.ovpn



```
root@kali:~# cd /root/Downloads
root@kali:~/Downloads# ls
VPNBook.com-OpenVPN-Euro1.zip
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
root@kali:~/Downloads# openvpn vpnbook-euro1-tcp80.ovpn
Thu Mar 10 17:48:07 2016 OpenVPN 2.3.8 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH]
[IPv6] built on Dec 15 2015
Thu Mar 10 17:48:07 2016 library versions: OpenSSL 1.0.2e 3 Dec 2015, LZO 2.08
Enter Auth Username: 
```

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



```
root@kali:~# cd /root/Downloads
root@kali:~/Downloads# ls
VPNBook.com-OpenVPN-Euro1.zip
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
root@kali:~/Downloads# openvpn vpnbook-euro1-tcp80.ovpn
Thu Mar 10 17:48:07 2016 OpenVPN 2.3.8 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH]
[IPv6] built on Dec 15 2015
Thu Mar 10 17:48:07 2016 library versions: OpenSSL 1.0.2e 3 Dec 2015, LZO 2.08
Enter Auth Username: *****
```

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

```

root@kali:~# cd /root/Downloads
root@kali:~/Downloads# ls
VPNBook.com-OpenVPN-Euro1.zip
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
Thu Mar 10 17:48:07 2016 OpenVPN 2.3.8 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH]
[IPv6] built on Dec 15 2015
Thu Mar 10 17:48:07 2016 library versions: OpenSSL 1.0.2e 3 Dec 2015, LZO 2.08
Enter Auth Username: *****
Enter Auth Password: *****

  * Username: vpnbook
  * Password: takuPhu5
More servers coming. Please Donate.

Choose an OpenVPN Server from above

```

After that hit enter it will do some processing.

```

inflating: vpnbook-euro1-tcp80.ovpn
inflating: vpnbook-euro1-tcp443.ovpn
inflating: vpnbook-euro1-udp53.ovpn
inflating: vpnbook-euro1-udp25000.ovpn
root@kali:~/Downloads# openvpn vpnbook-euro1-tcp80.ovpn
Thu Mar 10 17:48:07 2016 OpenVPN 2.3.8 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH]
[IPv6] built on Dec 15 2015
Thu Mar 10 17:48:07 2016 library versions: OpenSSL 1.0.2e 3 Dec 2015, LZO 2.08
Enter Auth Username: *****
Enter Auth Password: *****

Thu Mar 10 17:48:33 2016 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
Thu Mar 10 17:48:33 2016 NOTE: fast-io is disabled since we are not using UDP
Thu Mar 10 17:48:33 2016 Socket Buffers: R=[87380->131072] S=[16384->131072]
Thu Mar 10 17:48:33 2016 Attempting to establish TCP connection with [AF_INET]176.126.237.217:80 [nonblock]
  * Username: vpnbook
Thu Mar 10 17:48:34 2016 TCP connection established with [AF_INET]176.126.237.217:80
Thu Mar 10 17:48:34 2016 TCPv4_CLIENT link local: [undef]
Thu Mar 10 17:48:34 2016 TCPv4_CLIENT link remote: [AF_INET]176.126.237.217:80
Thu Mar 10 17:48:34 2016 TLS: Initial packet from [AF_INET]176.126.237.217:80, sid=bc0b3ef9 83cfcc7dd
Thu Mar 10 17:48:34 2016 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Thu Mar 10 17:48:37 2016 VERIFY OK: depth=1, C=CH, ST=Zurich, L=Zurich, O=vpnbook.com, OU=IT, CN=vpnbook.com, name=vpnbook.com, emailAddress=admin@vpnbook.com with
Thu Mar 10 17:48:37 2016 VERIFY OK: depth=0, C=CH, ST=Zurich, L=Zurich, O=vpnbook.com, OU=IT, CN=vpnbook.com, name=vpnbook.com, emailAddress=admin@vpnbook.com

```

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.

Applications ▾ Places ▾ Terminal ▾

Thu 17:48
root@kali: ~/Downloads

```

Thu Mar 10 17:48:39 2016 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Thu Mar 10 17:48:39 2016 Data Channel Decrypt: Cipher 'AES-128-CBC' initialized with 128 bit key
Thu Mar 10 17:48:39 2016 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Thu Mar 10 17:48:39 2016 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Thu Mar 10 17:48:39 2016 [vpnbook.com] Peer Connection Initiated with [AF_INET]176.126.237.217:80
Thu Mar 10 17:48:41 2016 SENT CONTROL [vpnbook.com]: 'PUSH_REQUEST' (status=1)
Thu Mar 10 17:48:41 2016 PUSH: Received control message: 'PUSH_REPLY, redirect-gateway def1,dhcp-option DNS 89.233.43.71,dhcp-option DNS 91.239.100.100,route 10.12.0.1,topology net30,ping 5,ping-restart 30 ,ifconfig 10.12.0.22 10.12.0.21' * CA OpenVPN Certificate Bundle (optimized)
Thu Mar 10 17:48:41 2016 OPTIONS IMPORT: timers and/or timeouts modified
Thu Mar 10 17:48:41 2016 OPTIONS IMPORT: --ifconfig/up options modified
Thu Mar 10 17:48:41 2016 OPTIONS IMPORT: route options modified
Thu Mar 10 17:48:41 2016 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Thu Mar 10 17:48:41 2016 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=eth0 HWADDR=00:e0:4c:5a:d2:01
Thu Mar 10 17:48:41 2016 TUN/TAP device tun3 opened
Thu Mar 10 17:48:41 2016 TUN/TAP TX queue length set to 100
Thu Mar 10 17:48:41 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Thu Mar 10 17:48:41 2016 /sbin/ip link set dev tun3 up mtu 1500
Thu Mar 10 17:48:41 2016 /sbin/ip addr add dev tun3 local 10.12.0.22 peer 10.12.0.21
Thu Mar 10 17:48:44 2016 /sbin/ip route add 176.126.237.217/32 via 192.168.0.1
Thu Mar 10 17:48:44 2016 /sbin/ip route add 0.0.0.0/1 via 10.12.0.21
Thu Mar 10 17:48:44 2016 /sbin/ip route add 128.0.0.0/1 via 10.12.0.21
Thu Mar 10 17:48:44 2016 /sbin/ip route add 10.12.0.1/32 via 10.12.0.21
Thu Mar 10 17:48:44 2016 Initialization Sequence Completed

```

```

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) local 10.12.0.22 peer 10.12.0.21
    RX errors 0 dropped 0 overruns 0 frame 0/32 via 192.168.0.1
    TX packets 215 bytes 19611 (19.1 KiB) via 10.12.0.21
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Thu Mar 10 17:48:44 2016 /sbin/ip route add 10.12.0.1/32 via 10.12.0.21

```

Applications ▾ Places ▾ Iceweasel ▾

Thu 17:49

what is my ip - Google Search - Iceweasel

G what is my ip - Google... x 🔍 Free VPN Accounts * ... x G what is my ip - Google... x +

https://www.google.co.in/search?q=what+is+my+ip&ie=utf-8&oe=utf-8&qws_rd=cr&ei=N2bhVprTNlvHuAS

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Google what is my ip

All Apps News Videos Images More Search tools

About 27,20,00,000 results (0.27 seconds)

176.126.237.217

Your public IP address

[Learn more about IP addresses](#)

Feedback

[What Is My IP - The IP Address Experts - WhatIsMyIP.com](#) ⓘ
<https://www.whatismyip.com/> ⓘ
 Lookup, Trace, Locate, Change, Hide ANY IP Address.
 IP Address Lookup - Internet Speed Test - Blacklist Check - IP WHOIS Lookup

[What Is My IP Address? IP Address Tools and More](#) ⓘ
<https://whatismyipaddress.com/> ⓘ
 IP address lookup, location, proxy detection, email tracing, IP hiding tips, blacklist check, speed test, and forums. Find, get, and show my IP address.
 IP Lookup - How to Hide Your IP Address - Update your IP location - None Detected

[What is my IP address? - IP Location Finder - Geolocation](#) ⓘ
<https://www.iplocation.net/find-ip-address> ⓘ

Practical No 3: Spoofing IP address any operating system.

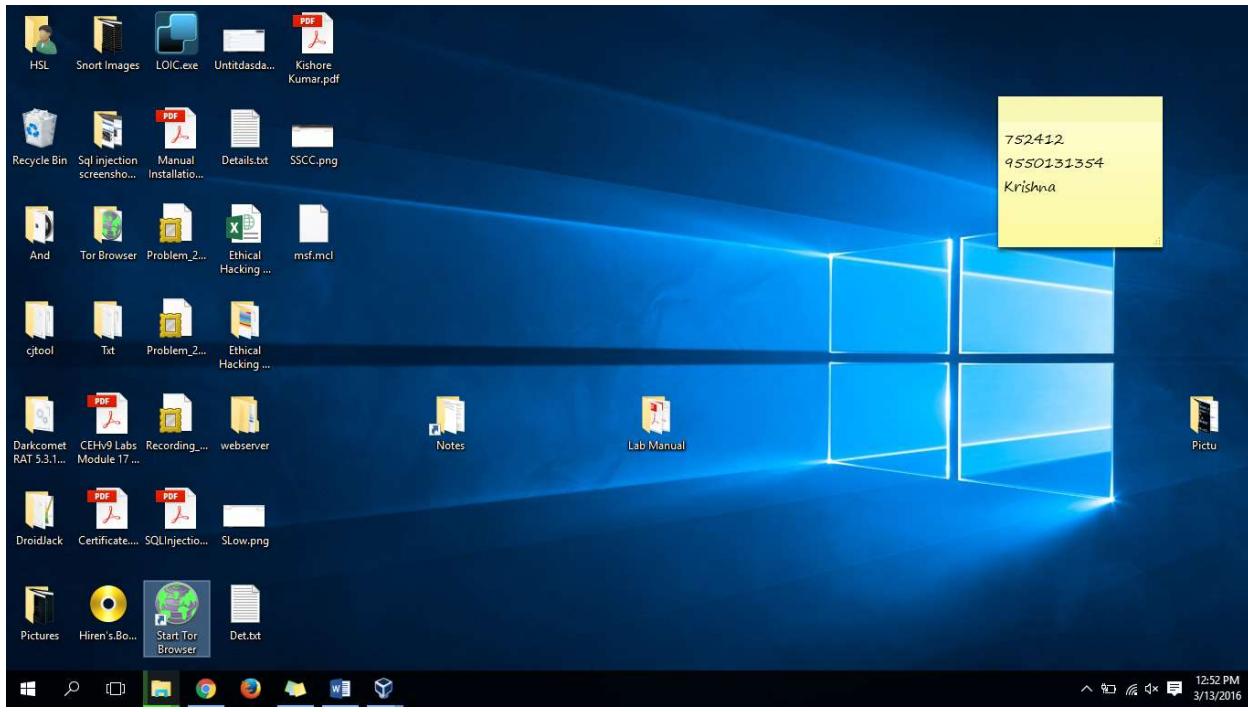
Step 1: Go to torproject.org and download the TOR browser

The screenshot shows the official Tor Project website at <https://www.torproject.org>. The main header features the 'Tor' logo. Below it, a large green banner with the heading 'Anonymity Online' and the subtext 'Protect your privacy. Defend yourself against network surveillance and traffic analysis.' A purple button labeled 'Download Tor' with a garlic icon is prominently displayed. To the right, there's a sidebar titled 'Recent Blog Posts' listing several entries from March 2016. The main content area includes sections for 'What is Tor?' and 'Why Anonymity Matters', along with a 'Get involved with Tor' link. At the bottom, a file download window for 'msf.mcl' is visible, showing the file path and a preview of the Microsoft Word document.

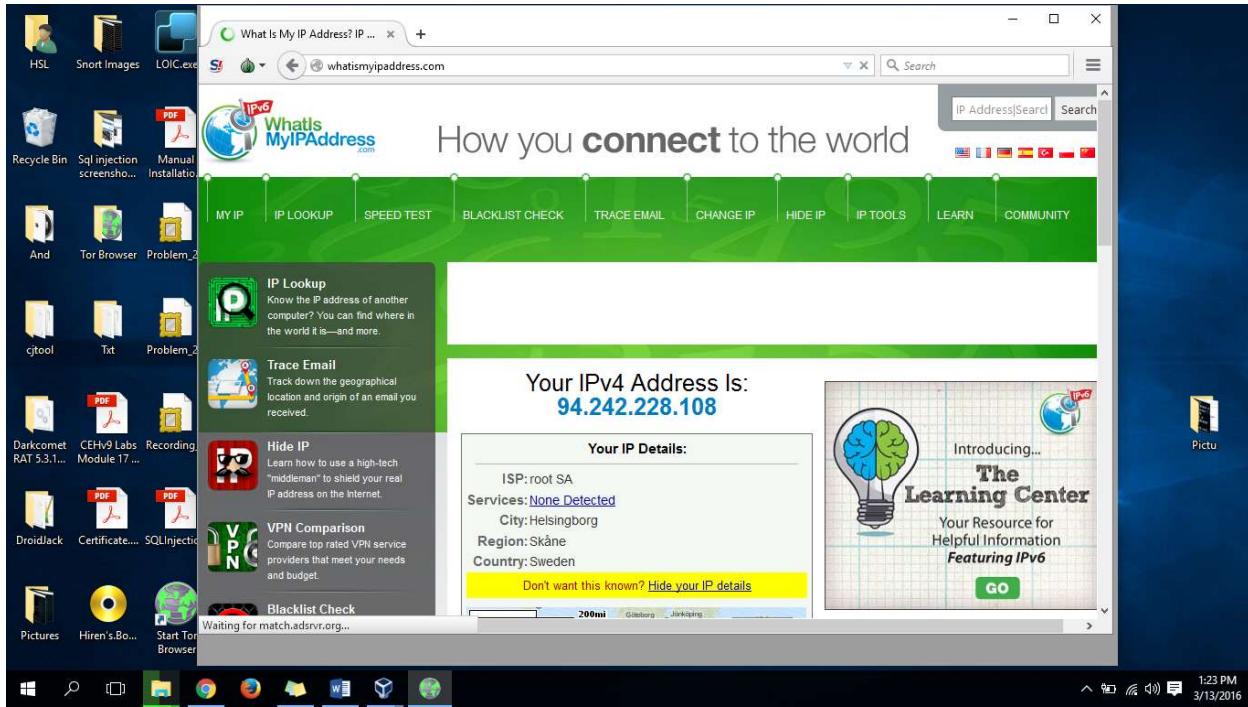
Step 2: After downloading run the Tor bundle to extract the browser package.

The screenshot shows a Microsoft Word document titled '001Introduction To Ethical Hacking.docx'. A security warning dialog box is open, asking if the user wants to run the file 'torbrowser-install-5.5.2_en-US.exe'. The dialog provides details about the file: Name: ...users\hs\Downloads\torbrowser-install-5.5.2_en-US.exe, Publisher: The Tor Project, Inc., Type: Application, From: C:\Users\hs\Downloads\torbrowser-install-5.5.2_en-US... It also includes a checkbox for 'Always ask before opening this file' and a note about potential risks. In the background, the Windows taskbar shows icons for various applications like File Explorer, Task View, and Start. A file explorer window is also visible, showing a list of files in the Downloads folder, including the downloaded Tor browser executable.

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

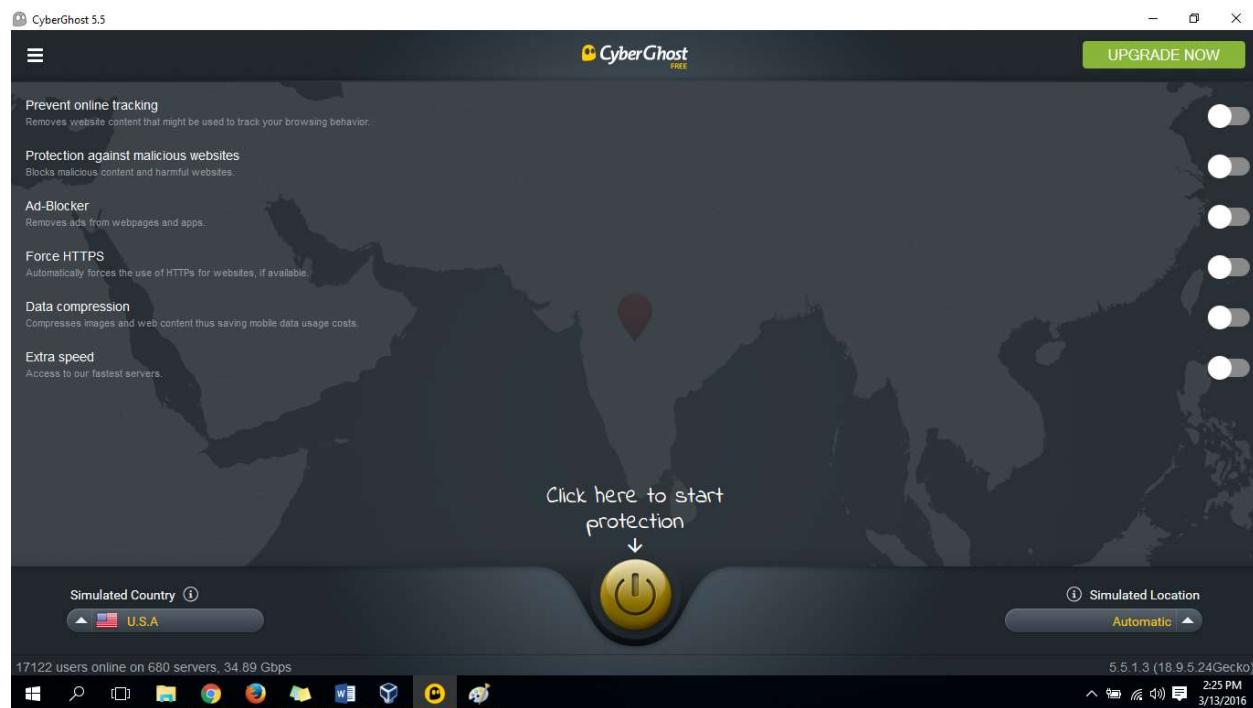
Step 1: Go to cyberghostvpn.com

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")

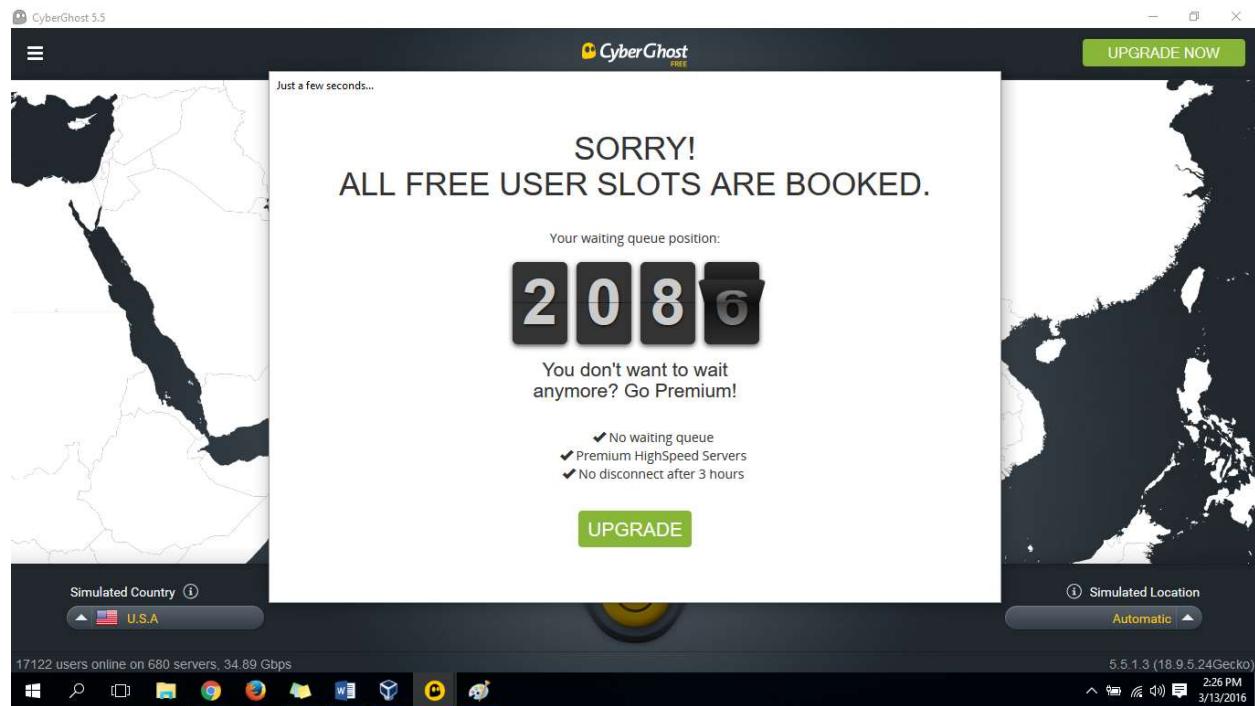
Step 3: after installing cyberghostvpn



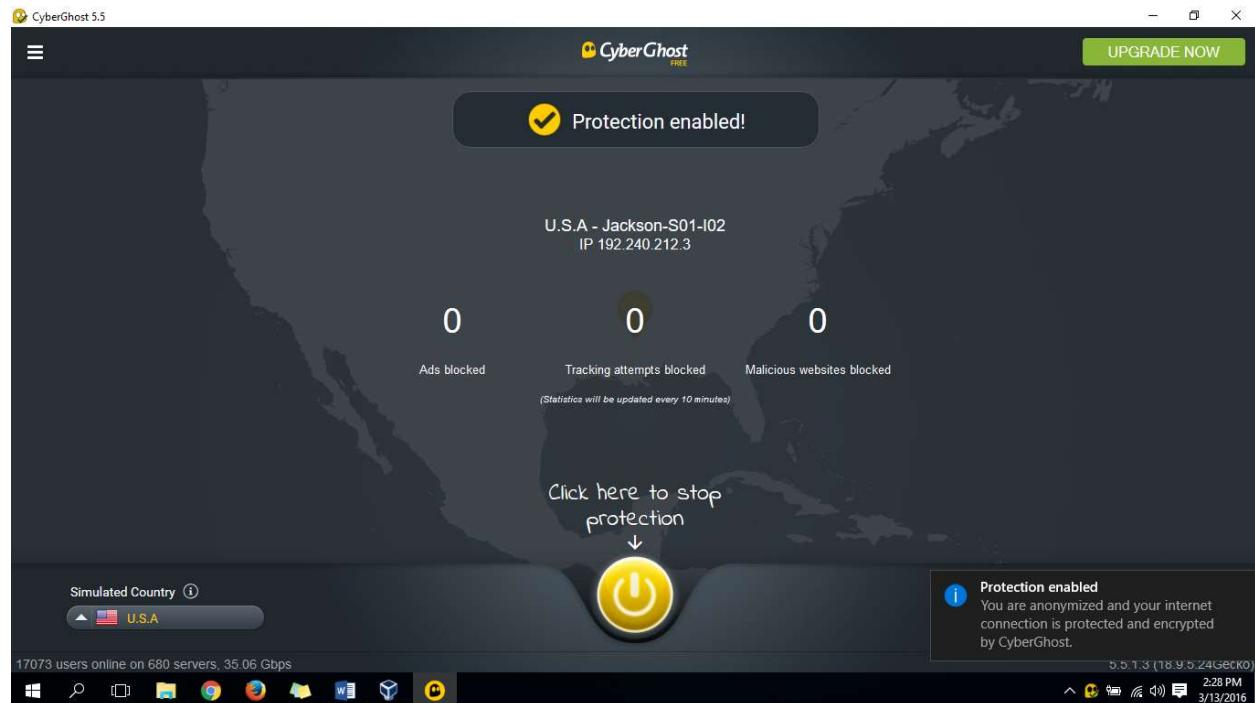
Just click on the power button on the interface to spoof your IP address completely.



This process will show some countdown numbers



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

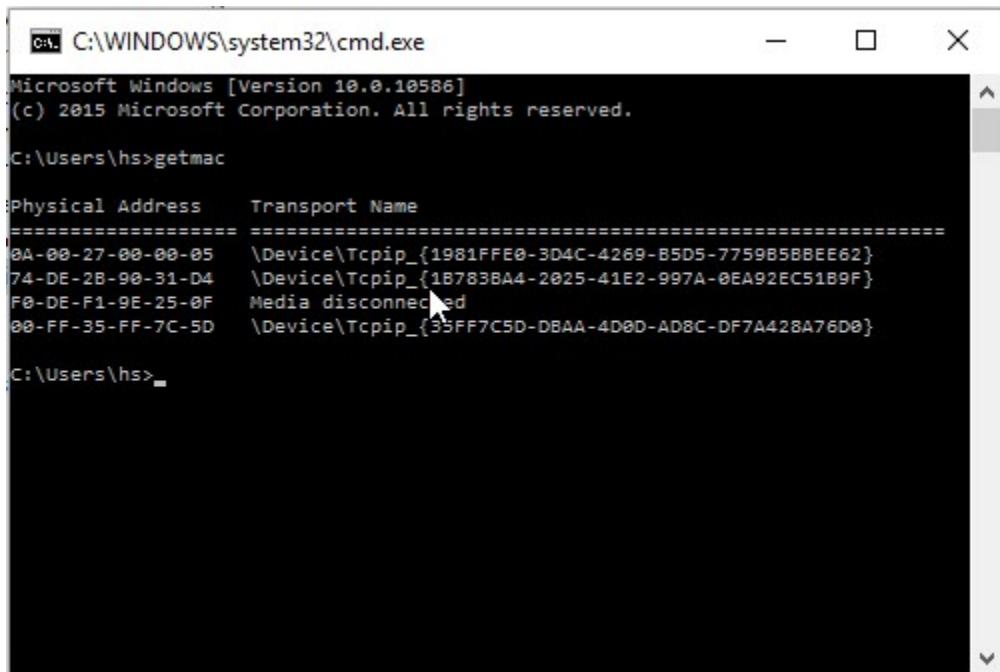


If you want you can select some other countries also and some other IPs also from the left and right menus.

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

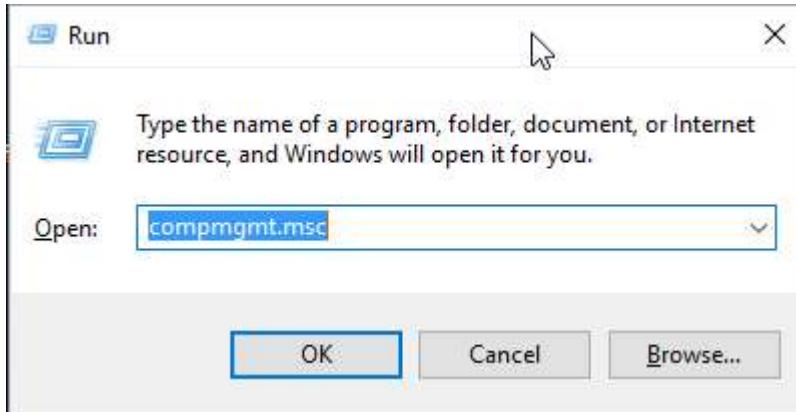
C:\Users\hs>getmac

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}

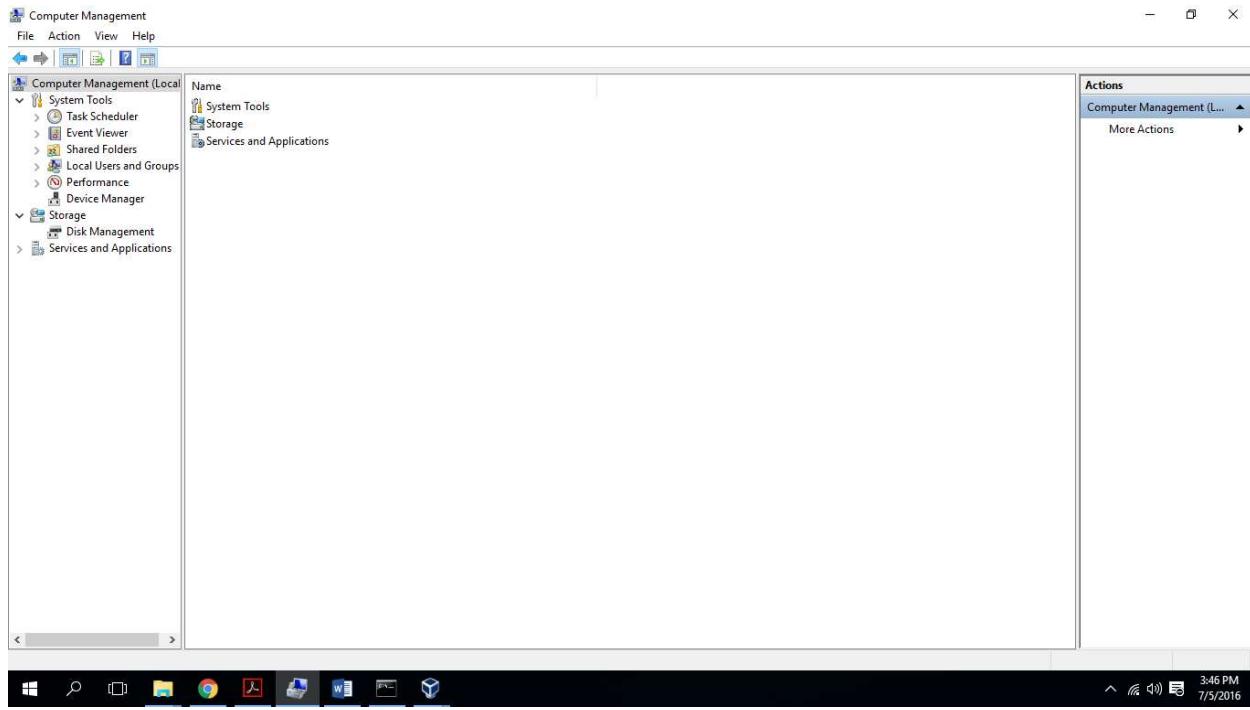
C:\Users\hs>
```

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.

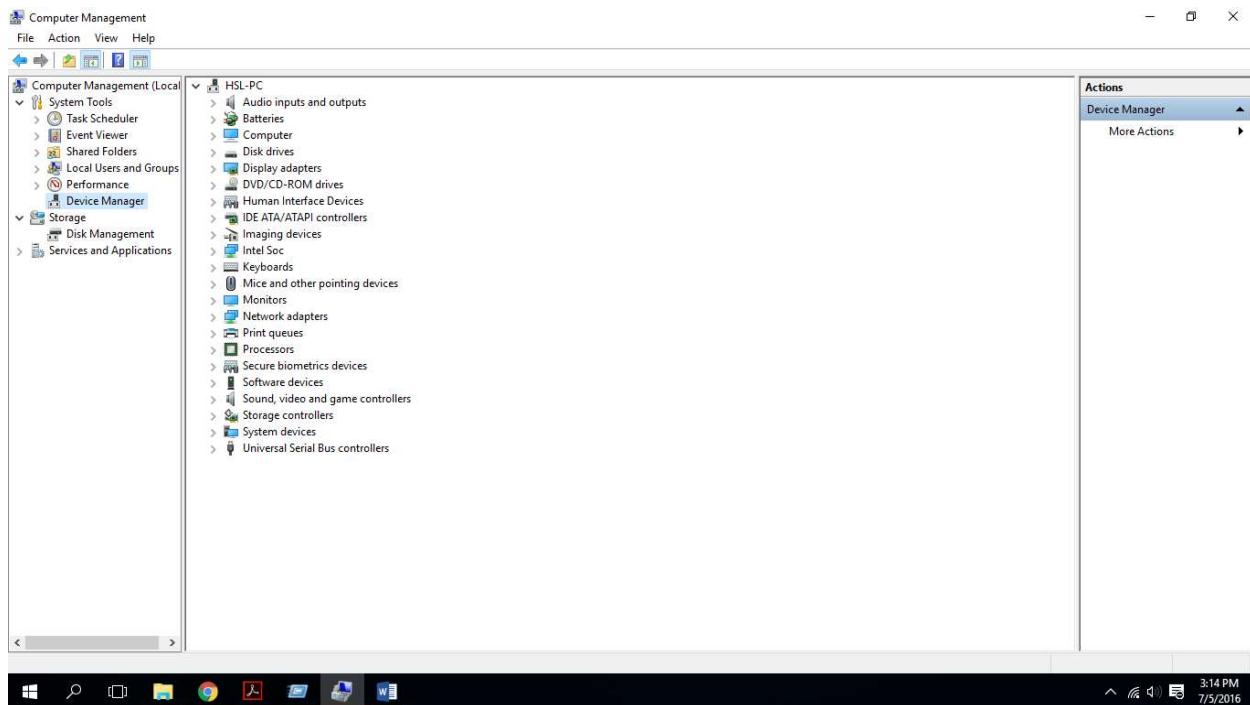
Then open computer management console by executing the below command in run dialog box.



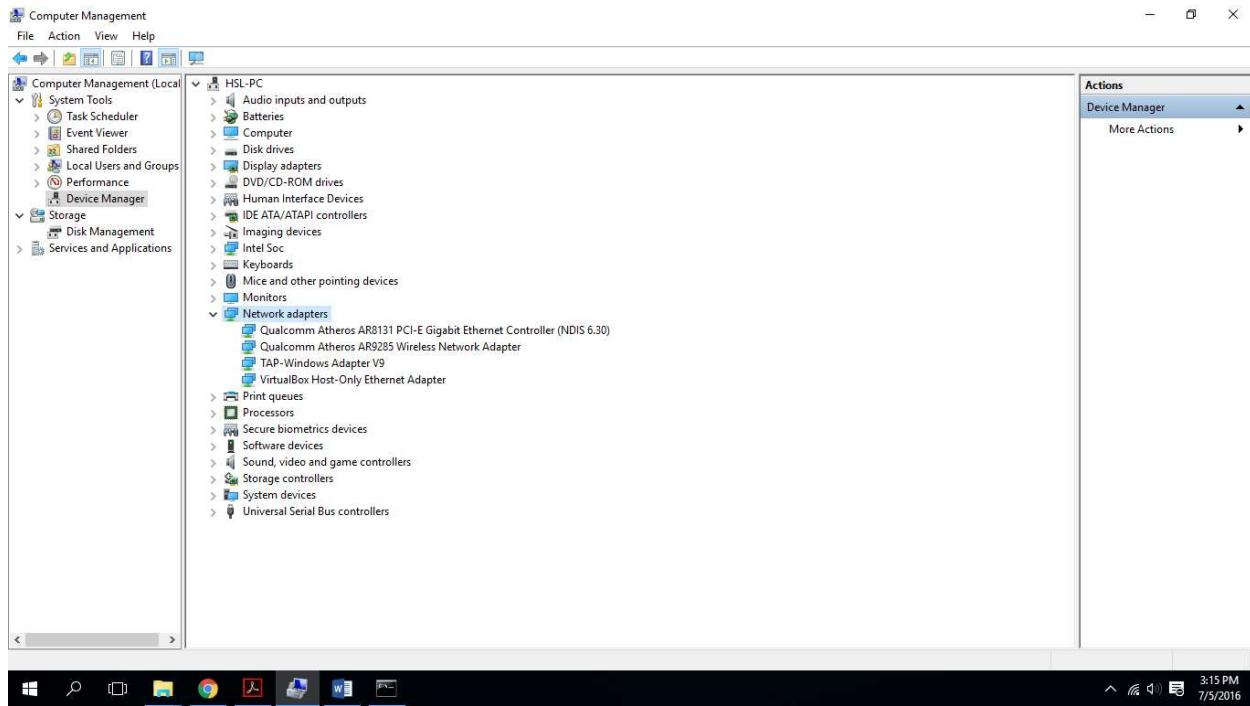
This is how the computer management windows will look like



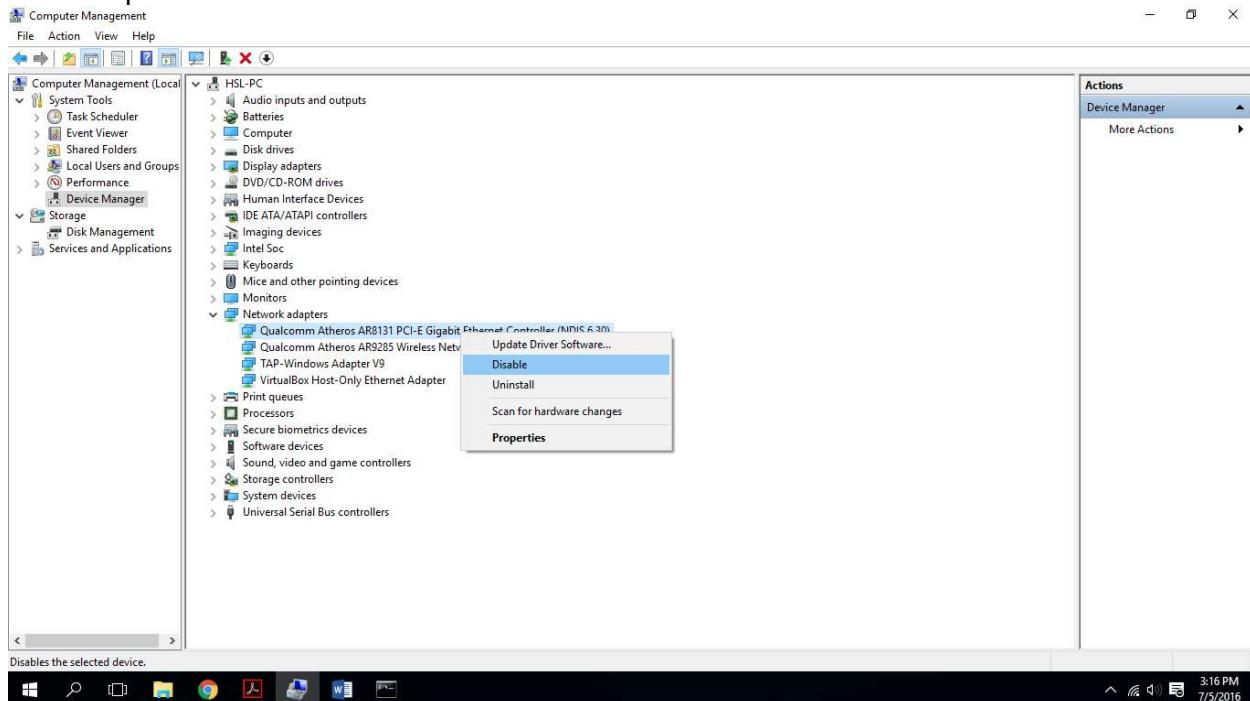
In this computer management window Please select device manager so that you can see right side a list of devices which you have in your machine



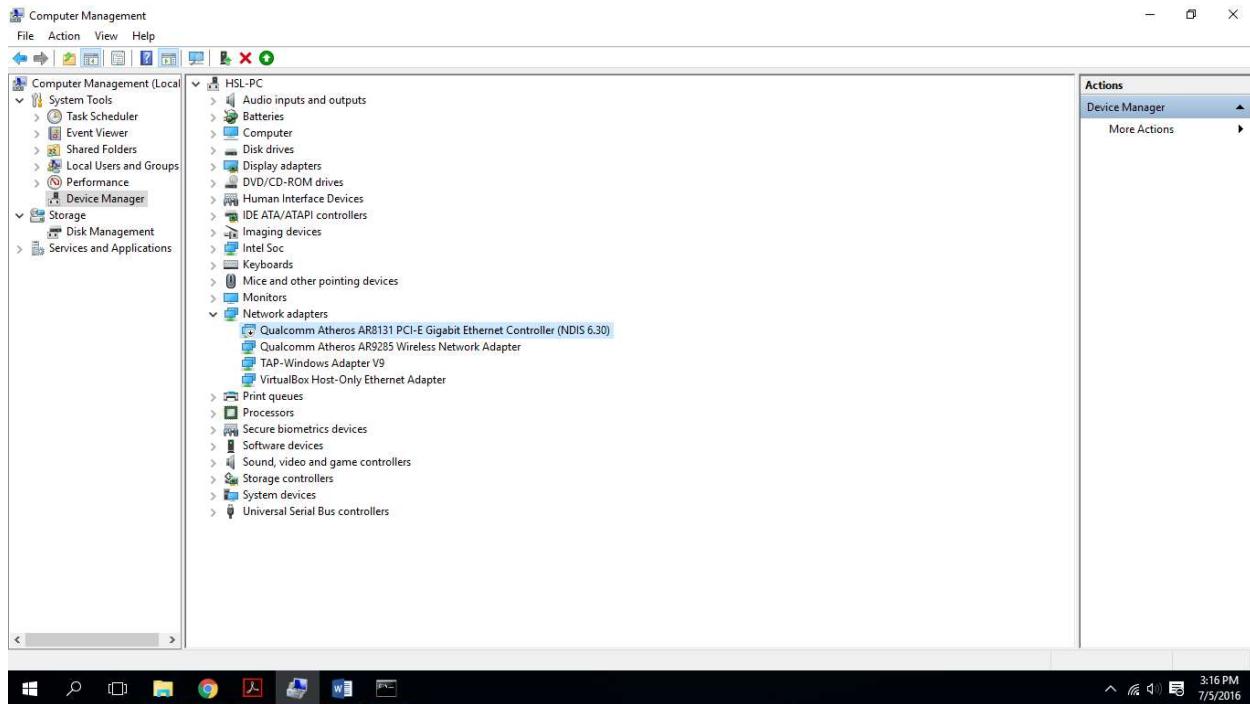
From the list you need to find out network adaptors section and expand the section so you can see whatever NIC cards you have in your machine will be listed out there



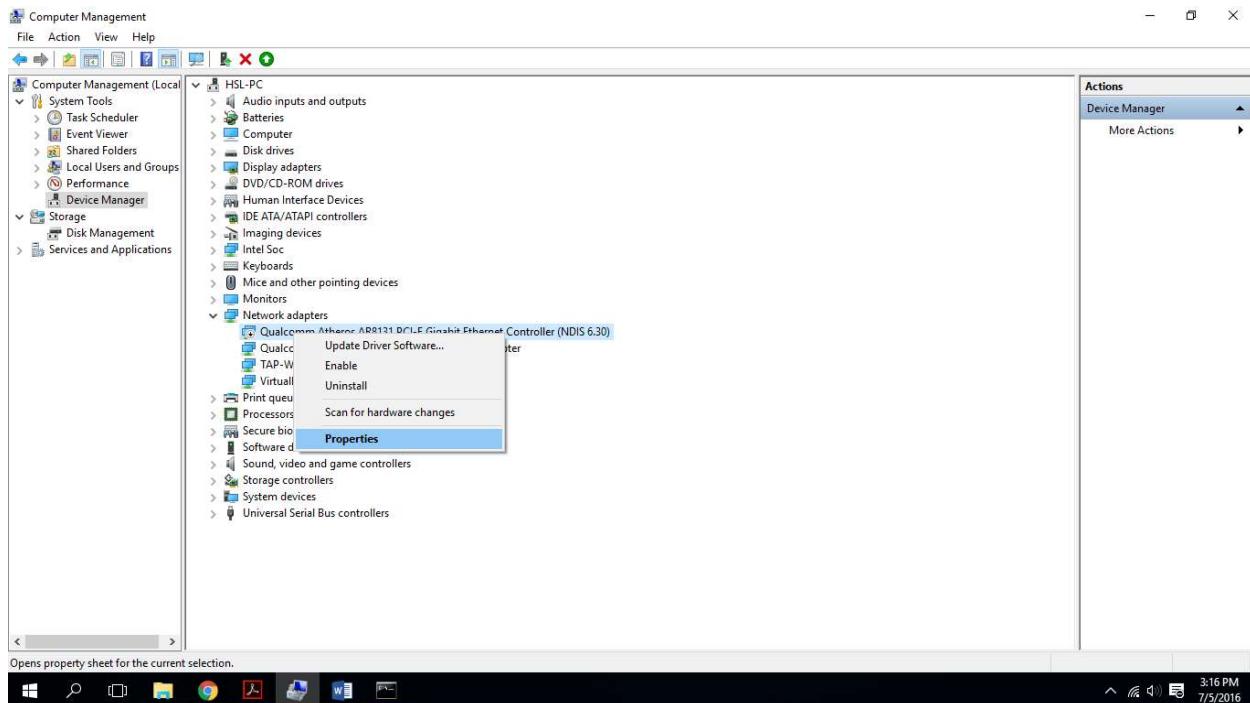
To spoof MAC address to spoof MAC address first you need to disable the NIC card to do that all you have to do is simply right click on it so you can see a Button called Disable select that disable option.



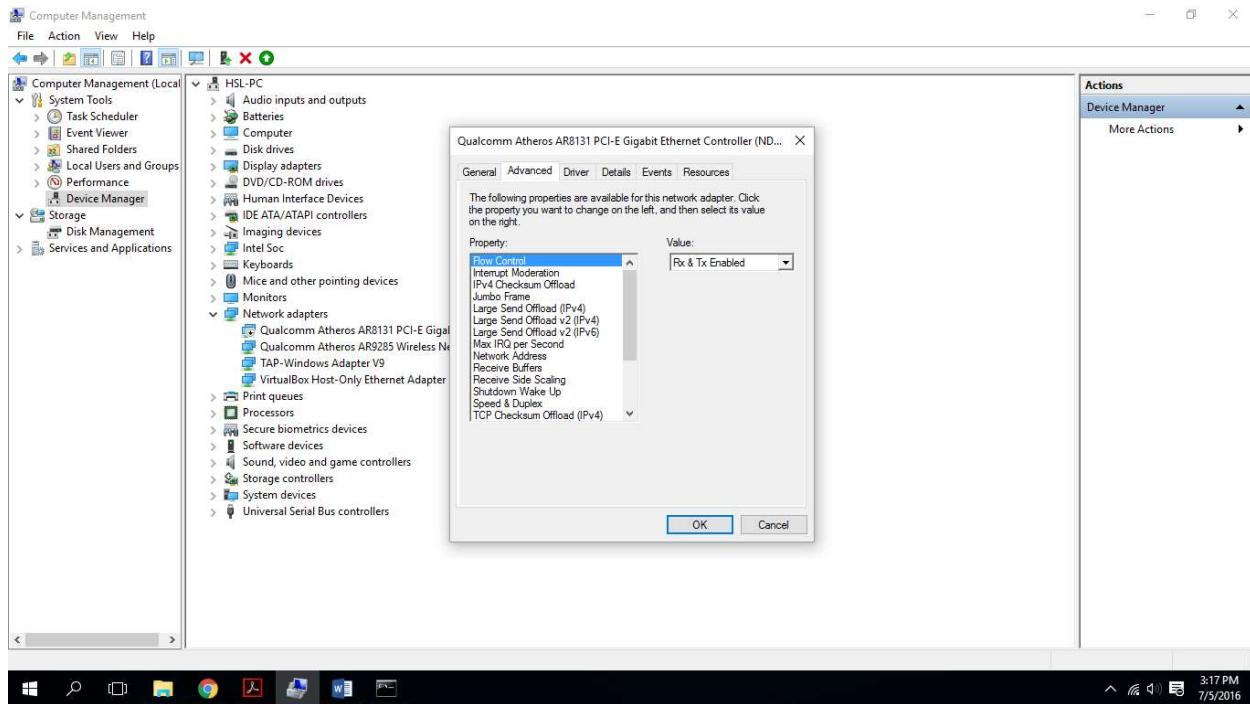
So that your NIC card will be disabled.



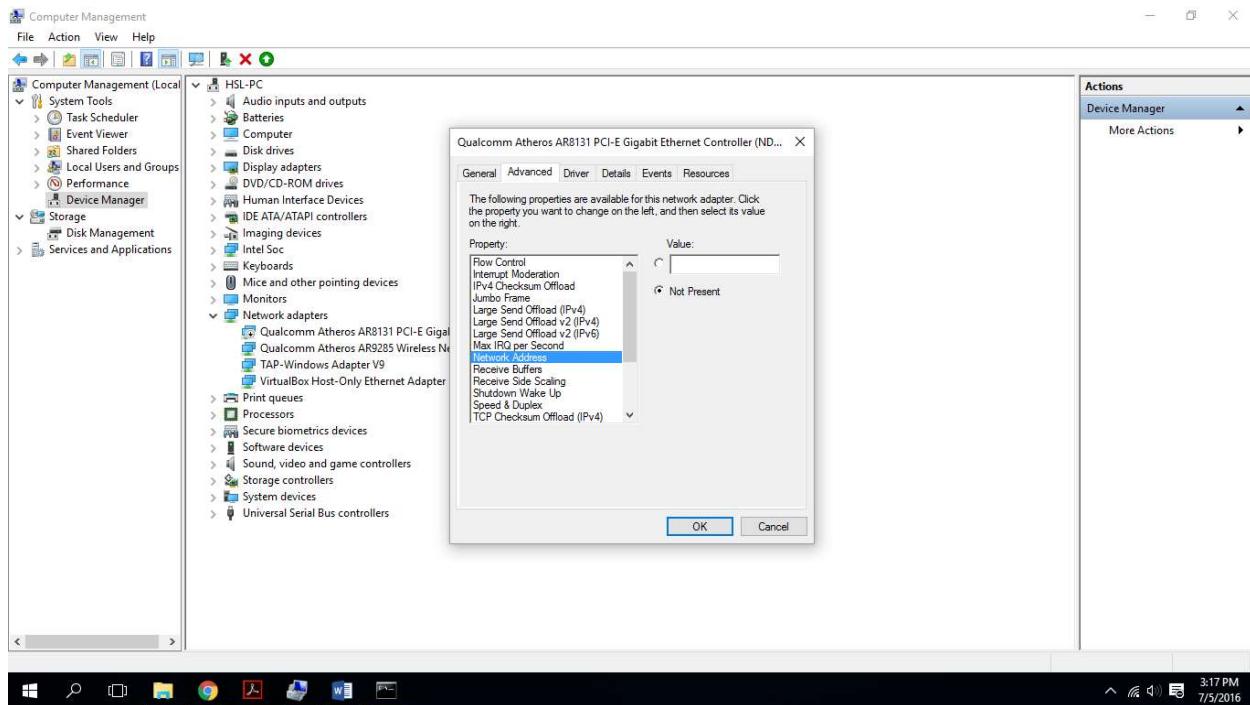
Once its disabled right click on the NIC card and select properties so that you can see a dialogue box



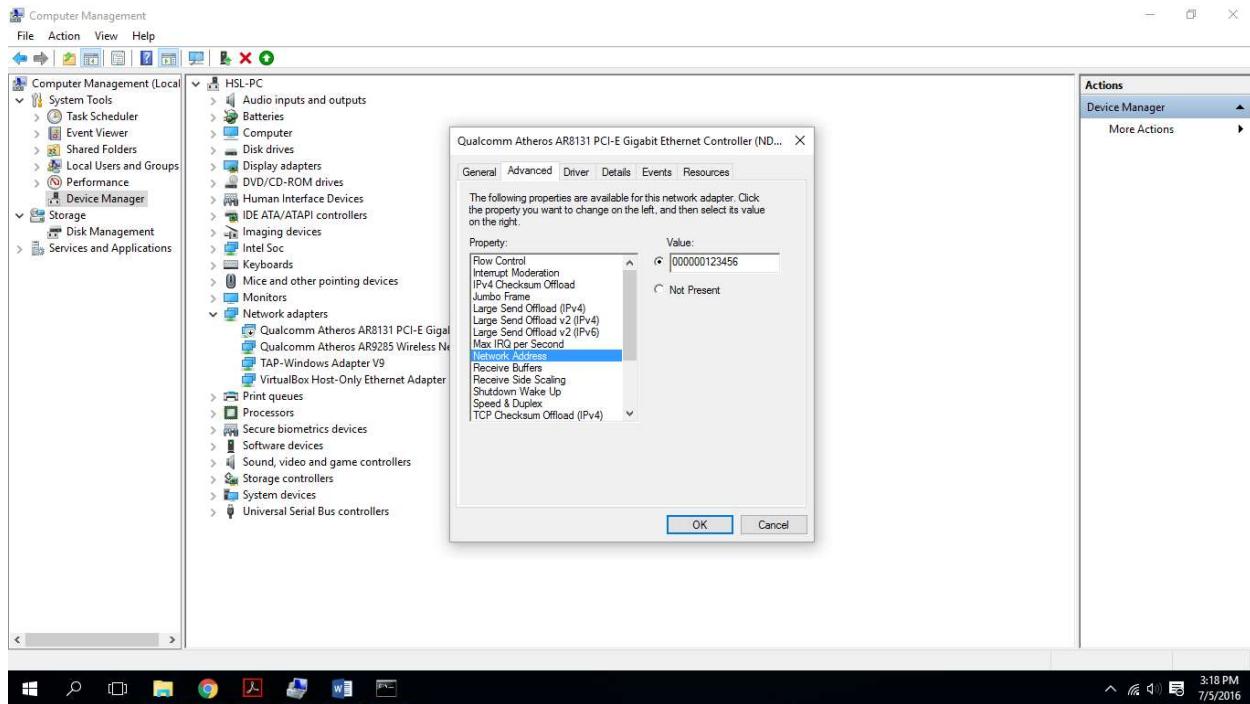
In that dialogue box go to advanced section in the advanced section



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

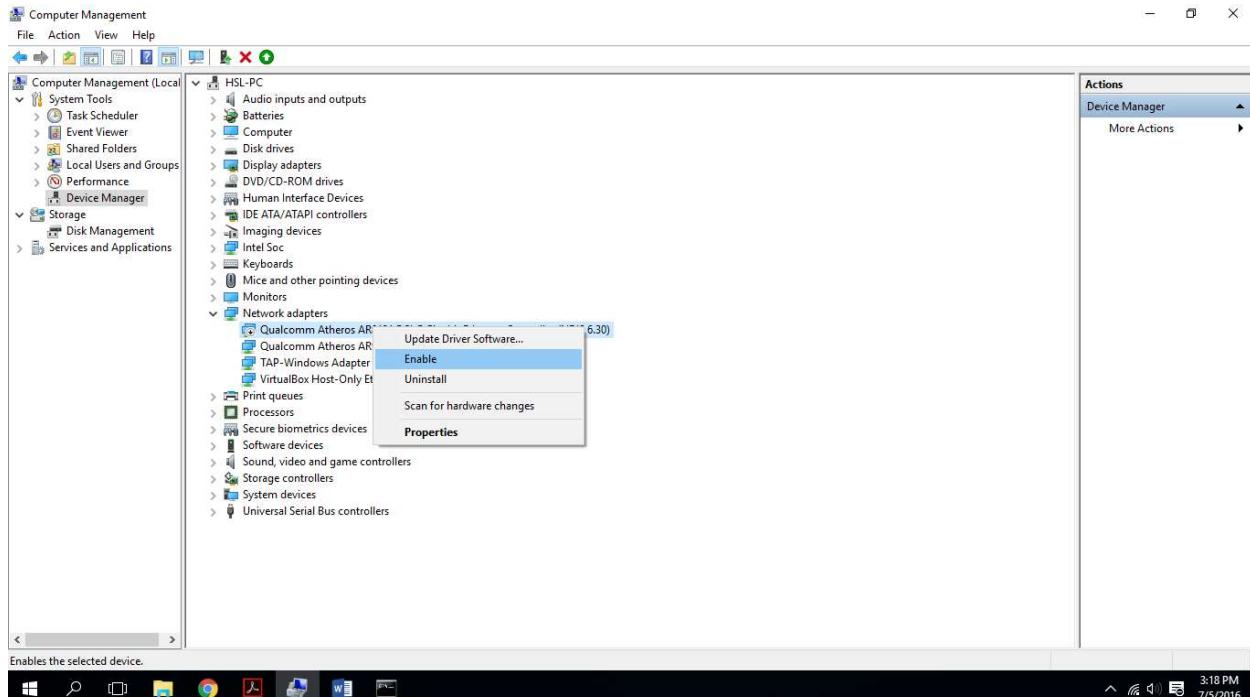


here the not present represents the default MAC address whereas the value represents your custom MAC address by default it will select the not present what you have to do is Select the value and give whatever MAC address you want to use.

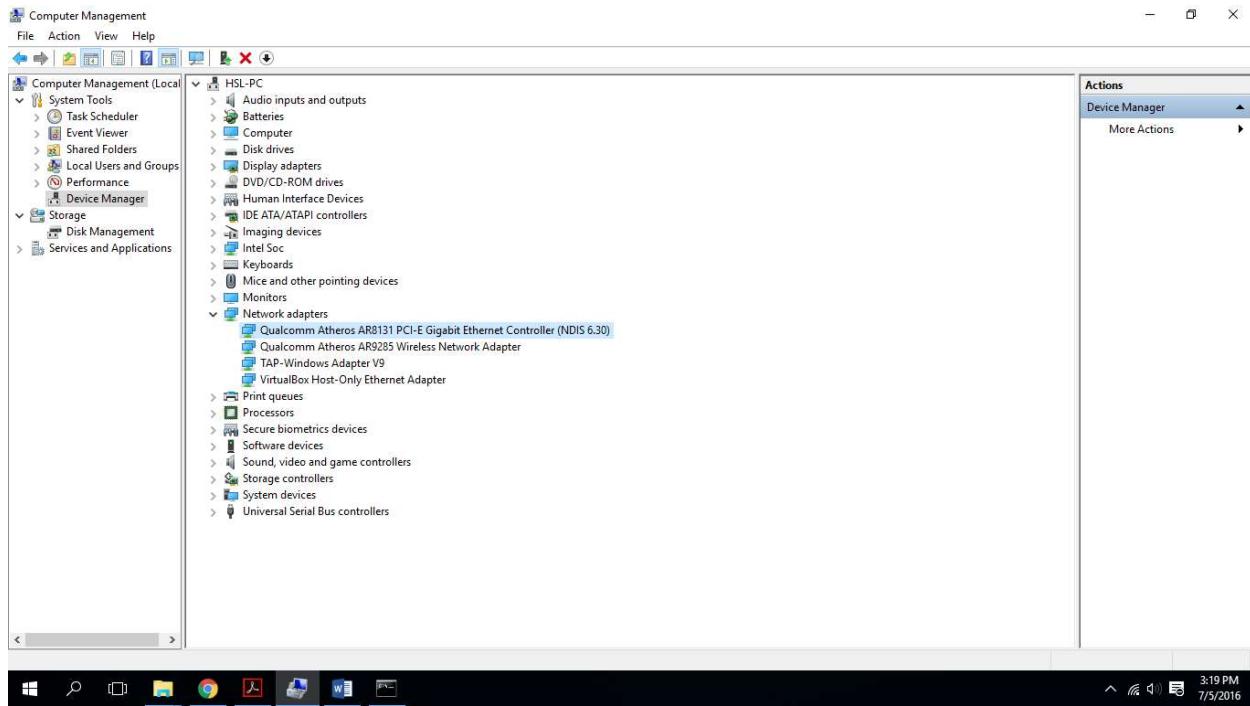


Once you are custom MAC address is given click on Ok so that the settings will be saved.

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

```
cmd 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>
```

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

HSL-PC

Computer Management (Local)

- System Tools
 - Task Scheduler
 - Event Viewer
 - Shared Folders
 - Local Users and Groups
 - Performance
 - Device Manager
- Storage
 - Disk Management
- Services and Applications

Qualcomm Atheros AR8131 PCI-E Gigabit Ethernet Controller (ND...)

Events Resources Power Management

General Advanced Driver Details

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)

OK Cancel

Actions Device Manager More Actions

Windows Taskbar: 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.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.129 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe2d:9dc0 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:2d:9d:cd txqueuelen 1000 (Ethernet)
                RX packets 35 bytes 3320 (3.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1122 bytes 210478 (205.5 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 28 bytes 1680 (1.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 28 bytes 1680 (1.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
Applications ▾ Places ▾ Terminal ▾ Tue 18:02 •
root@kali:~
```

File Edit View Search Terminal Help

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.129 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe2d:9dc0 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:2d:9d:cd txqueuelen 1000 (Ethernet)
                RX packets 35 bytes 3320 (3.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1122 bytes 210478 (205.5 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 28 bytes 1680 (1.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 28 bytes 1680 (1.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ifconfig eth0 down
root@kali:~# ifconfig
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 28 bytes 1680 (1.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 28 bytes 1680 (1.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

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

```
Applications ▾ Places ▾ Terminal ▾  
File Edit View Search Terminal Help  
root@kali:~# macchanger -e eth0  
Current MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
New MAC: 08:00:27:74:ed:7f (CADMUS COMPUTER SYSTEMS)
```

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

```
root@kali:~#  
File Edit View Search Terminal Help  
root@kali:~# macchanger -r eth0  
Current MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
New MAC: 4a:f3:2d:27:fd:46 (unknown)
```

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

```
Applications ▾ Places ▾ Terminal ▾  
File Edit View Search Terminal Help  
root@kali:~# macchanger -b -r eth0  
Current MAC: 20:8d:4a:e5:36:f5 (unknown)  
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
New MAC: 18:d0:5a:d9:f8:f3 (unknown)
```

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.

```
root@kali:~# macchanger -a eth0  
Current MAC: 08:00:27:74:ed:7f (CADMUS COMPUTER SYSTEMS)  
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
New MAC: 54:54:14:fa:85:12 (Digital RF Corea, Inc)
```

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.

```
root@kali:~# macchanger -A eth0  
Current MAC: 54:54:14:fa:85:12 (Digital RF Corea, Inc)  
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)  
New MAC: 00:19:da:fe:ae:b3 (Welltrans O&E Technology Co. , Ltd.)
```

Option I 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

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

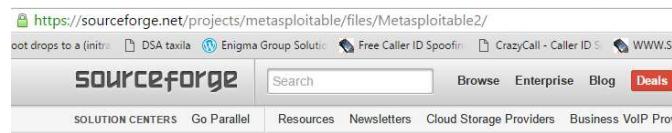
```
root@kali:~# macchanger -p eth0
Current MAC: 00:00:00:11:22:33 (XEROX CORPORATION)
Permanent MAC: 08:00:27:2d:9d:cd (CADMUS COMPUTER SYSTEMS)
New MAC: 00:00:00:11:22:33 (XEROX CORPORATION)
```

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

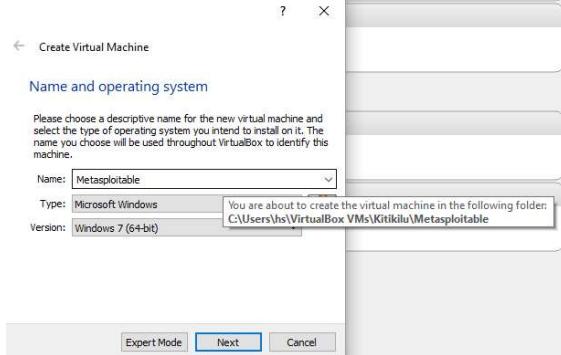
Metasploitable.nvram	5/20/2012 2:56 PM	NVRAM File	9 KB
Metasploitable.vmdk	7/26/2016 1:23 PM	Virtual Machine Disk	1,911,488 KB
Metasploitable.vmsd	5/7/2010 2:46 PM	VMSD File	0 KB
Metasploitable.vmx	5/20/2012 3:00 PM	VMX File	3 KB
Metasploitable.vmf	5/7/2010 2:46 PM	VMXF File	1 KB

Now start your Virtual Box



Click On New Button

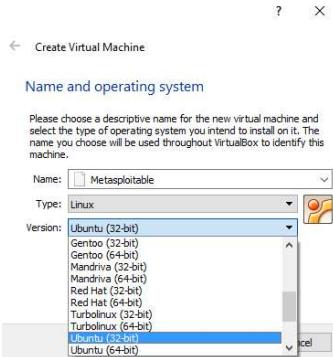
Give a name



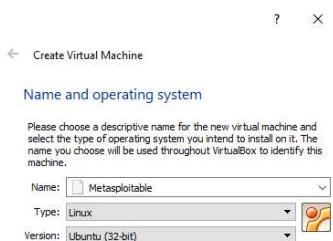
Select Type as Linux



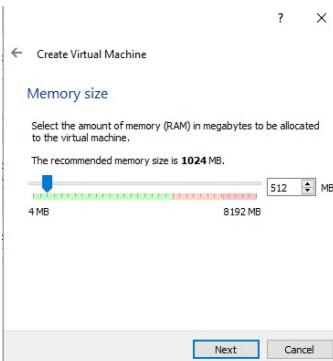
Select Version as Ubuntu 32 Bit.



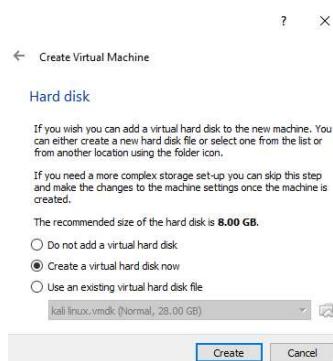
Click On Next



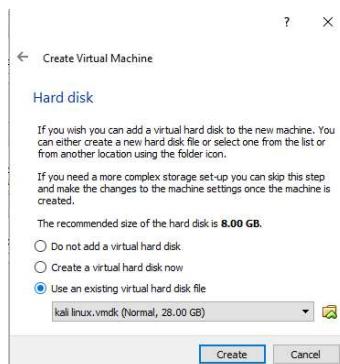
Give RAM(you can choose upto Green Area In The BAR) then Click on next



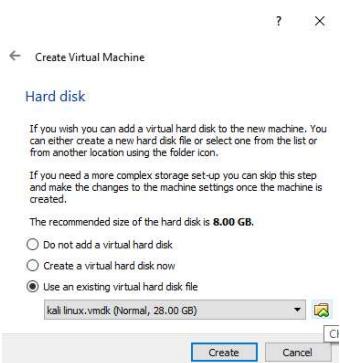
In this screen



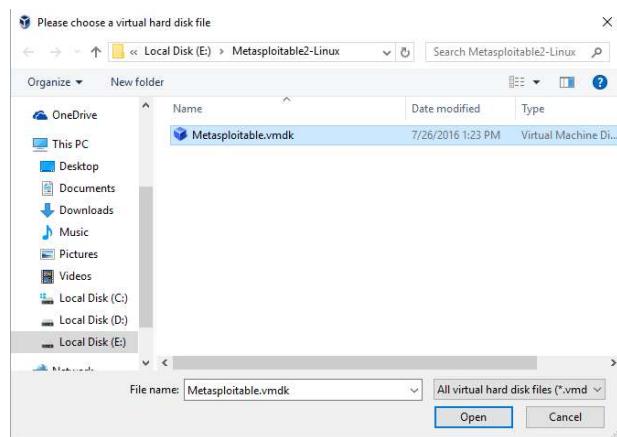
Select third option that is “Use an existing virtual harddisk file”



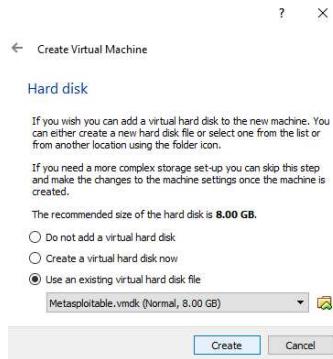
Click on the folder icon to select a file



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

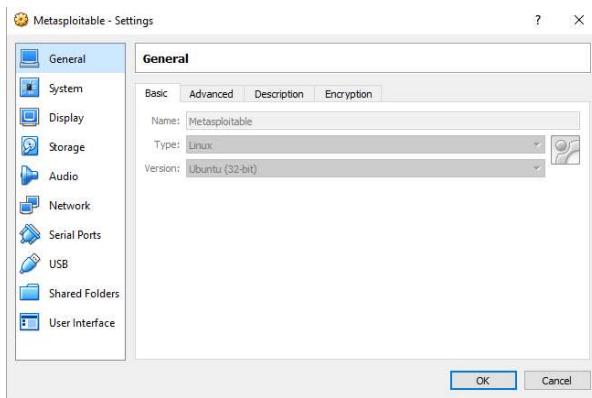
Select the VM you want to change the settings



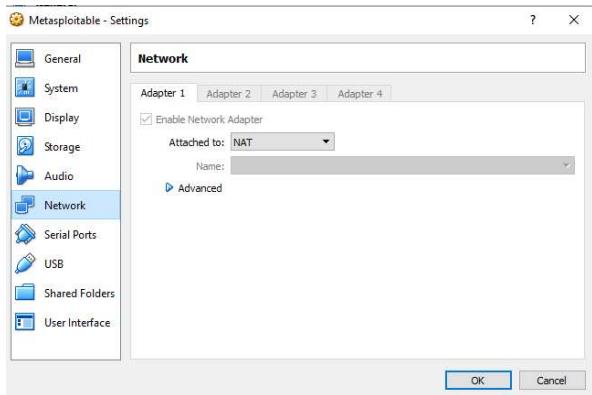
Then click on settings button on the TOP



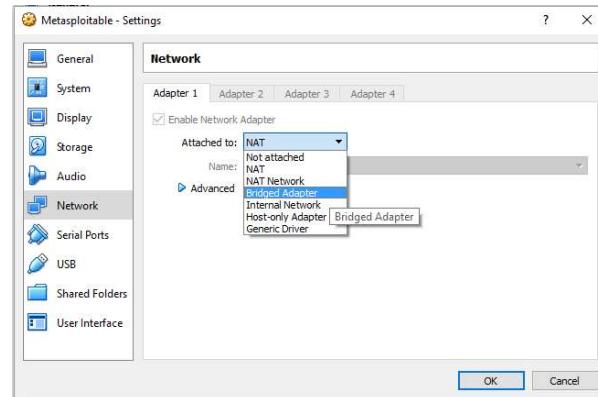
Then you should see the following box on screen.



Click on network tab to switch towards network related settings.



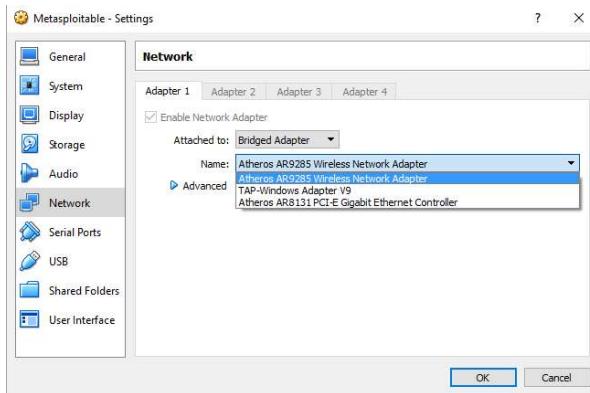
There by default "attached to" is selected as NAT, which results your VM getting Class A IP change it to "Bridged adapter" from the Drop-Down Menu.



Then if you are using a wifi like this



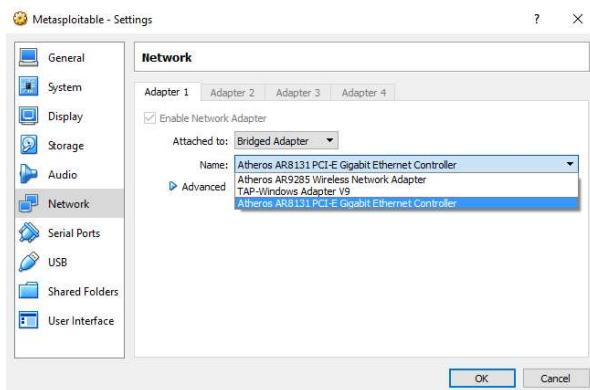
Select WIFI adapter from the "Name" Drop-Down Menu. (Adapter Name will not be same as mine)



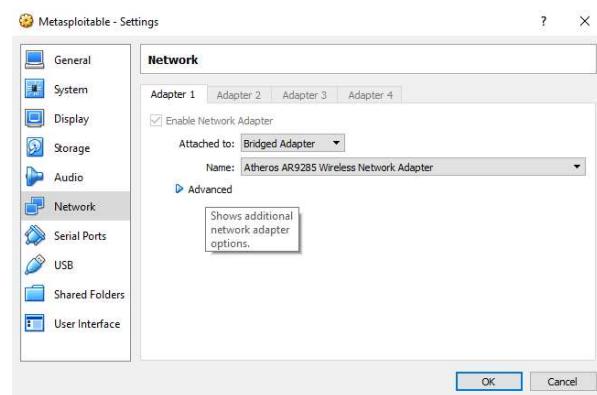
Or if you are using LAN like this



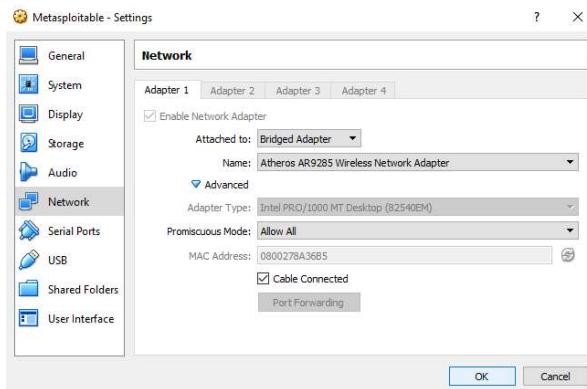
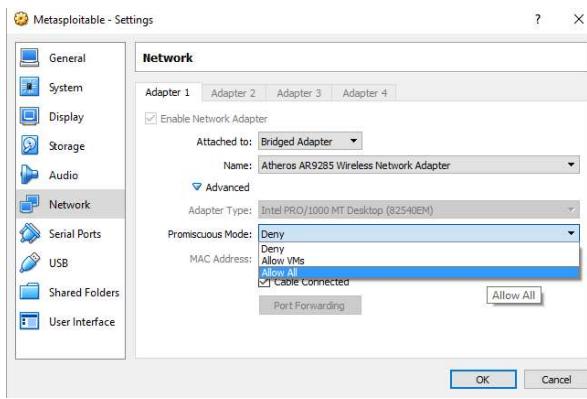
Select Ethernet adapter from the “Name” Drop-Down Menu. (Adapter Name will not be same as mine)



Next click on “Advanced” to expand advanced options.



In the “Advanced” under “Promiscuous 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)
```