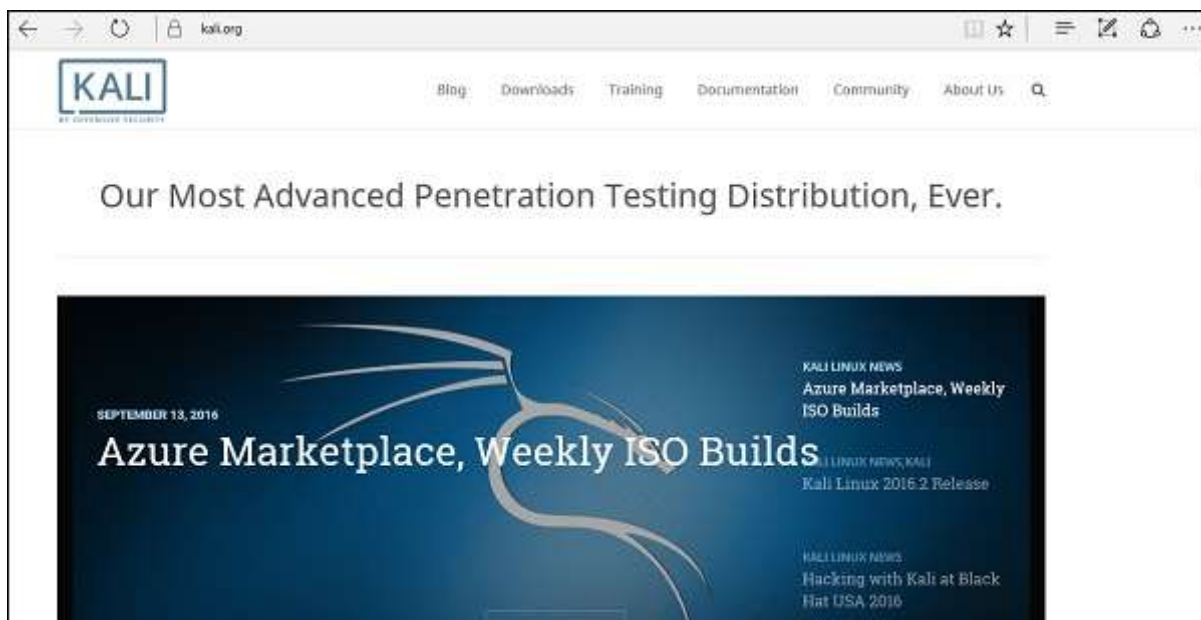


## Kali Linux - Installation and Configuration

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.

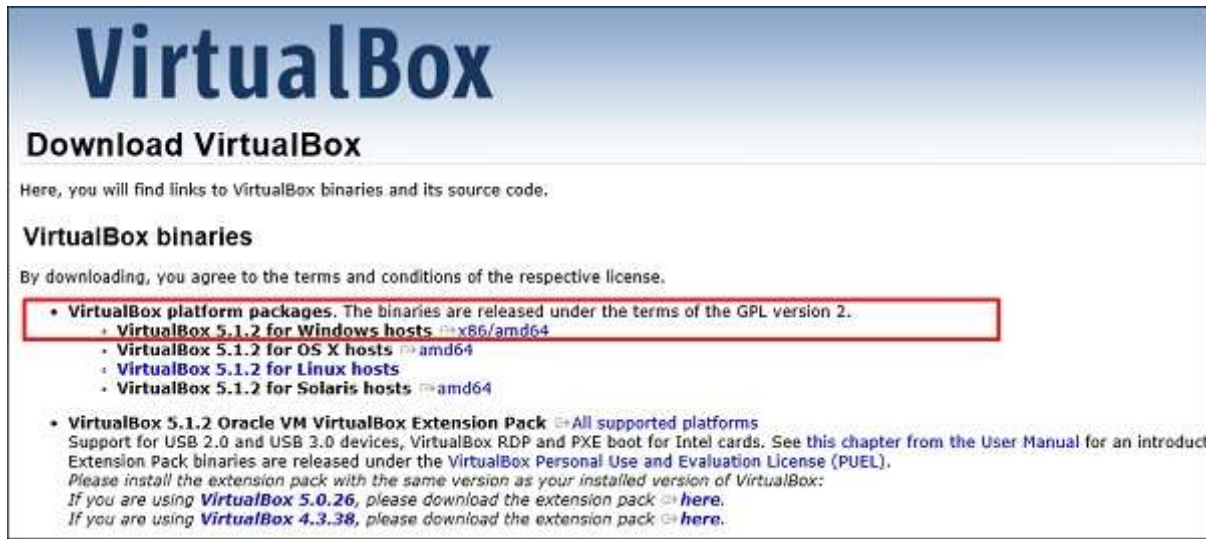
### Download and Install the Virtual Box

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.

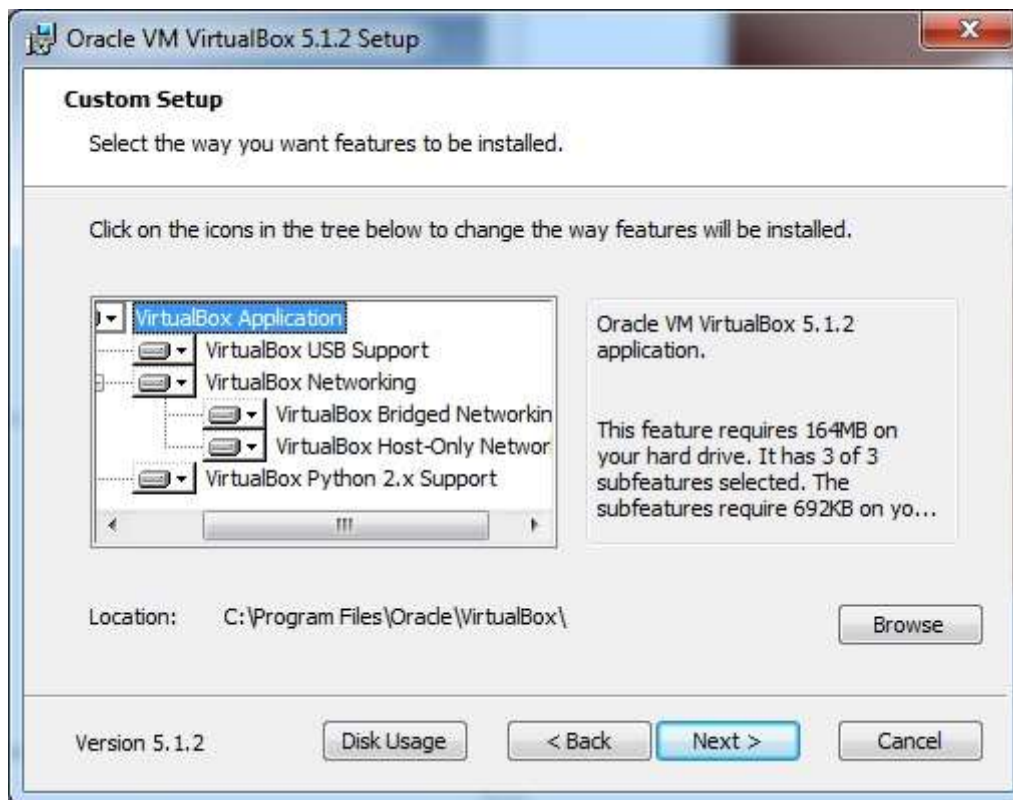
**Step 1** – To download, go to <https://www.virtualbox.org/wiki/Downloads> . Depending on your operating system, select the right package. In this case, it will be the first one for Windows as shown in the following screenshot.



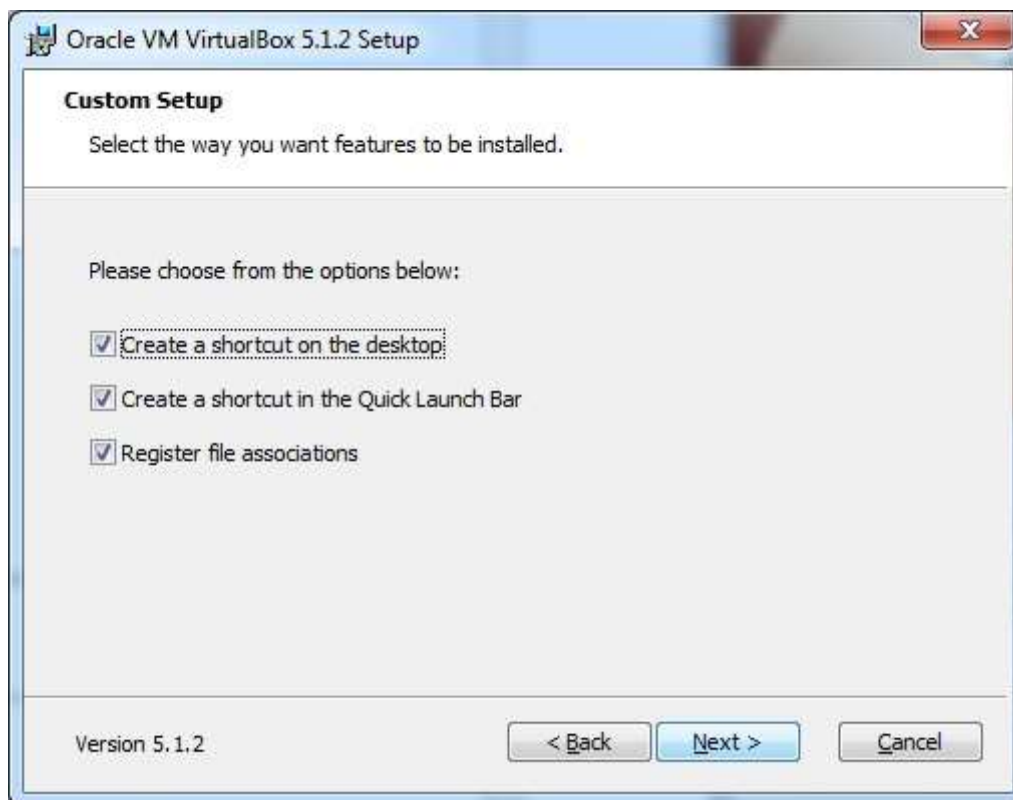
**Step 2** – Click **Next**.



**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**.



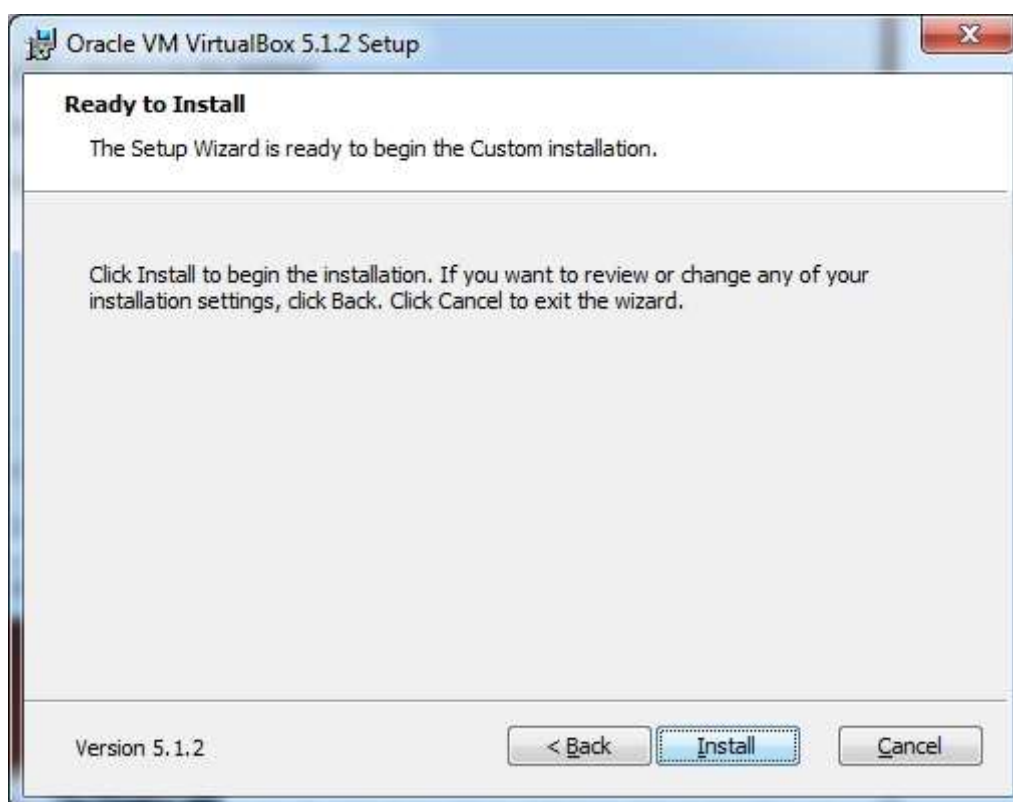
**Step 4** – Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



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



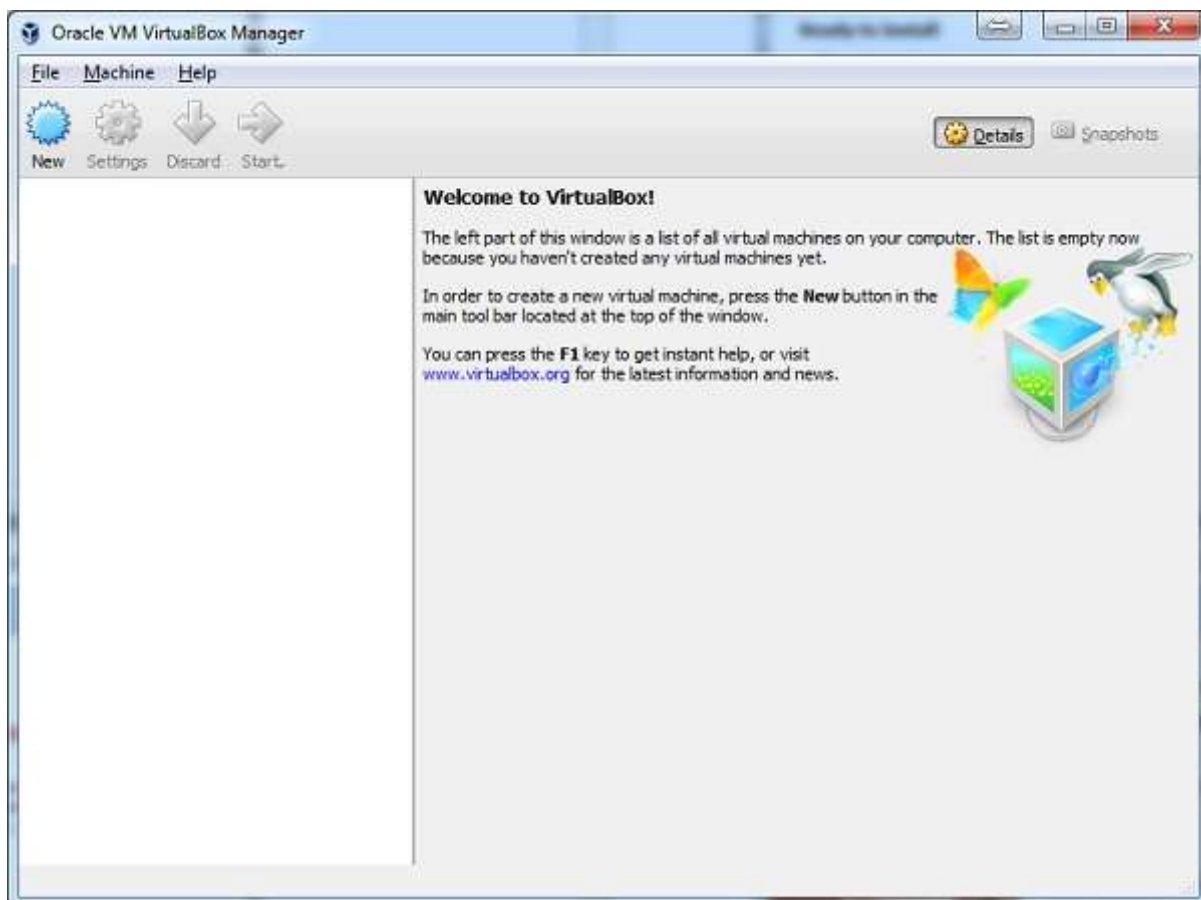
**Step 6** – The **Ready to Install** screen pops up. Click **Install**.



**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

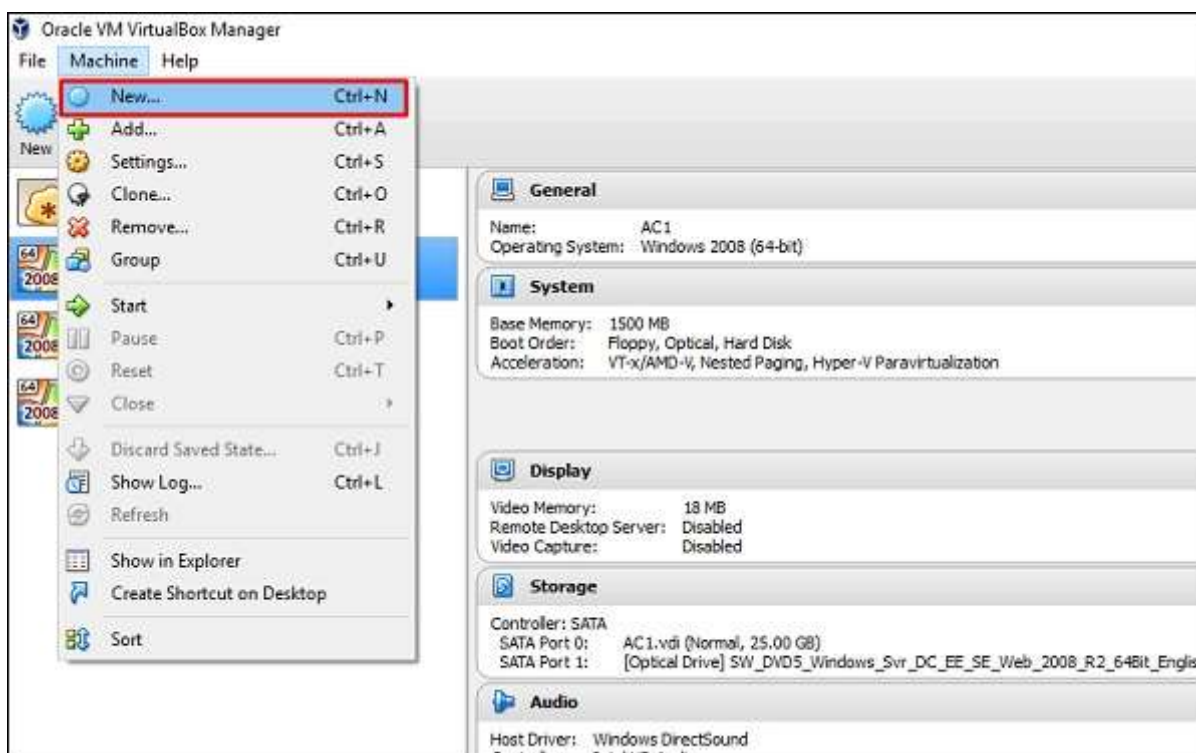
Now that we have successfully installed the Virtual Box, let's move on to the next step and install Kali Linux.

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

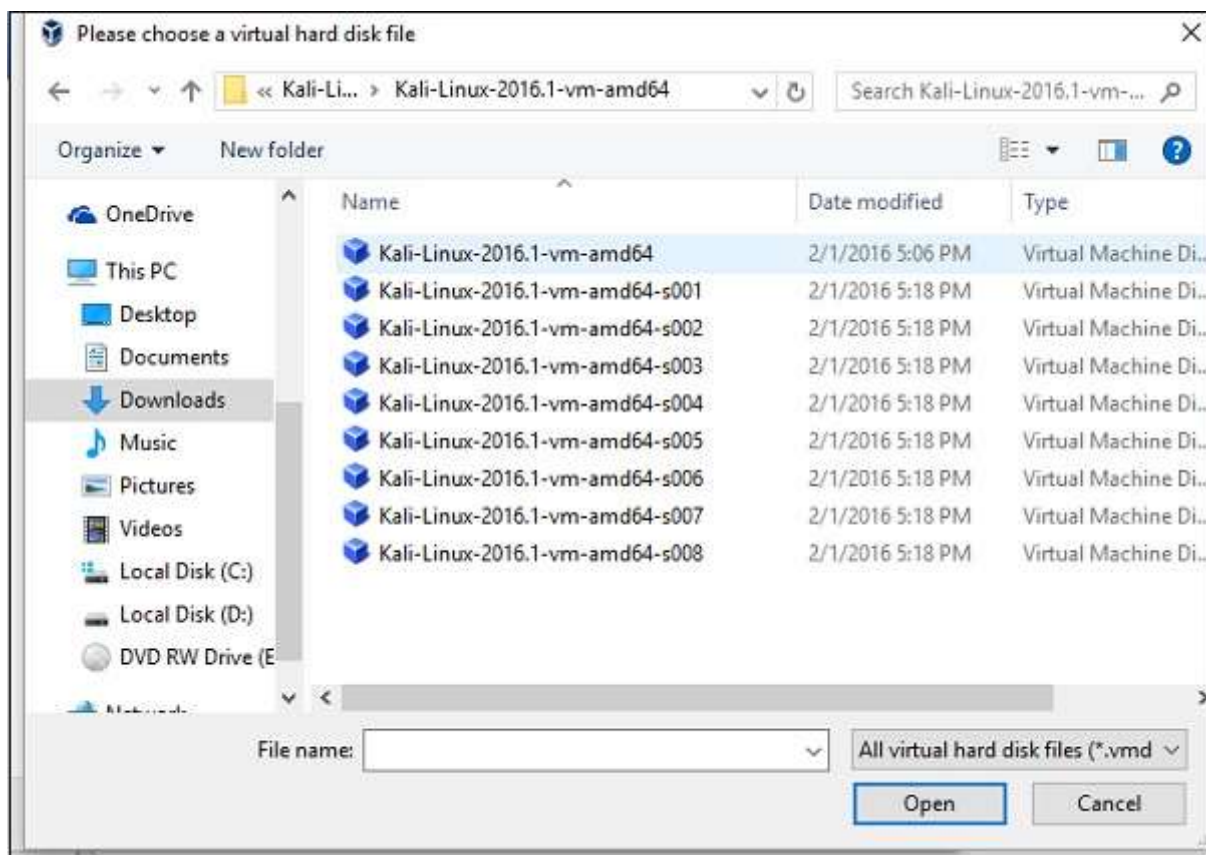


Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

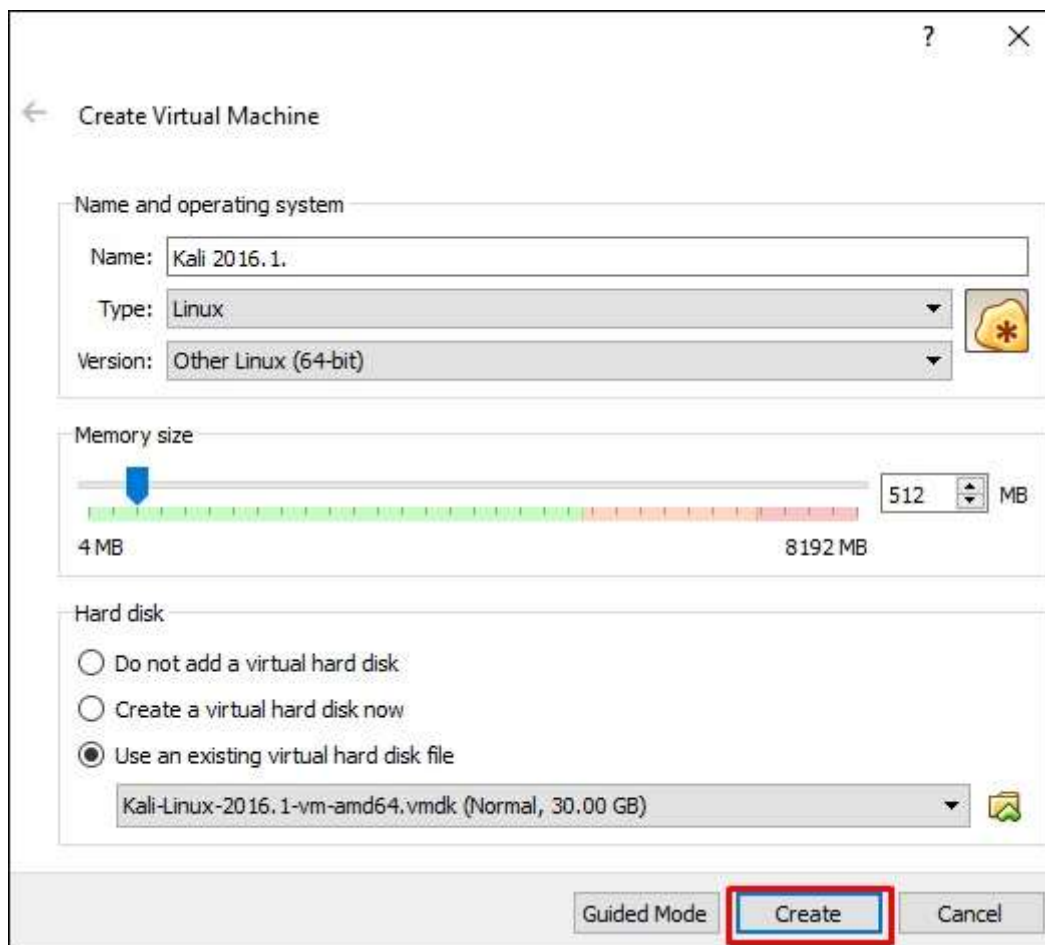
**Step 2** – Click **VirtualBox** → **New** as shown in the following screenshot.



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



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



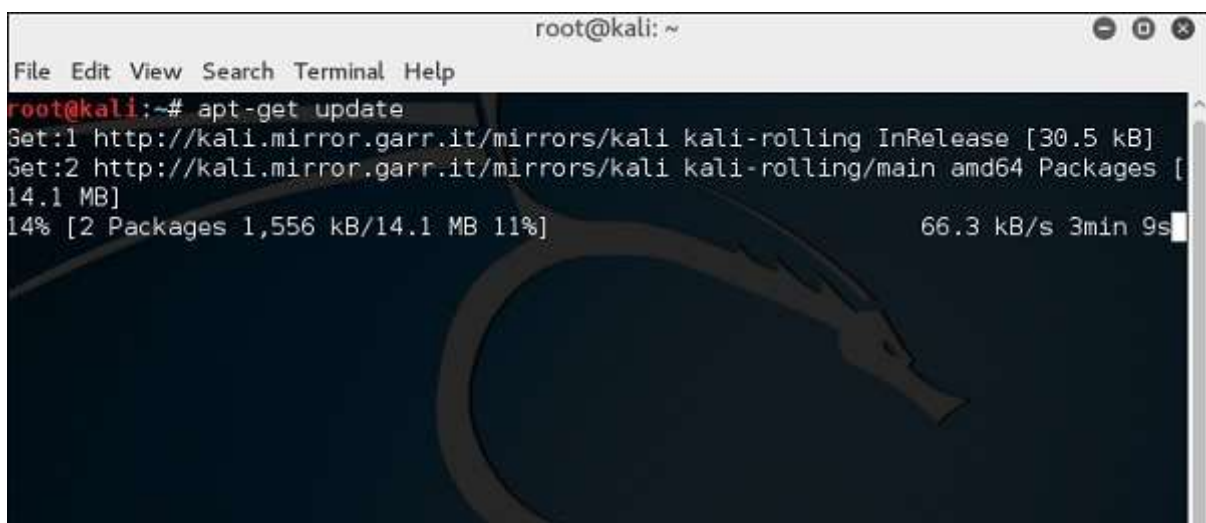
**Step 5** – Start Kali OS. The default username is **root** and the password is **toor**.



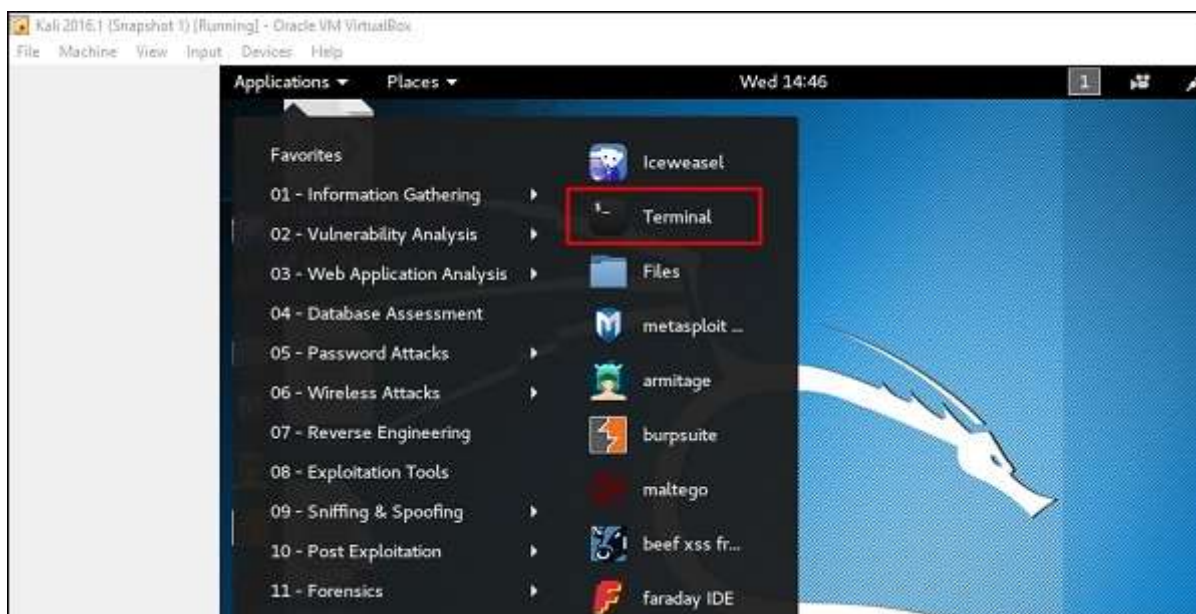
## Update Kali

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.

```

Applications ▾ Places ▾ Terminal ▾ Wed 14:56
root@kali: ~
File Edit View Search Terminal Help
Reading package lists... Done
root@kali:~#
root@kali:~#
root@kali:~# apt-get 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:
  castxml gccxml gdebi-core libasn1-8-heimdal libgssapi3-heimdal
  libhcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal
  libheimntlm0-heimdal libhx509-5-heimdal libkdc2-heimdal libkrb5-26-heimdal
  libntdb1 libroken18-heimdal libwind0-heimdal python-ctypeslib python-ecdsa
  python-ntdb python-pyatspi python-tidylib vlc-plugin-notify vlc-plugin-samba
Use 'apt autoremove' to remove them.
The following packages have been kept back:
  adwaita-icon-theme apktool backdoor-factory bind9-host binwalk bluez
  bluez-obexd bundler cadaver couchdb cpp cpp-5 cutycapt default-jdk
  default-jre default-jre-headless dnsutils dradis driftnet erlang-asn1
  erlang-base erlang-crypto erlang-eunit erlang-inets erlang-mnesia
  erlang-os-mon erlang-public-key erlang-runtime-tools erlang-snmp erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl evolution-data-server
  evolution-data-server-common file folks-common ftp g++ g++-5 gcc gcc-5
  gcc-5-base gdm3 gedit gedit-common ghostscript gir1.2-gdkpixbuf-2.0
  gir1.2-gnomedesktop-3.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
  gir1.2-launchpadlib-4.0 gir1.2-mutter-3.0 gir1.2-totem-1.0

```

**Step 3** – It will ask if you want to continue. Type “Y” and “Enter”.

```

zsh-common
1264 upgraded, 0 newly installed, 0 to remove and 480 not upgraded.
Need to get 955 MB of archives.
After this operation, 162 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

**Step 4** – To upgrade to a newer version of Operating System, type “**apt-get distupgrade**”.

```

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-evinced-3.0 girl.2-gtkbd-3.0
girl.2-packagekit-glib-1.0 girl.2-xkl-1.0 gnome-icon-theme-symbolic gnome-packagekit gnome-packagekit-data
gtk2-engines-gucharmap hwd-data libapache2-mod-php5 libasnl-8-heimdal libavcodec-ffmpeg56 libavdevice-ffmpeg56
libavfilter-ffmpeg56 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 libdataserver-1.2-21 libexporter-tiny-perl libfftw3-single3 libgdic-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 libical1 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-5.1-8 libphonon4 libpoppler57
libpostproc-ffmpeg53 libpth20 libqdbm14 libqmi-glib1 libquvi-scripts libquvi7 libradare2-0.9.9 libregfi8
libroken18-heimdal libsodium13 libswresample-ffmpeg1 libswscale-ffmpeg3 libtask-weak-perl libtre5 libtrio2
libusageenvironment1 libvp3 libwebp5 libwebpdemux1 libwebpmux1 libwebRTC-audio-processing-0 libwildmidi1

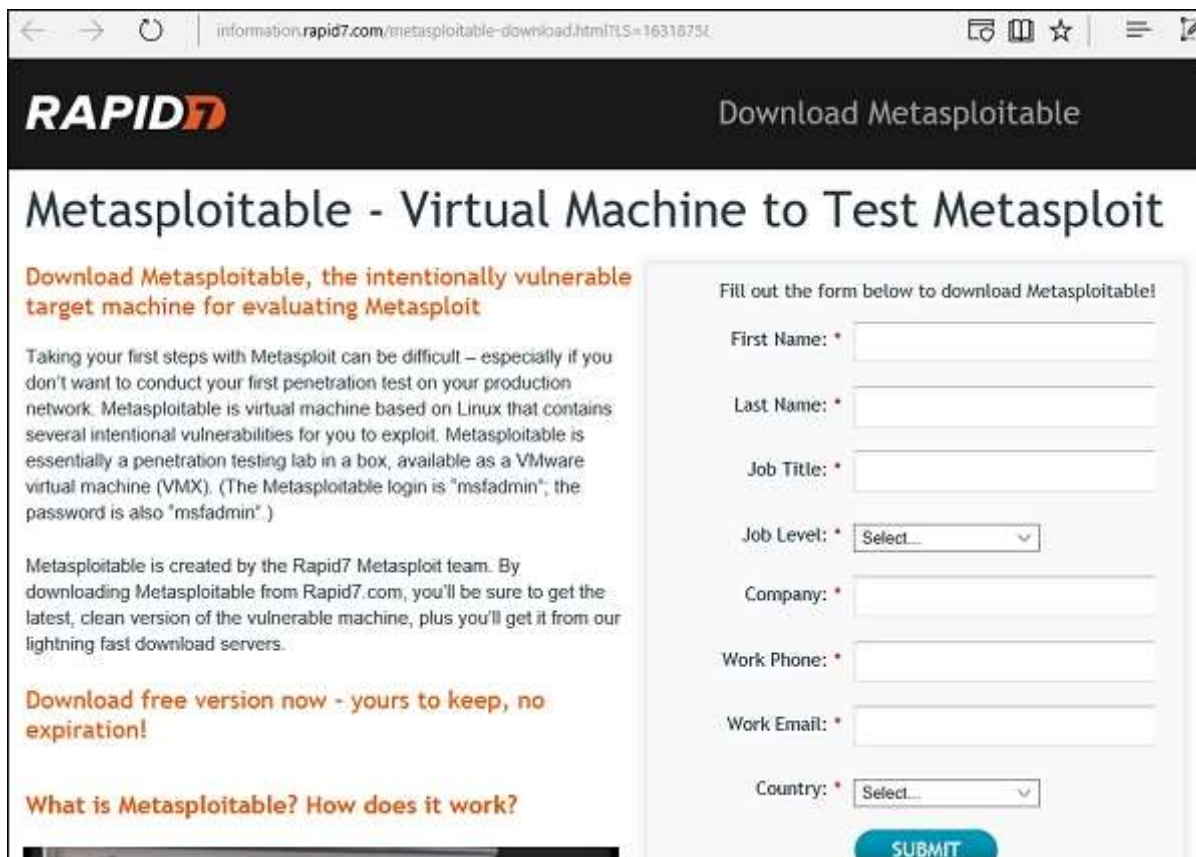
```

## 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/metasploitabledownload.html?LS=1631875&CS=web>





information:rapid7.com/metasploitable-download.html?LS=16316734

# RAPID7

## Download Metasploitable

### Metasploitable - Virtual Machine to Test Metasploit

**Download Metasploitable, the intentionally vulnerable target machine for evaluating Metasploit**

Taking your first steps with Metasploit can be difficult – especially if you don't want to conduct your first penetration test on your production network. Metasploitable is virtual machine based on Linux that contains several intentional vulnerabilities for you to exploit. Metasploitable is essentially a penetration testing lab in a box, available as a VMware virtual machine (VMX). (The Metasploitable login is "msfadmin", the password is also "msfadmin".)

Metasploitable is created by the Rapid7 Metasploit team. By downloading Metasploitable from Rapid7.com, you'll be sure to get the latest, clean version of the vulnerable machine, plus you'll get it from our lightning fast download servers.

**Download free version now - yours to keep, no expiration!**

**What is Metasploitable? How does it work?**

Fill out the form below to download Metasploitable!

First Name: \*

Last Name: \*

Job Title: \*

Job Level: \*

Company: \*

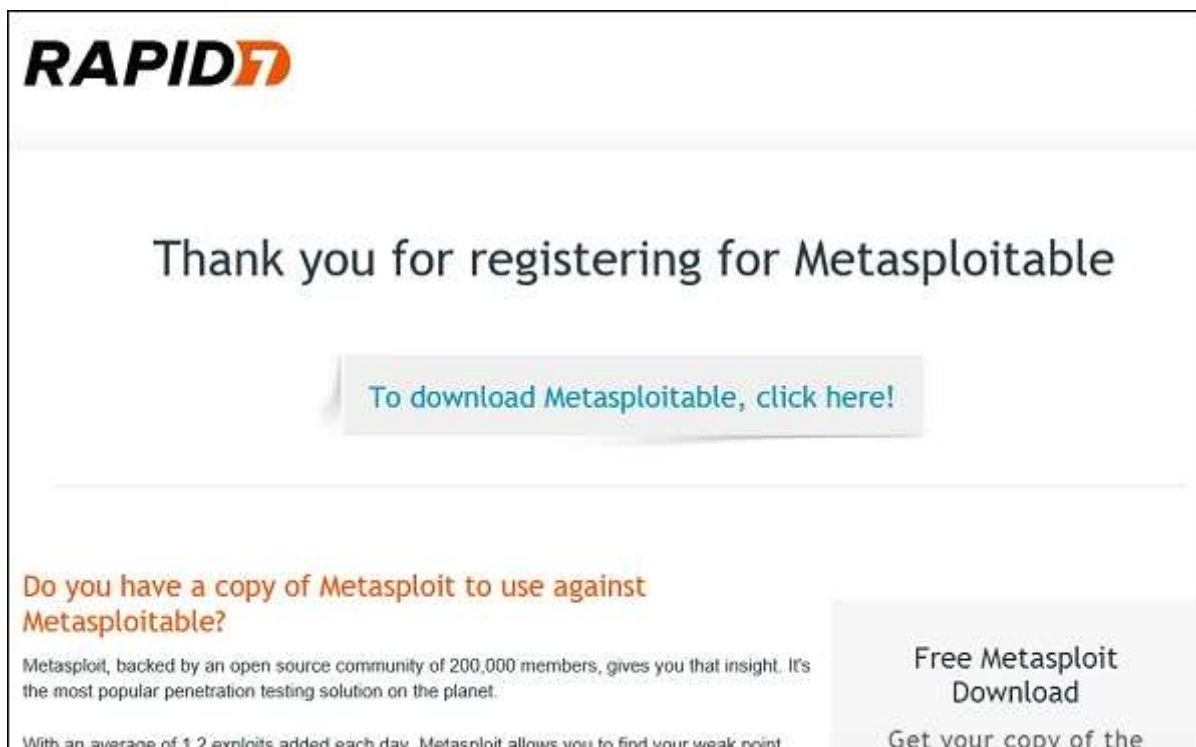
Work Phone: \*

Work Email: \*

Country: \*

**SUBMIT**

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



# RAPID7

## Thank you for registering for Metasploitable

**To download Metasploitable, click here!**

**Do you have a copy of Metasploit to use against Metasploitable?**

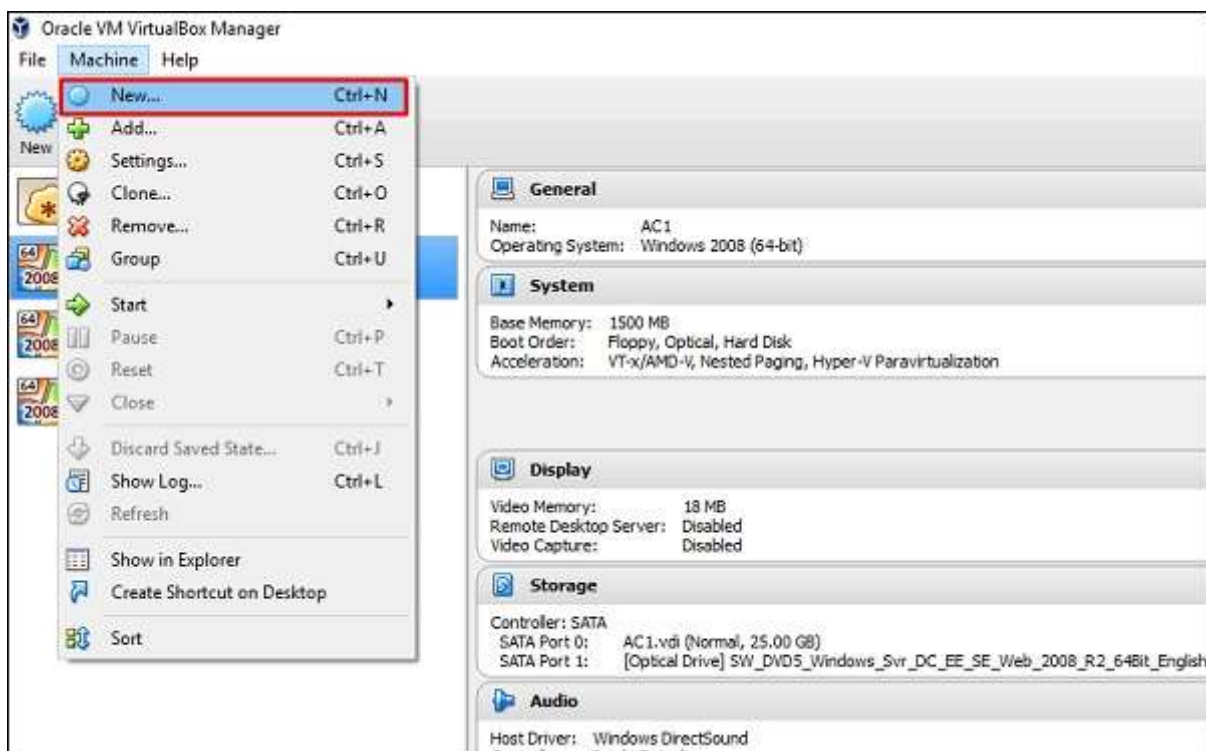
Metasploit, backed by an open source community of 200,000 members, gives you that insight. It's the most popular penetration testing solution on the planet.

With an average of 1.2 exploits added each day, Metasploit allows you to find your weak point.

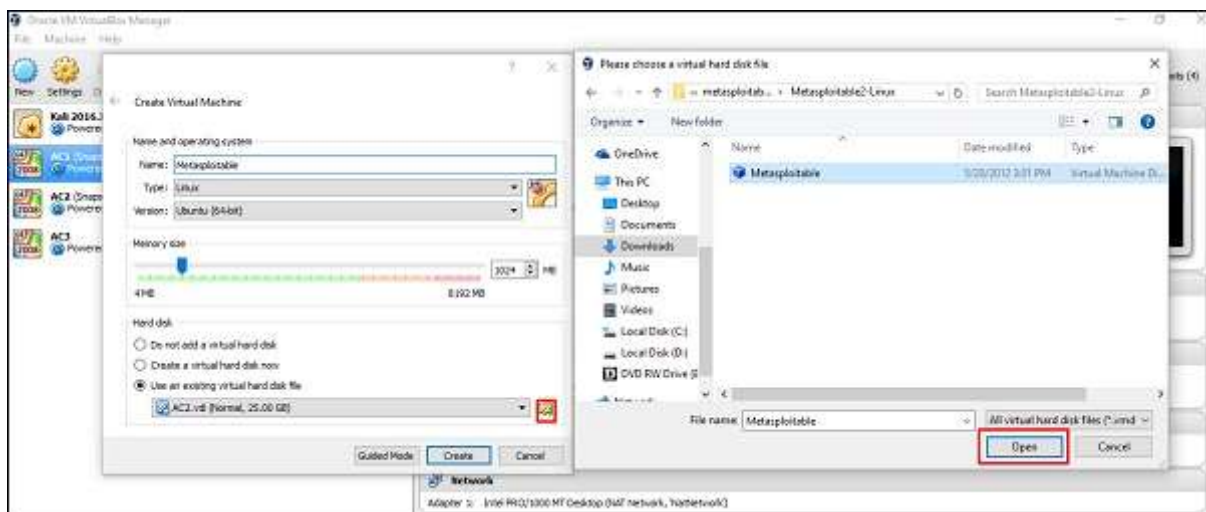
**Free Metasploit Download**

Get your copy of the

**Step 3** – Click **VirtualBox** → **New**.

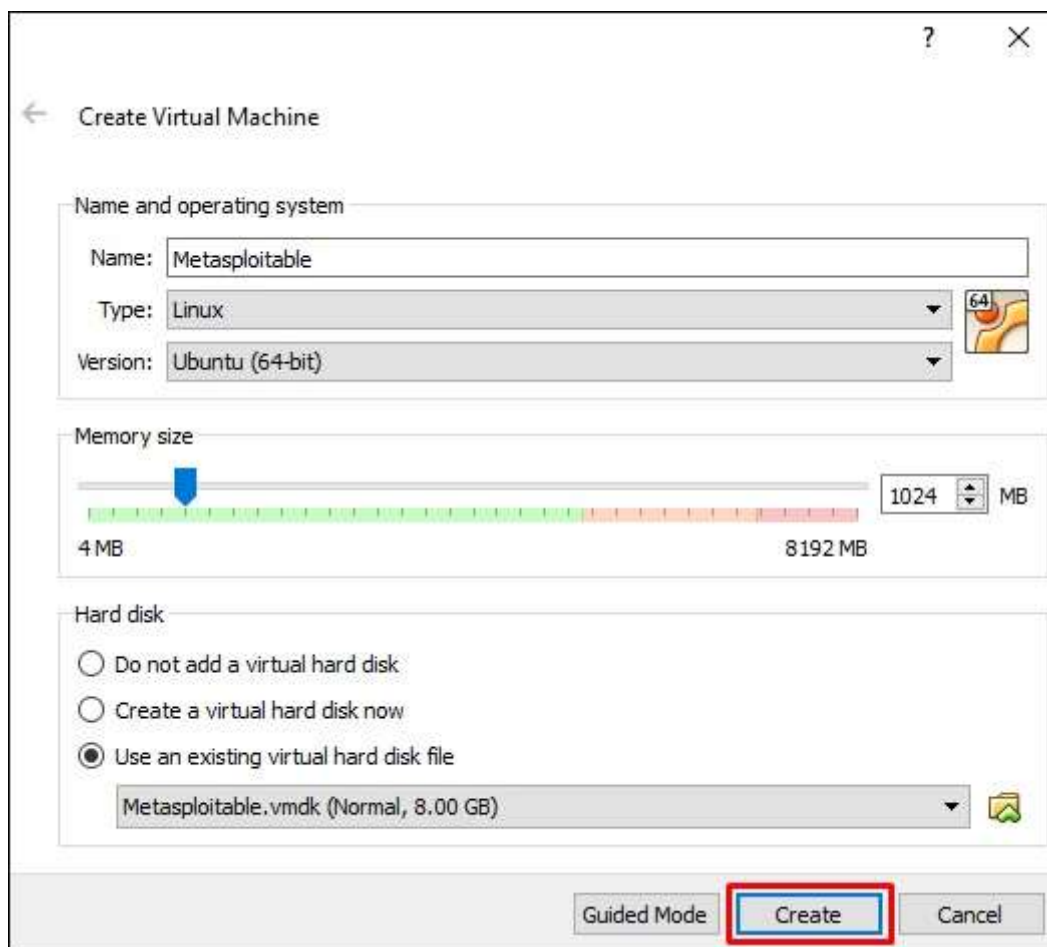


**Step 4** – Click “**Use an existing virtual hard disk file**”. Browse the file where you have downloaded **Metasploitable** and click **Open**.



**Step 5** – A screen to create a virtual machine pops up. Click “**Create**”.





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

