Kali Linux

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

Kali Linux is one of the best open-source security packages of an ethical hacker, containing a set of tools divided by categories. Kali Linux can be installed in a machine as an Operating System, which is discussed in this tutorial. Installing Kali Linux is a practical option as it provides more options to work and combine the tools.

This tutorial gives a complete understanding on Kali Linux and explains how to use it in practice.

Audience

This tutorial has been prepared for beginners to help them understand the fundamentals of Kali Linux. It will specifically be useful for penetration testing professionals. After completing this tutorial, you will find yourself at a moderate level of expertise from where you can take yourself to the next levels.

Prerequisites

Although this tutorial will benefit most of the beginners, it will definitely be a plus if you are familiar with the basic concepts of any Linux operating system.

Copyright & Disclaimer

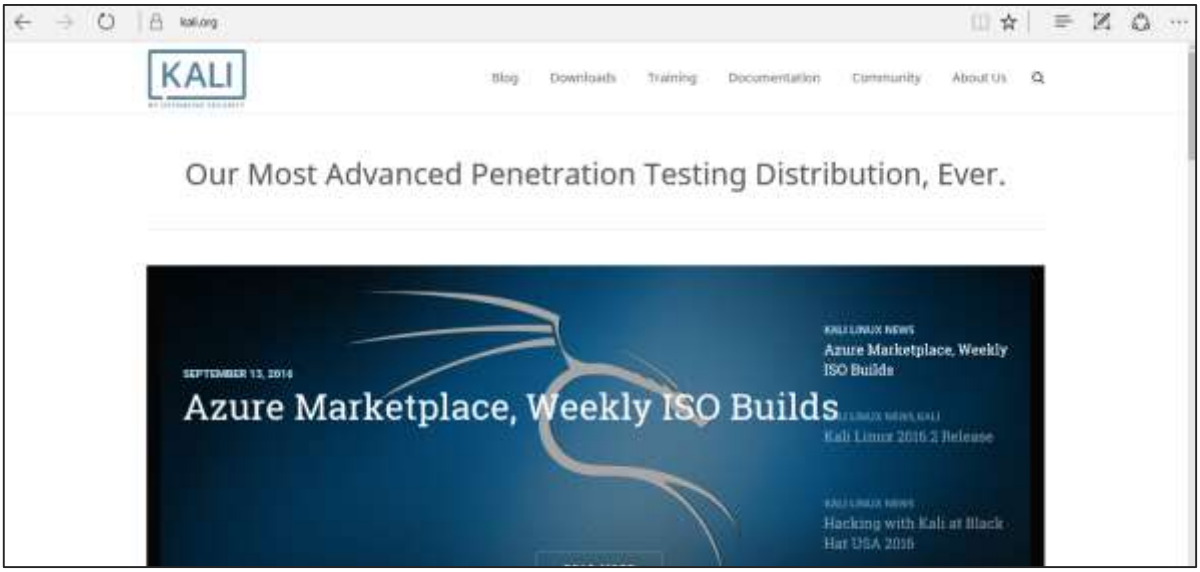
Table of Contents

1. Kali Linux – Installation & Configuration

Kali Linux is one of the best security packages of an ethical hacker, containing a set of tools divided by the categories. It is an open source and its official webpage is https://www.kali.org.

Generally, Kali Linux can be installed in a machine as an Operating System, as a virtual machine which we will discuss in the following section. Installing Kali Linux is a practical option as it provides more options to work and combine the tools. You can also create a live boot CD or USB. All this can be found in the following link: https://www.kali.org/downloads/

BackTrack was the old version of Kali Linux distribution. The latest release is Kali 2016.1 and it is updated very often.



To install Kali Linux –

- First, we will download the Virtual box and install it.
- Later, we will download and install Kali Linux distribution.

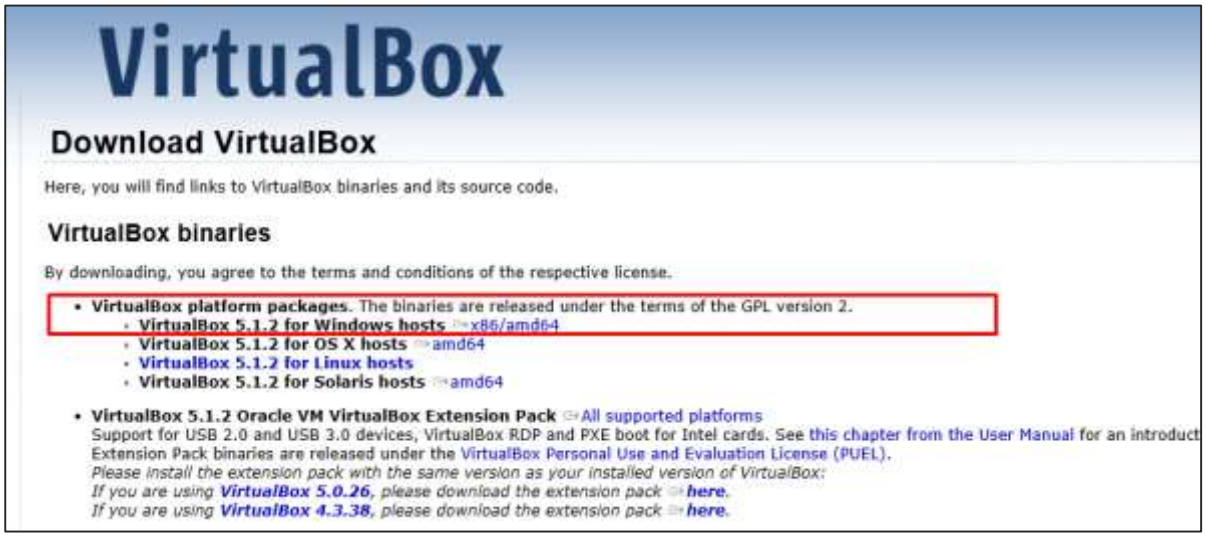
Download and Install the Virtual Box

A Virtual Box is particularly useful when you want to test something on Kali Linux that you are unsure of. Running Kali Linux on a Virtual Box is safe when you want to experiment with unknown packages or when you want to test a code.

With the help of a Virtual Box, you can install Kali Linux on your system (not directly in your hard disk) alongside your primary OS which can MAC or Windows or another flavor of Linux.

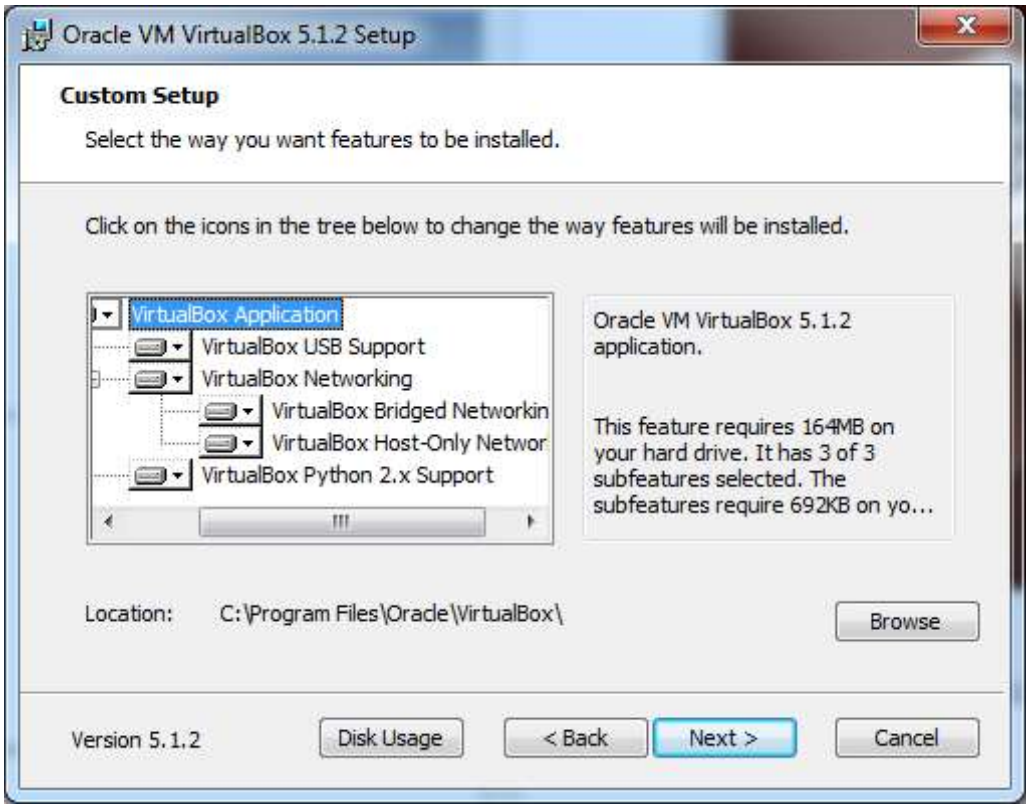
Let's understand how you can download and install the Virtual Box on your system.

Step 1: To download, go to https://www.virtualbox.org/wiki/Downloads. Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.

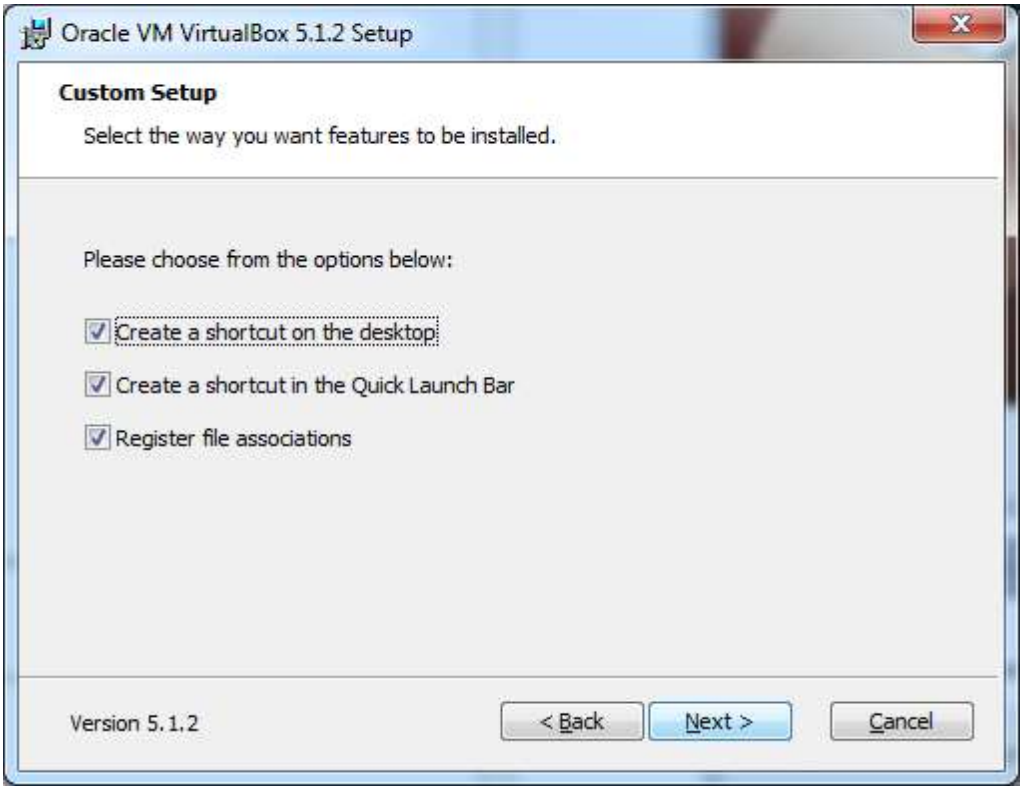


Step 2: Click **Next**.

Step 3: The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click **Next**.

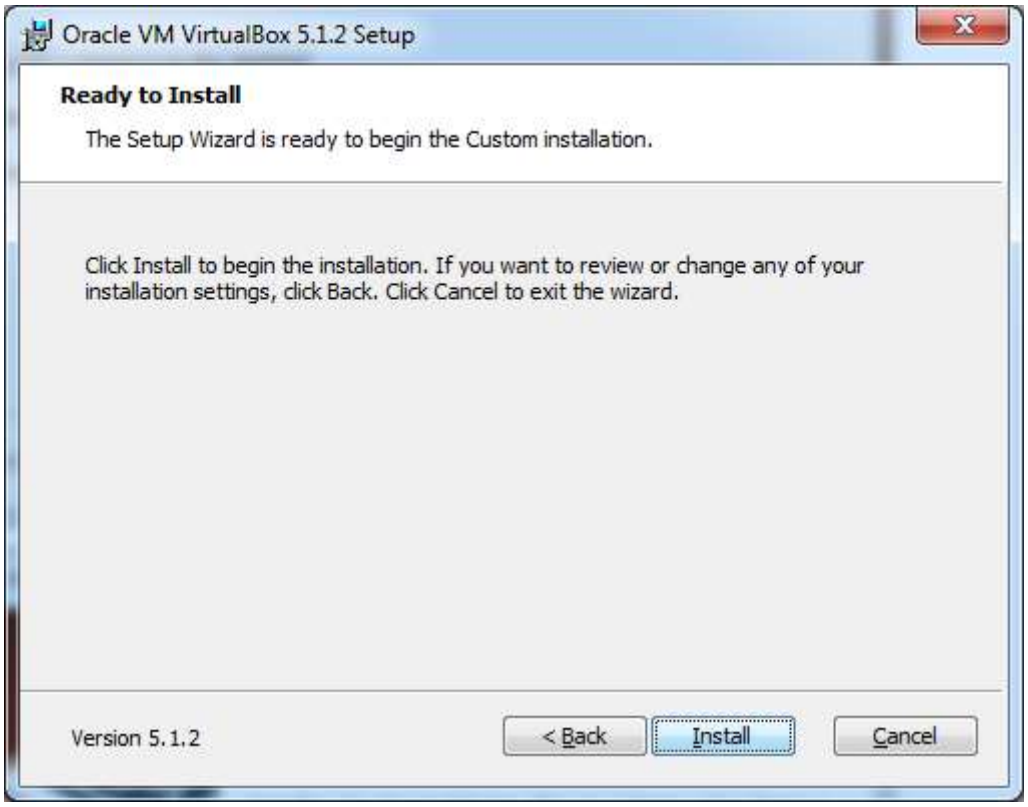


Step 4: Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



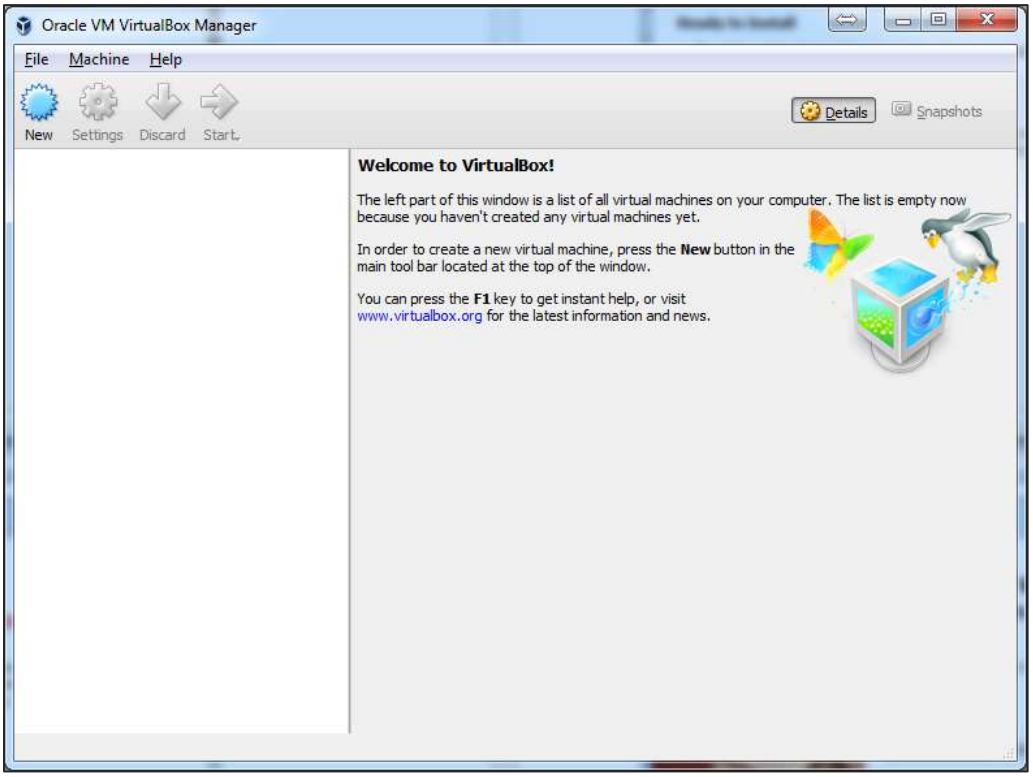
Step 5: Click **Yes** to proceed with the installation.

Step 6: The **Ready to Install** screen pops up. Click Install.



Step 7: Click the **Finish** button.

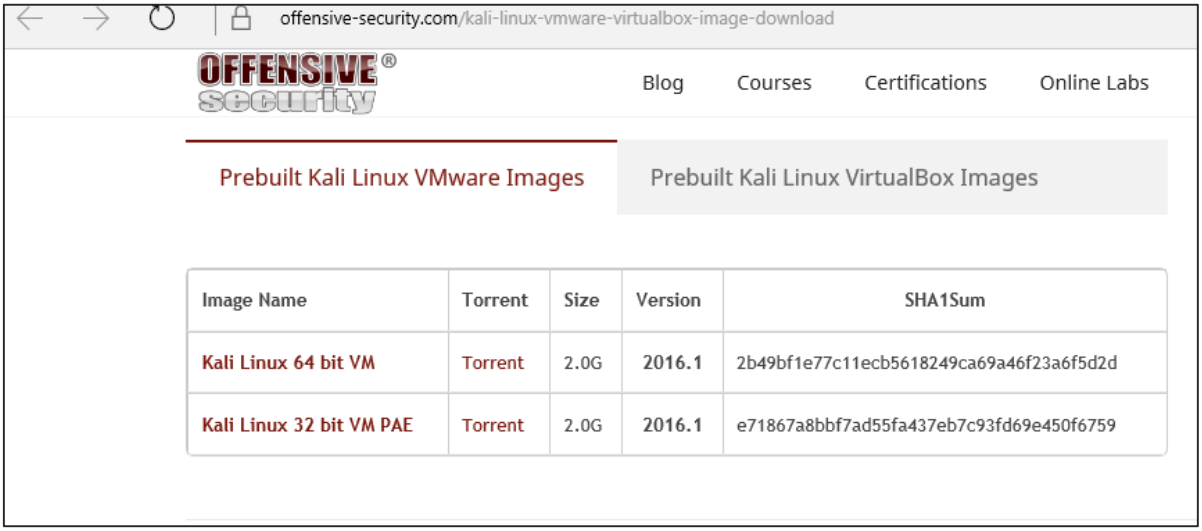
The Virtual Box application will now open as shown in the following screenshot. Now we are ready to install the rest of the hosts for this manual and this is also recommended for professional usage.



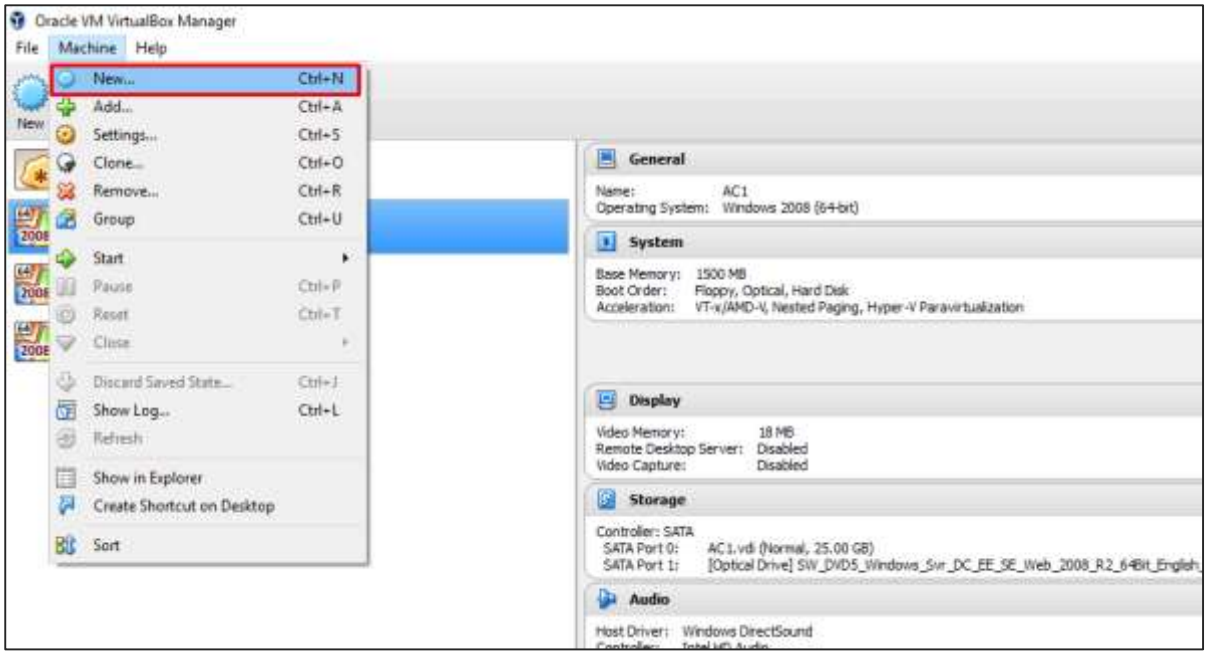
Install Kali Linux

Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

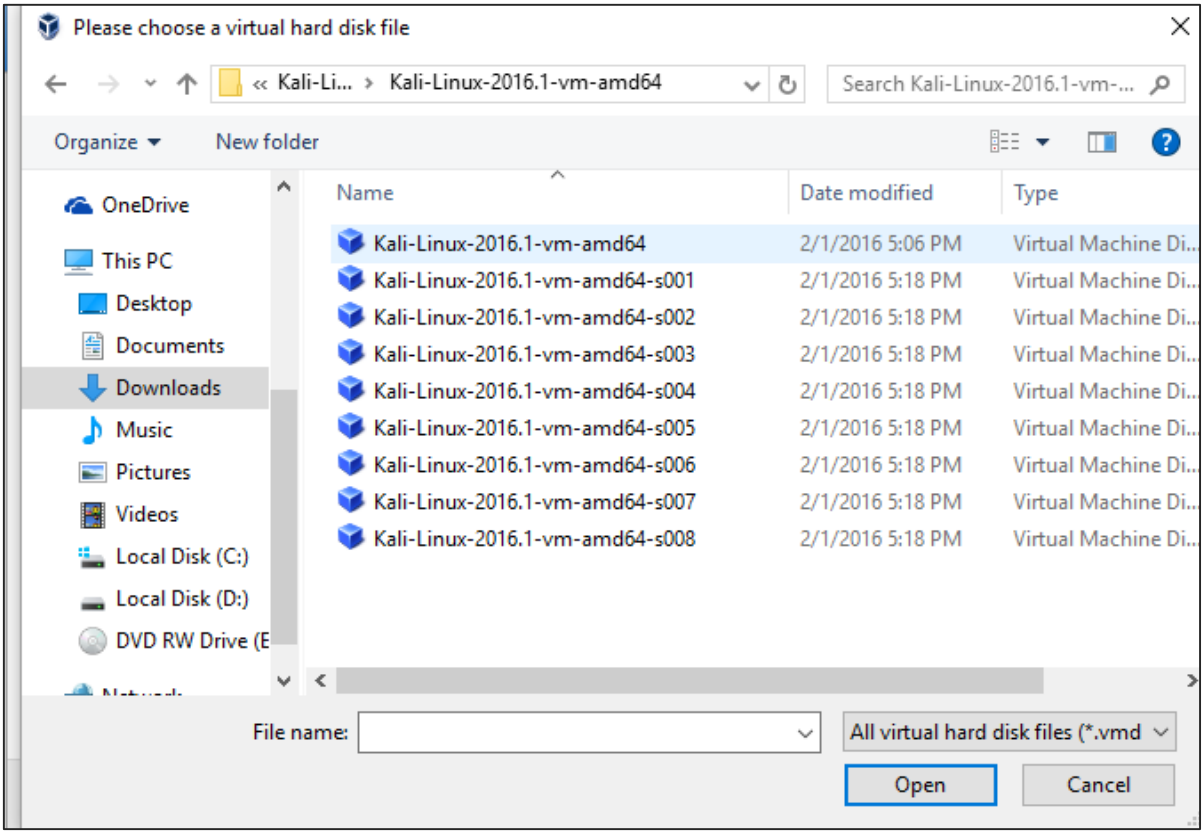
Step 1: Download the Kali Linux package from its official website: https://www.kali.org/downloads/



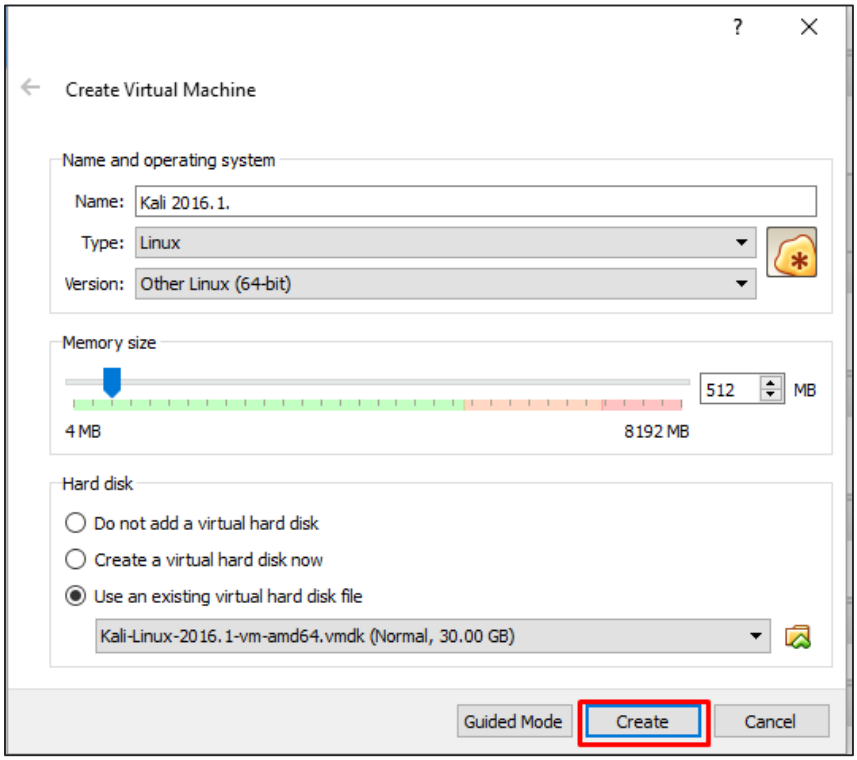
Step 2: Click **VirtualBox -> New** as shown in the following screenshot.



Step 3: Choose the right **virtual hard disk file** and click **Open**.



Step 4: The following screenshot pops up. Click the **Create** button.

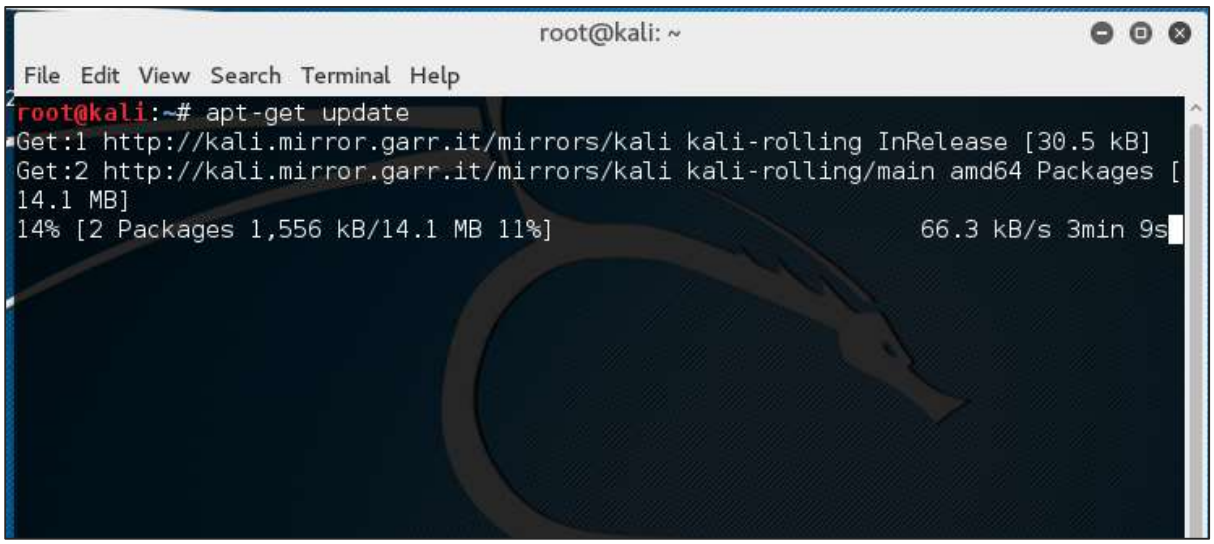


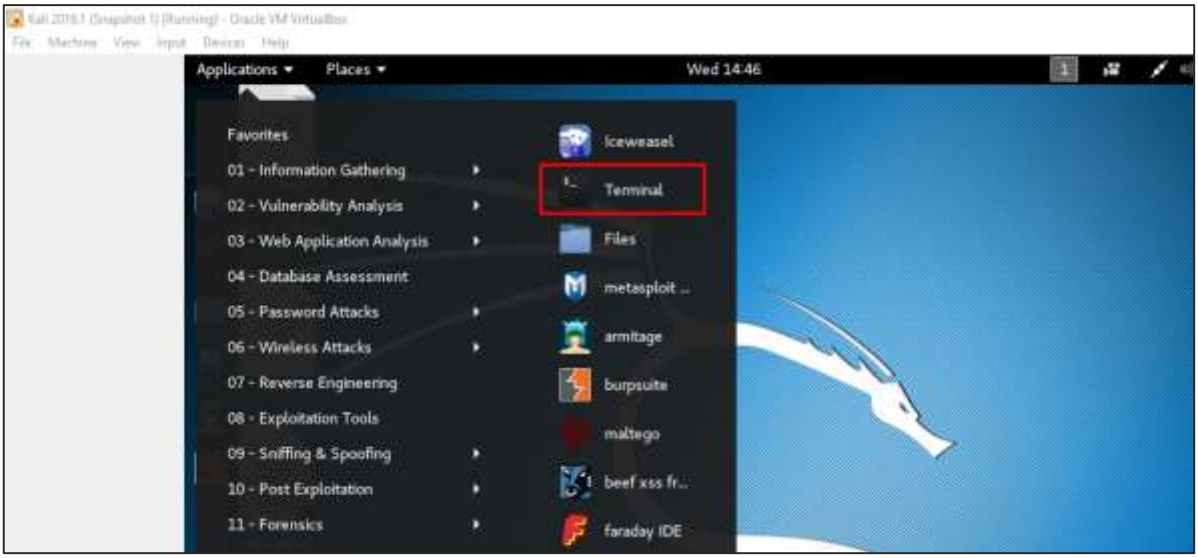
Step 5: Start Kali OS. The default username is **root** and the password is **toor**.

Update Kali

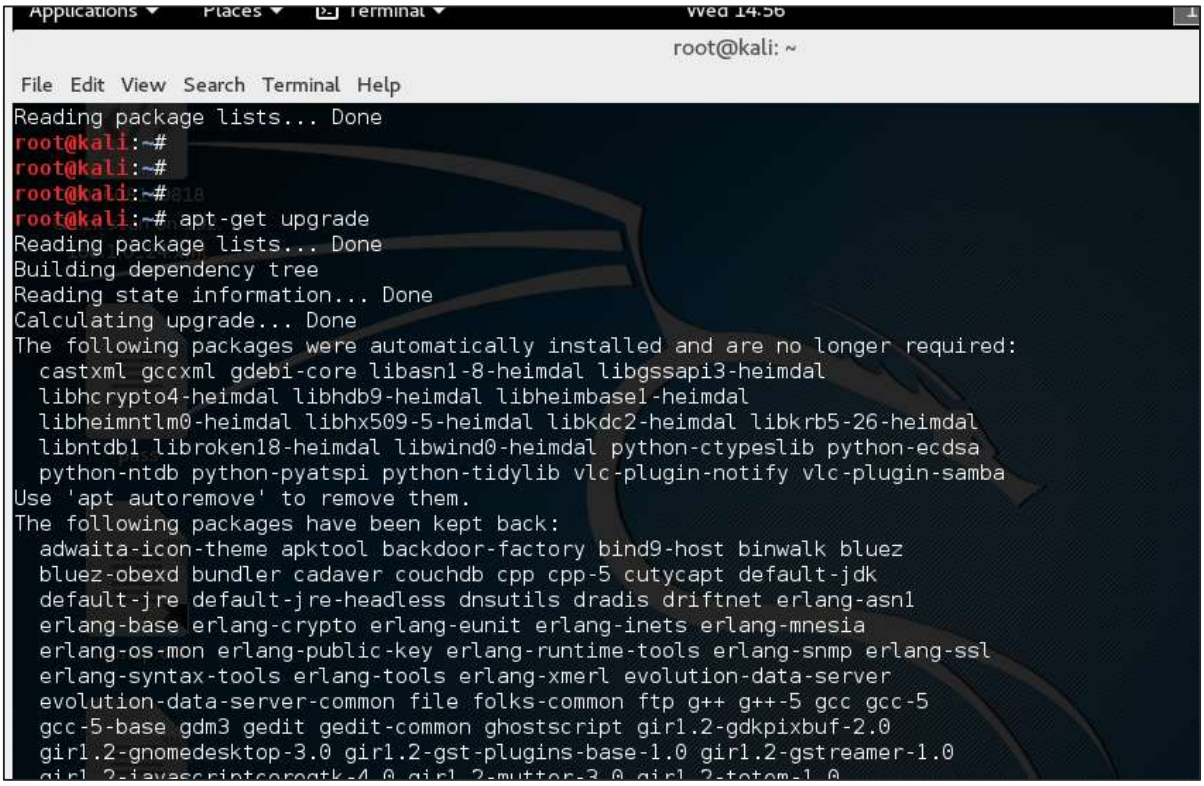
It is important to keep updating Kali Linux and its tools to the new versions, to remain functional. Following are the steps to update Kali.

Step 1: Go to Application -> Terminal. Then, type "apt-get update" and the update will take place as shown in the following screenshot.

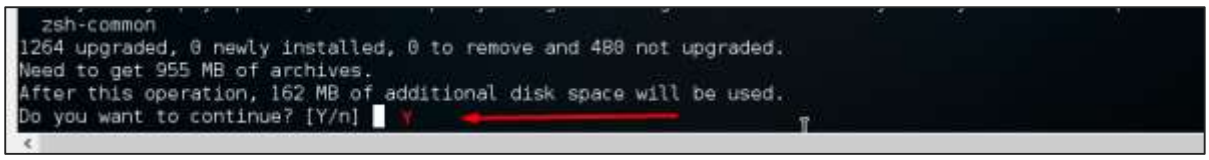




Step 2: Now to upgrade the tools, type "apt-get upgrade" and the new packages will be downloaded.



Step 3: It will ask if you want to continue. Type "**Y**" and "**Enter**".



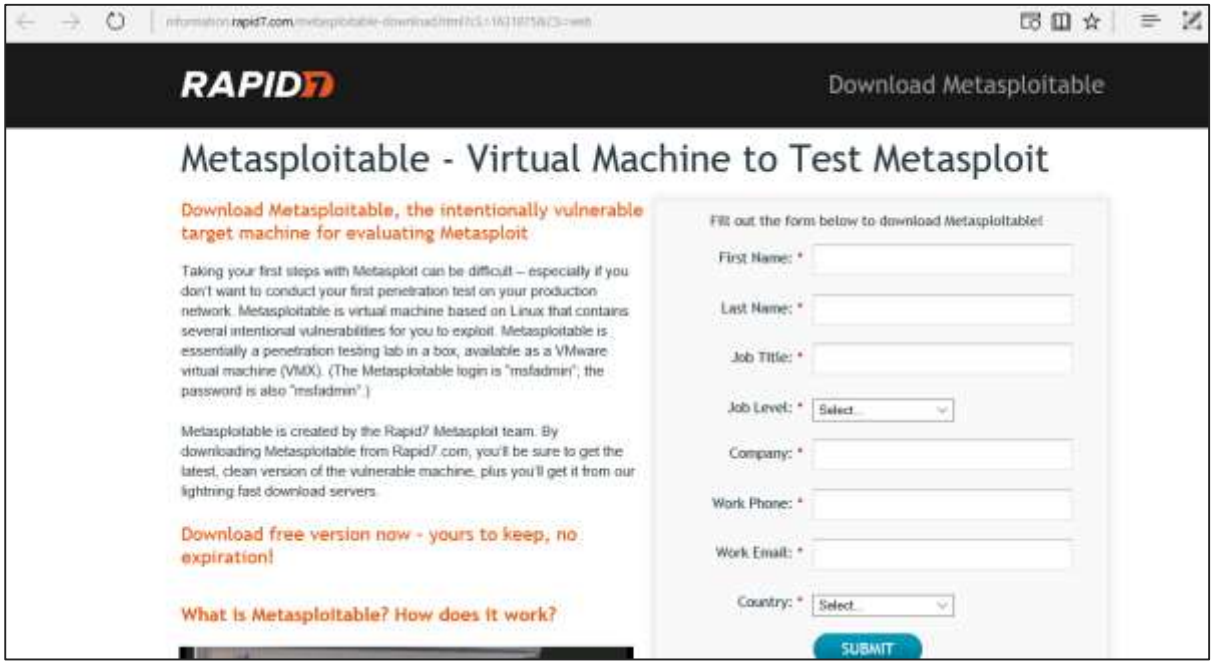
Step 4: To upgrade to a newer version of Operating System, type "**apt-get dist-upgrade**".

```
root@kali:~# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  caribou-antler castxml creepy dff gccxml gdebi-core girl.2-clutter-gst-2.0 girl.2-evince-3.0 girl.2-gkbd-3.0
  girl.2-packagekitglib-1.0 girl.2-xkl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
  gtk2-engines gucharmap hwdata libapache2-mod-php5 libasn1-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56
  libavfilter-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
  libbind9-90 libboost-filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.0 libboost-system1.58.0
  libboost-thread1.58.0 libcamel-1.2-54 libchromaprint0 libclutter-gst-2.0-0 libcrypto++9v5 libcurses-perl
  libcurses-ui-perl libdns100 libedataserver-1.2-21 libexporter-tiny-perl libfftw3-single3 libgdict-1.0-9
  libglew1.13 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglext1 libgucharmap-2-90-7
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
  libhx509-5-heimdal libicalla libilmbase6v5 libisc95 libisccc90 libisccfg90 libjasper1 libjpeg9
  libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 libllvm3.7 liblouis9 liblwres90
  libnm-glib-vpn1 libntdb1 libonig2 libopenexr6v5 libopenjpeg5 libpff1 libpgm-5.1-0 libphonon4 libpoppler57
  libpostproc-ffmpeg53 libpth20 libqdbm14 libqmi-glib1 libquvi-scripts libquvi7 libradare2-0.9.9 libregfi0
  libroken18-heimdal libsodium13 libswresample-ffmpeg1 libswscale-ffmpeg3 libtask-weaken-perl libtre5 libtrio2
  libusageenvironment1 libvpx3 libwebp5 libwebpdemux1 libwebpmux1 libwebrtc-audio-processing-0 libwildmidi1
```

Laboratory Setup

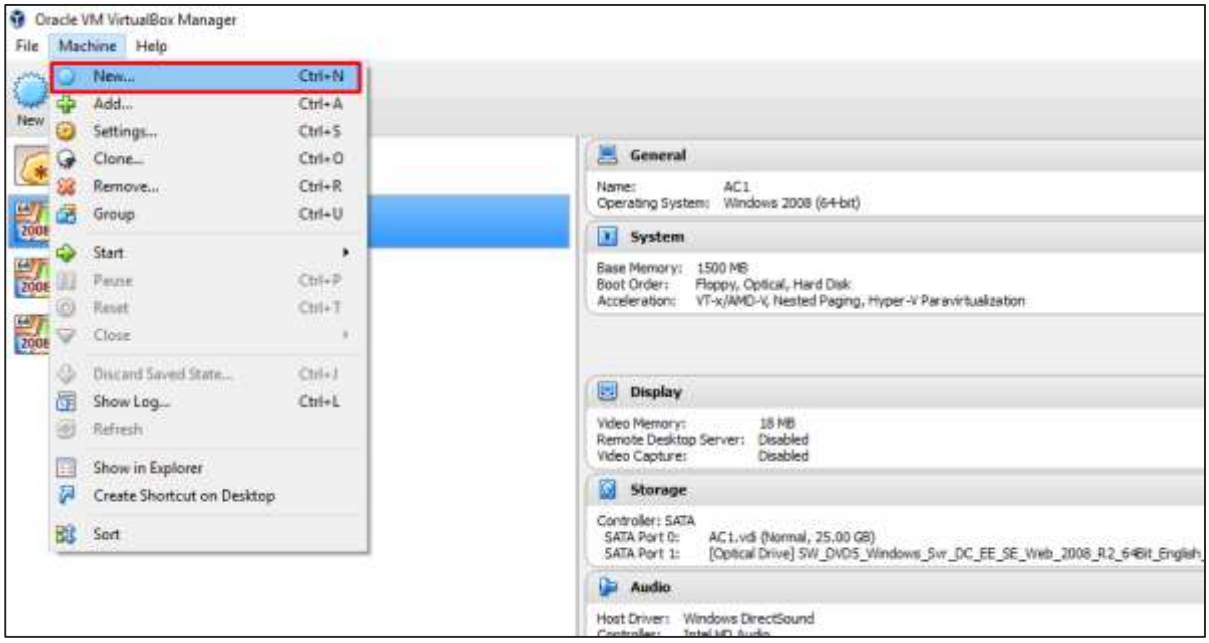
In this section, we will set up another testing machine to perform the tests with the help of tools of Kali Linux.

Step 1: Download **Metasploitable**, which is a Linux machine. It can be downloaded from the official webpage of **Rapid7**: https://information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web

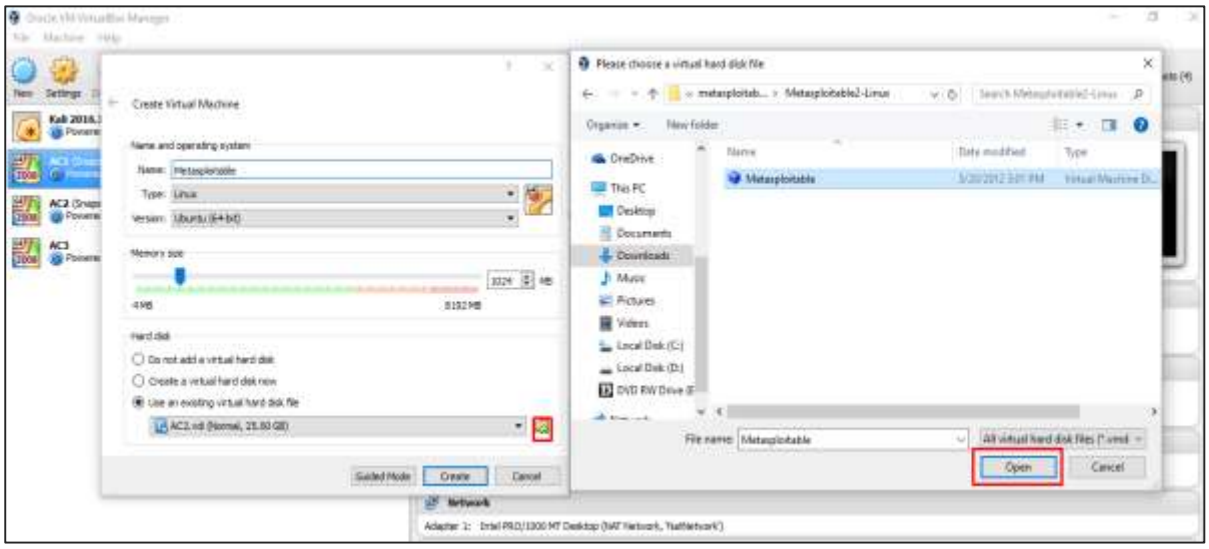


Step 2: Register by supplying your details. After filling the above form, we can download the software.

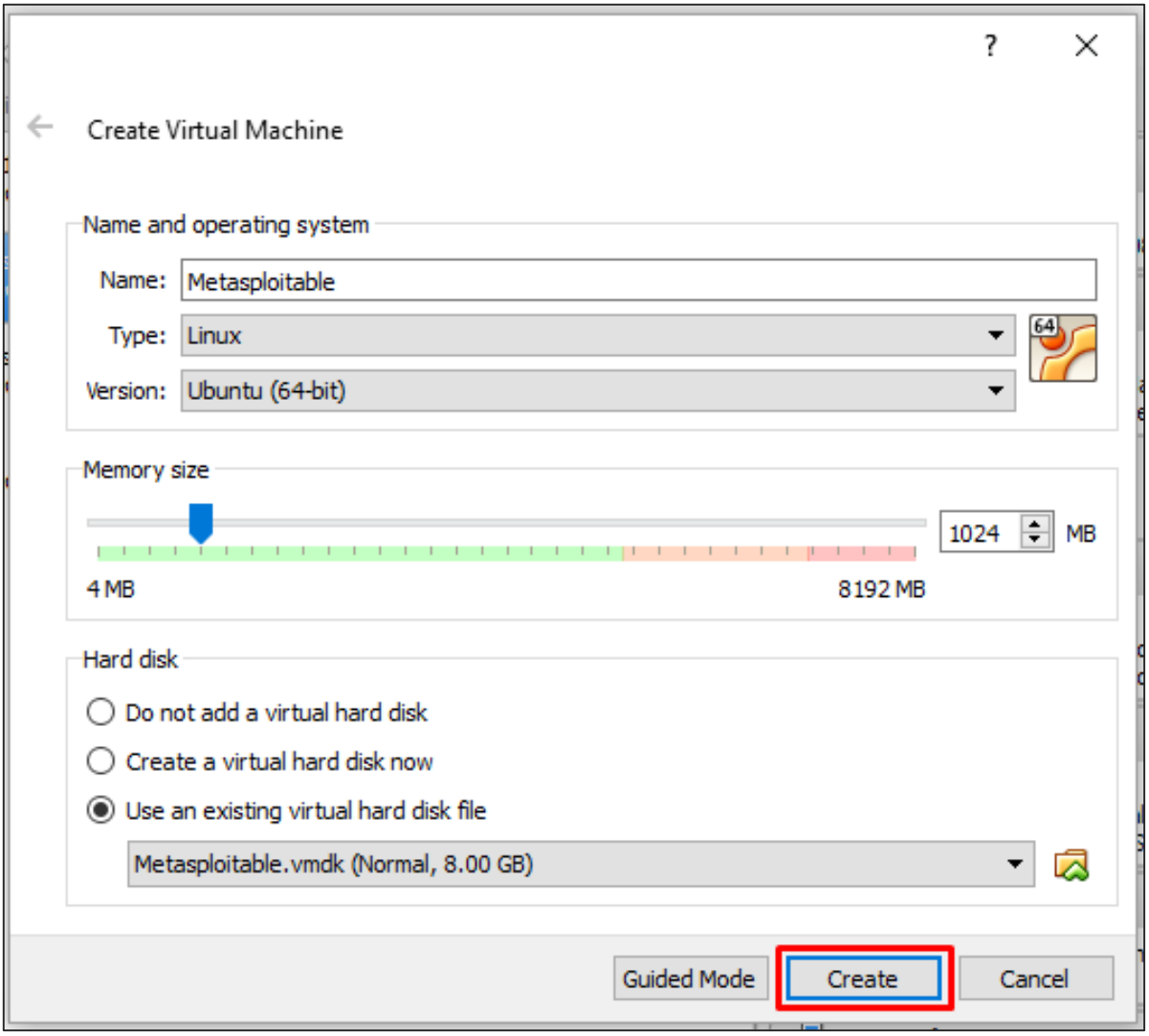
Step 3: Click **VirtualBox -> New**.



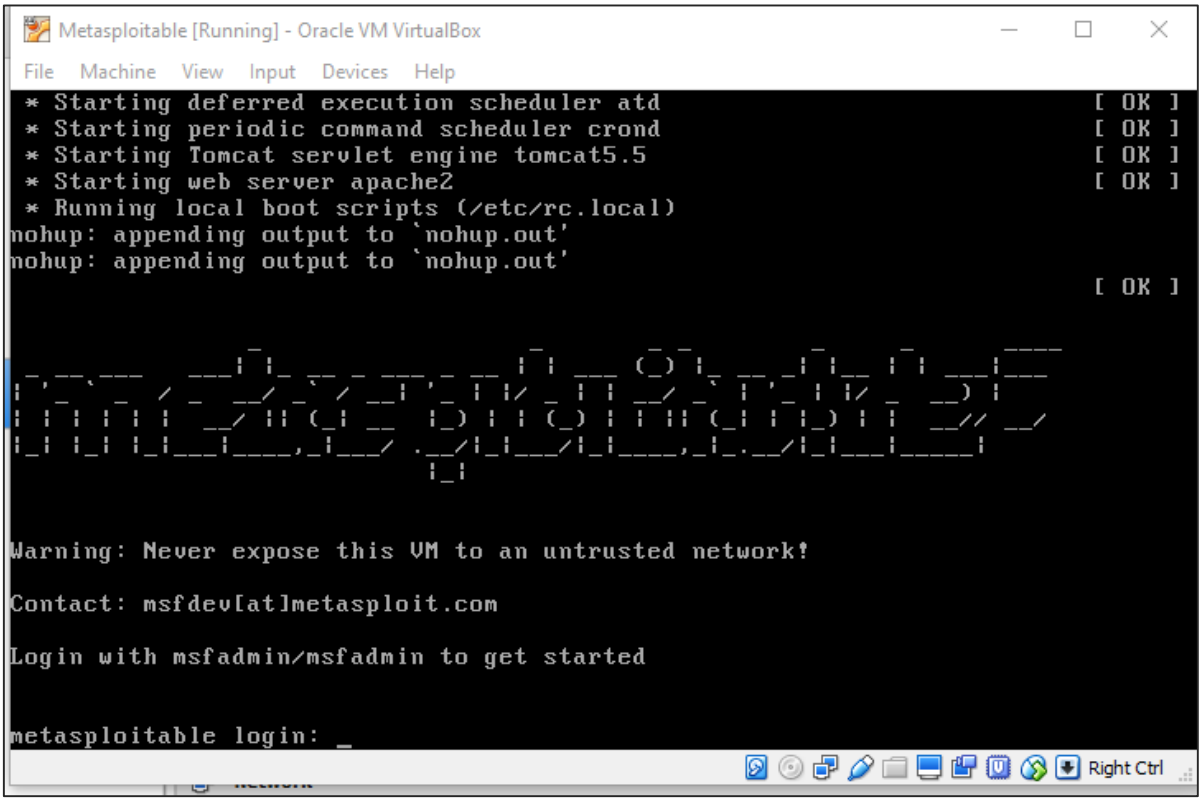
Step 4: Click "**Use an existing virtual hard disk file**". Browse the file where you have downloaded **Metasploitable** and click **Open**.



Step 5: A screen to create a virtual machine pops up. Click "Create".



The default username is **msfadmin** and the password is **msfadmin**.



2. Kali Linux – Information Gathering Tools

In this chapter, we will discuss the information gathering tools of Kali Linux.

NMAP and ZenMAP

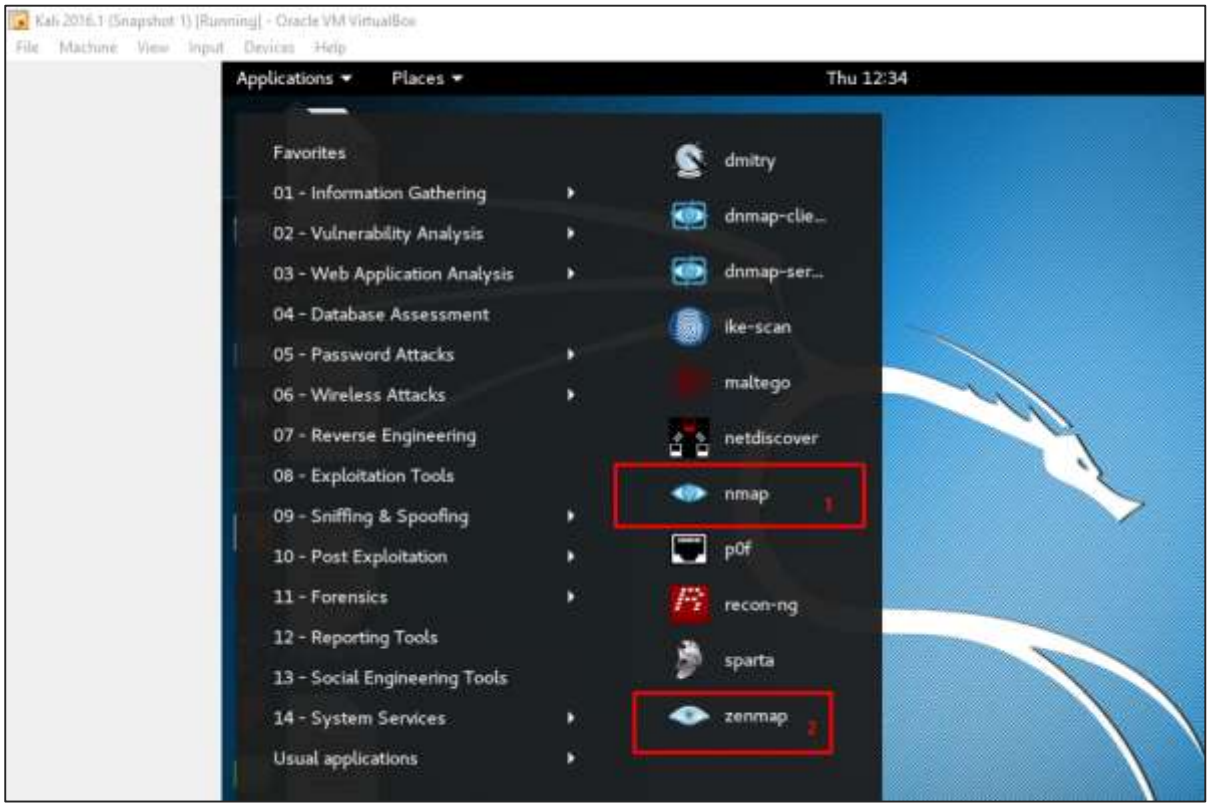
NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

Now, let's go step by step and learn how to use NMAP and ZenMAP.

Step 1: To open, go to Applications -> 01-Information Gathering -> nmap or zenmap.

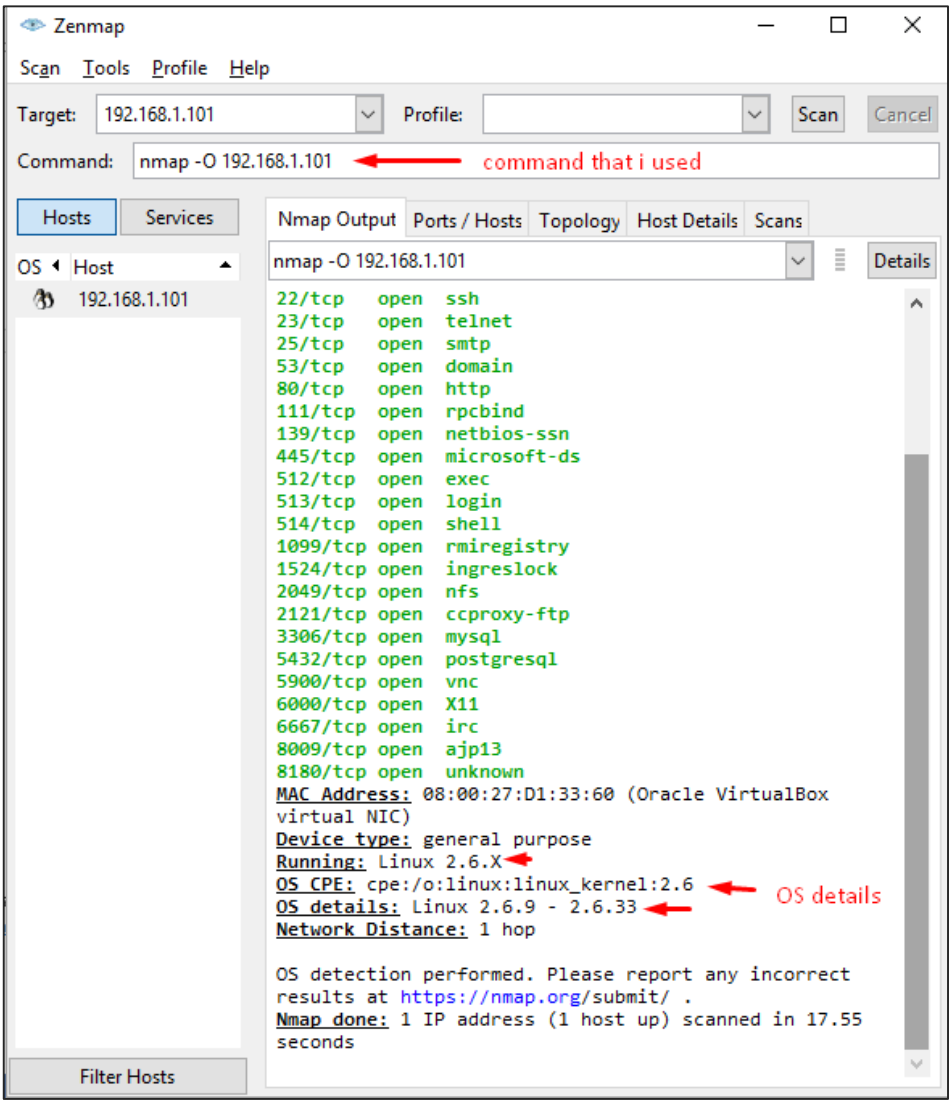


Step 2: The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable "-O". For more information, use this link: https://nmap.org/book/man-os-detection.html

The command that we will use is:

```
nmap -O 192.168.1.101
```

The following screenshot shows where you need to type the above command to see the Nmap output:

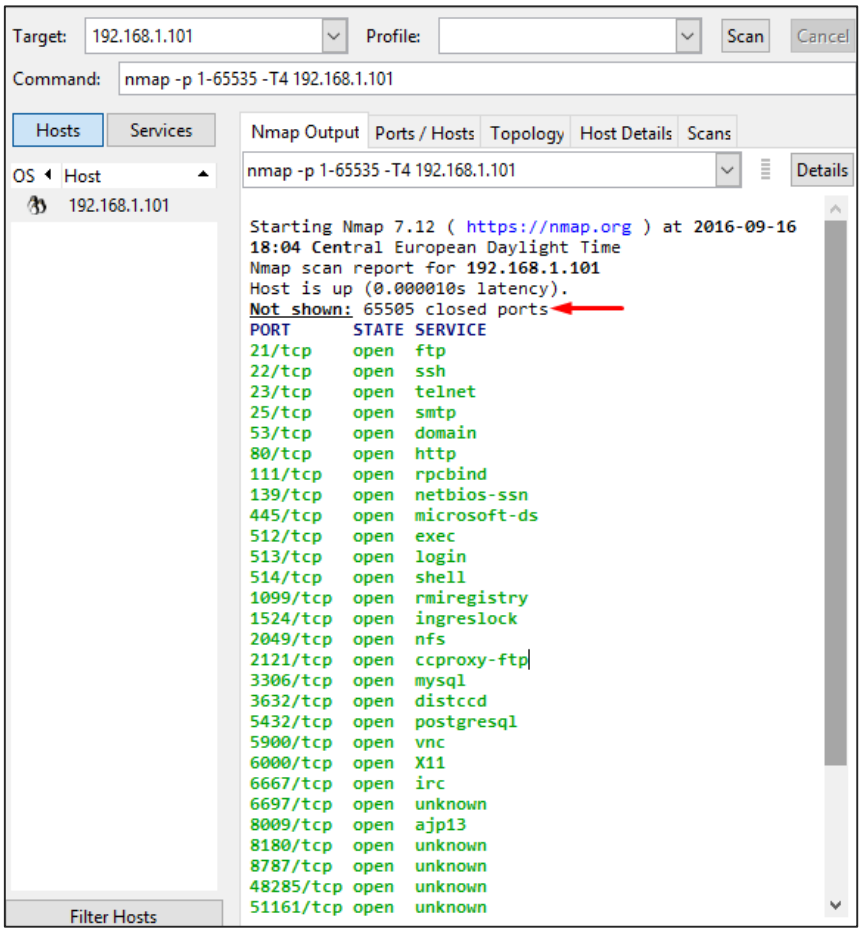


Step 3: Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command:

```
nmap -p 1-65535 -T4  192.168.1.101
```

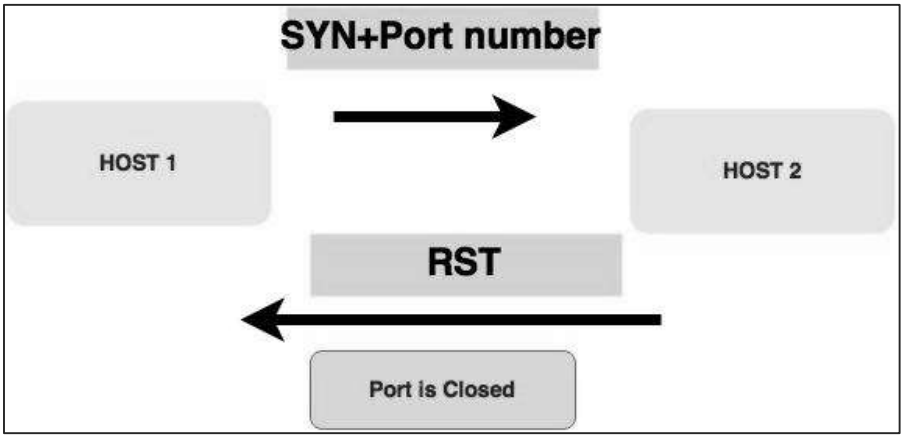
Where the parameter "–p" indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and "-T4" is the speed of scanning at which NMAP has to run.

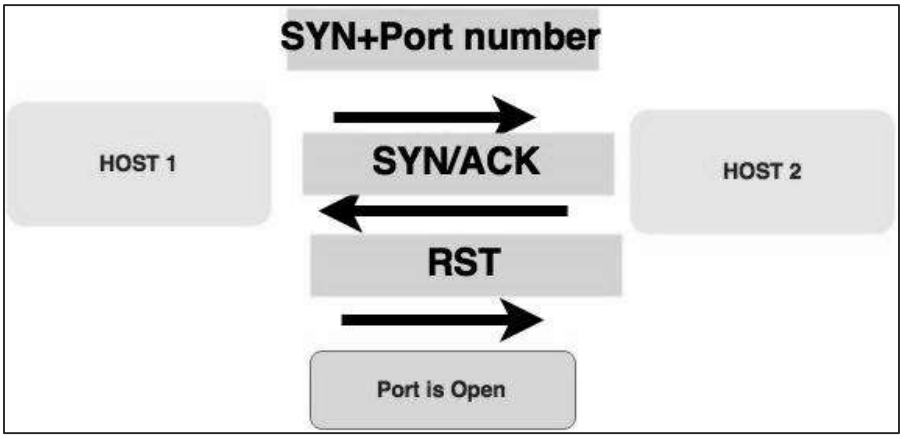
Following are the results. In green are all the TCP open ports and in red are all the closed ports. However, NMAP does not show as the list is too long.



Stealth Scan

Stealth scan or SYN is also known as **half-open scan**, as it doesn't complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn't active or is closed.





Now to see the SYN scan in practice, use the parameter **–sS** in NMAP. Following is the full command –

```
nmap -sS -T4 192.168.1.101
```

The following screenshot shows how to use this command: