



Metasploit

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com



<https://www.facebook.com/tutorialspointindia>



<https://twitter.com/tutorialspoint>

About the Tutorial

Metasploit is one of the most powerful and widely used tools for penetration testing. In this tutorial, we will take you through the various concepts and techniques of Metasploit and explain how you can use them in a real-time environment. This tutorial is meant for instructional purpose only.

Audience

This tutorial is meant for beginners who would like to learn the basic-to-advanced concepts of Metasploit and how to use it in penetration testing to safeguard their systems and networks.

Prerequisites

Before proceeding with this tutorial, you should have a good grasp over all the fundamental concepts of a computer and how it operates in a networked environment.

Copyright & Disclaimer

© Copyright 2018 by Tutorials Point (I) Pvt. Ltd.

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

Table of Contents

About the Tutorial	i
Audience	i
Prerequisites	i
Copyright & Disclaimer	i
Table of Contents	ii
1. METASPLOIT – INTRODUCTION	1
2. METASPLOIT – ENVIRONMENT SETUP.....	2
Install Virtual Box	2
Install Kali Linux.....	6
3. METASPLOIT – BASIC COMMANDS	9
4. METASPLOIT – ARMITAGE GUI	13
5. METASPLOIT – PRO CONSOLE	15
6. METASPLOIT – VULNERABLE TARGET.....	17
7. METASPLOIT – DISCOVERY SCANS	20
8. METASPLOIT – TASK CHAINS	23
9. METASPLOIT – IMPORT DATA	26
10. METASPLOIT – VULNERABILITY SCAN.....	28
11. METASPLOIT – VULNERABILITY VALIDATION.....	30
12. METASPLOIT – EXPLOIT.....	35
13. METASPLOIT – PAYLOAD.....	39
14. METASPLOIT – CREDENTIAL	42

15. METASPLOIT – BRUTE-FORCE ATTACKS.....	45
16. METASPLOIT – PIVOTING	49
17. METASPLOIT – MAINTAINING ACCESS	53
18. METASPLOIT – METAMODULES.....	55
19. METASPLOIT – SOCIAL ENGINEERING.....	61
20. METASPLOIT – EXPORT DATA	67
21. METASPLOIT – REPORTS	71

1. Metasploit – Introduction

Metasploit is one of the most powerful tools used for penetration testing. Most of its resources can be found at: <https://www.metasploit.com>. It comes in two versions: commercial and free edition. There are no major differences in the two versions, so in this tutorial, we will be mostly using the Community version (free) of Metasploit.

As an Ethical Hacker, you will be using “Kali Distribution” which has the Metasploit community version embedded in it along with other ethical hacking tools. But if you want to install Metasploit as a separate tool, you can easily do so on systems that run on Linux, Windows, or Mac OS X.

The hardware requirements to install Metasploit are:

- 2 GHz+ processor
- 1 GB RAM available
- 1 GB+ available disk space

Metasploit can be used either with command prompt or with Web UI.

The recommended OS versions for Metasploit are:

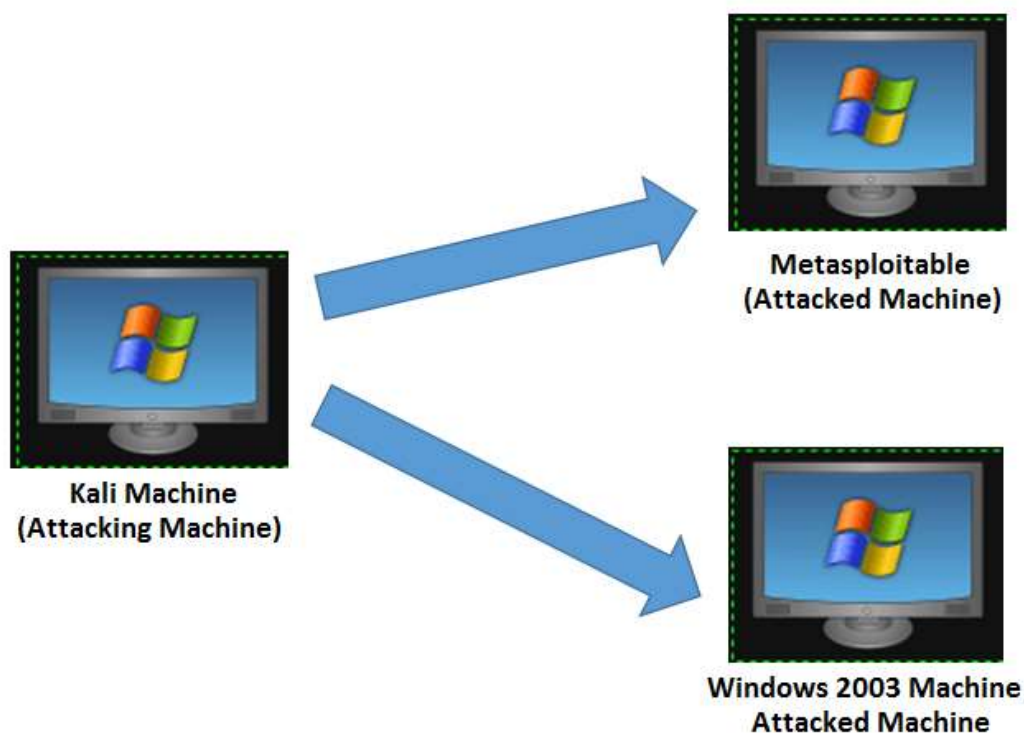
- Kali Linux 2.0 or Upper Versions
- Backtrack 3 and Upper Versions
- Red Hat Enterprise Linux Server 5.10+
- Red Hat Enterprise Linux Server 6.5+
- Red Hat Enterprise Linux Server 7.1+
- Ubuntu Linux 10.04 LTS
- Ubuntu Linux 12.04 LTS
- Ubuntu Linux 14.04 LTS
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7
- Windows 8.1

2. Metasploit – Environment Setup

We will take the following actions to set up our test environment:

- We will download Virtual box and install it.
- Download and install **Kali** distribution.
- Download and install **Metasploitable** which will be our hacking machine.
- Download and install Windows XP which will be another hacking machine.

In total, we will have 3 machines which will be logically connected in the same network.



Install Virtual Box

To download Virtual Box, go to <https://www.virtualbox.org/wiki/Downloads>

Select the appropriate version depending on your OS and the hardware configuration of your system.

VirtualBox

Download VirtualBox

Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

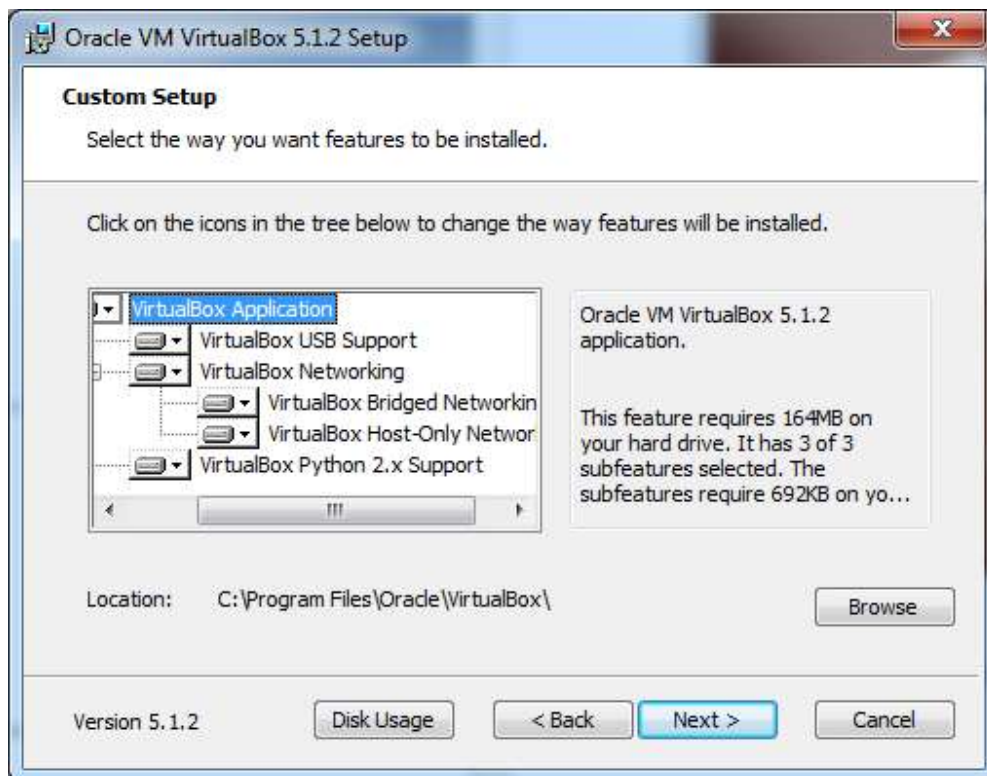
By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
 - **VirtualBox 5.1.2 for Windows hosts** → [x86/amd64](#)
 - **VirtualBox 5.1.2 for OS X hosts** → [amd64](#)
 - **VirtualBox 5.1.2 for Linux hosts** → [amd64](#)
 - **VirtualBox 5.1.2 for Solaris hosts** → [amd64](#)
- **VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack** → [All supported platforms](#)
Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP and PXE boot for Intel cards. See [this chapter from the User Manual](#) for an introduction. Extension Pack binaries are released under the [VirtualBox Personal Use and Evaluation License \(PUEL\)](#). Please install the extension pack with the same version as your installed version of VirtualBox:
If you are using **VirtualBox 5.0.26**, please download the extension pack → [here](#).
If you are using **VirtualBox 4.3.38**, please download the extension pack → [here](#).

After selecting the appropriate version of Virtual Box, the following screen will appear. Click **Next**.



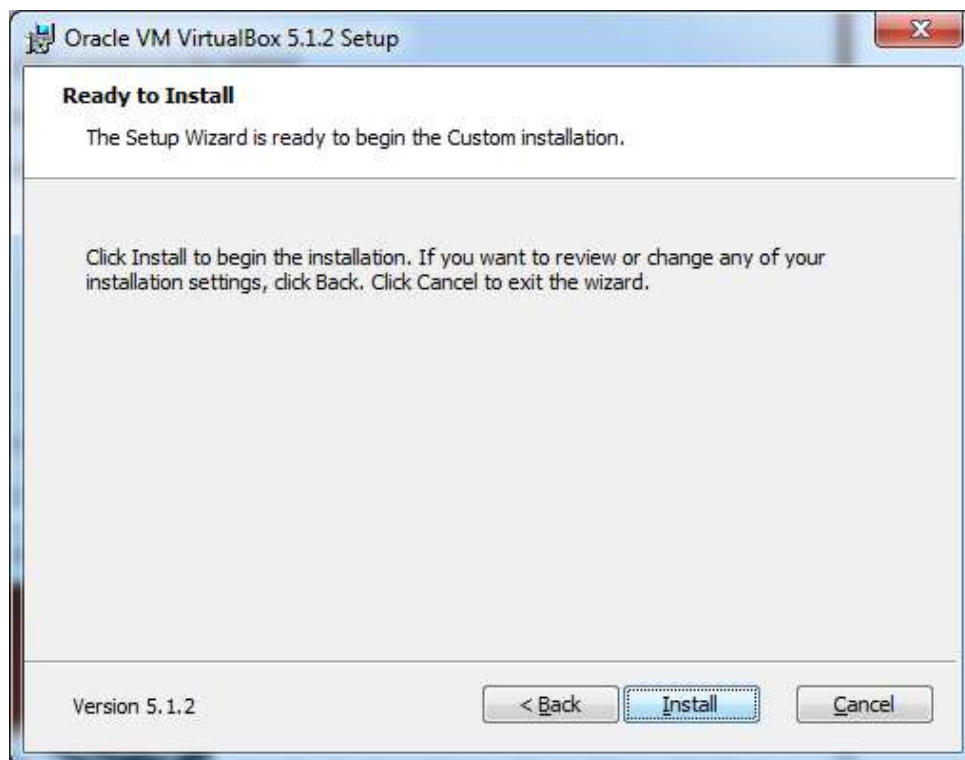
On the next screen, set the location where you want to install the application.



You will get a Warning message before proceeding with the installation.



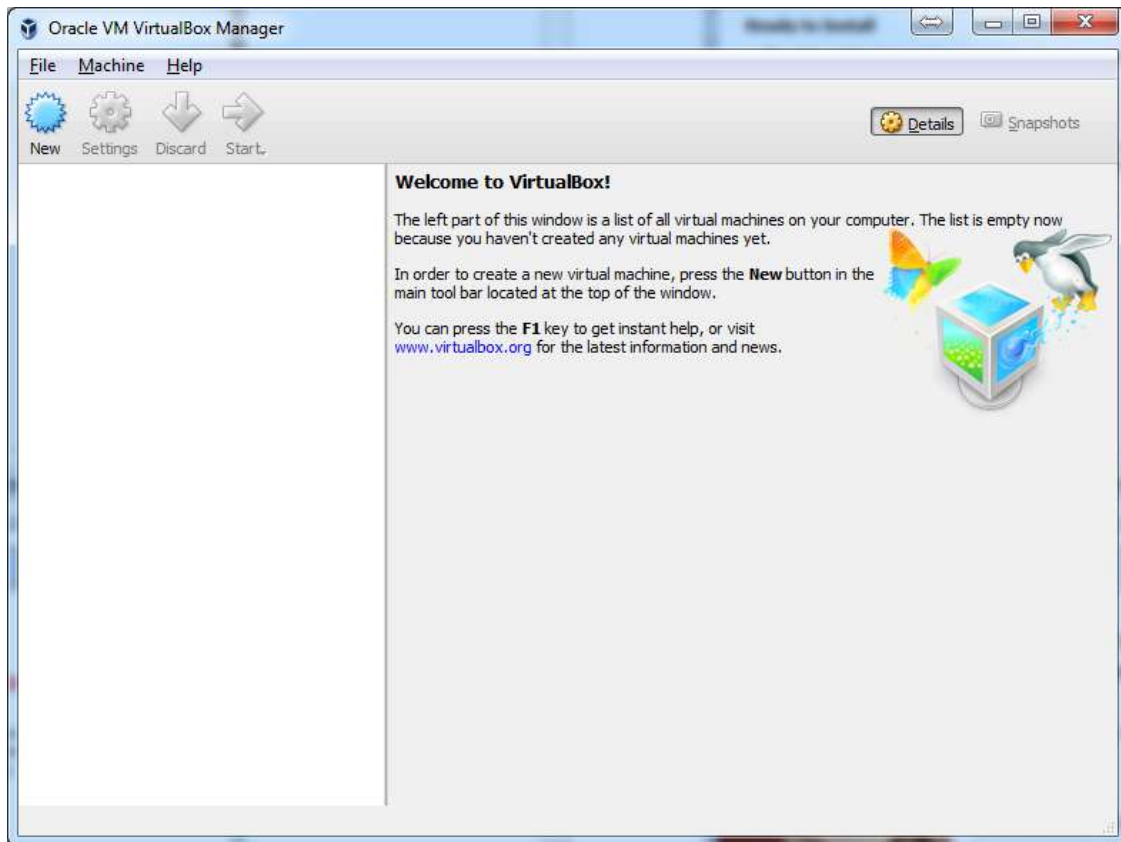
Click Yes on the above screen which will display the following screen. Click **Install** to begin the installation.



Once the installation is complete, you will get the following screen. Click **Finish** to exit the Setup Wizard.



Now, you will be greeted with the opening screen of VirtualBox.



Now we are ready to install the rest of the hosts for this tutorial.

Install Kali Linux

You can download Kali Linux from its official website: <https://www.kali.org/downloads/>

← → ↻ | offensive-security.com/kali-linux-vmware-virtualbox-image-download

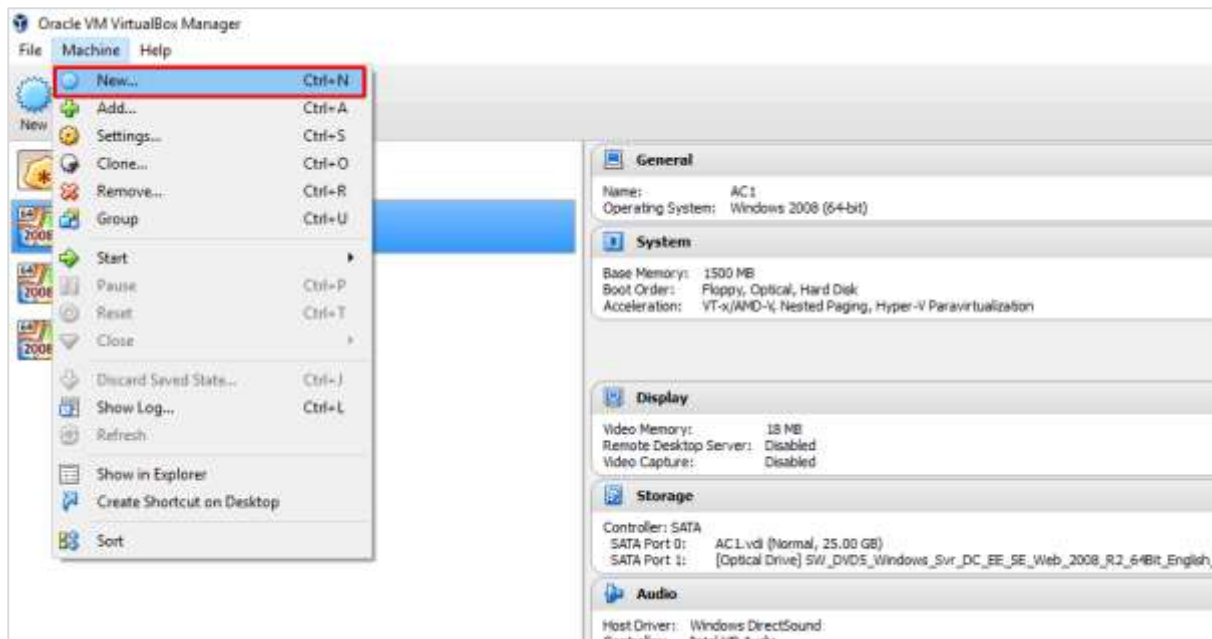
OFFENSIVE[®] security Blog Courses Certifications Online Labs

Prebuilt Kali Linux VMware Images Prebuilt Kali Linux VirtualBox Images

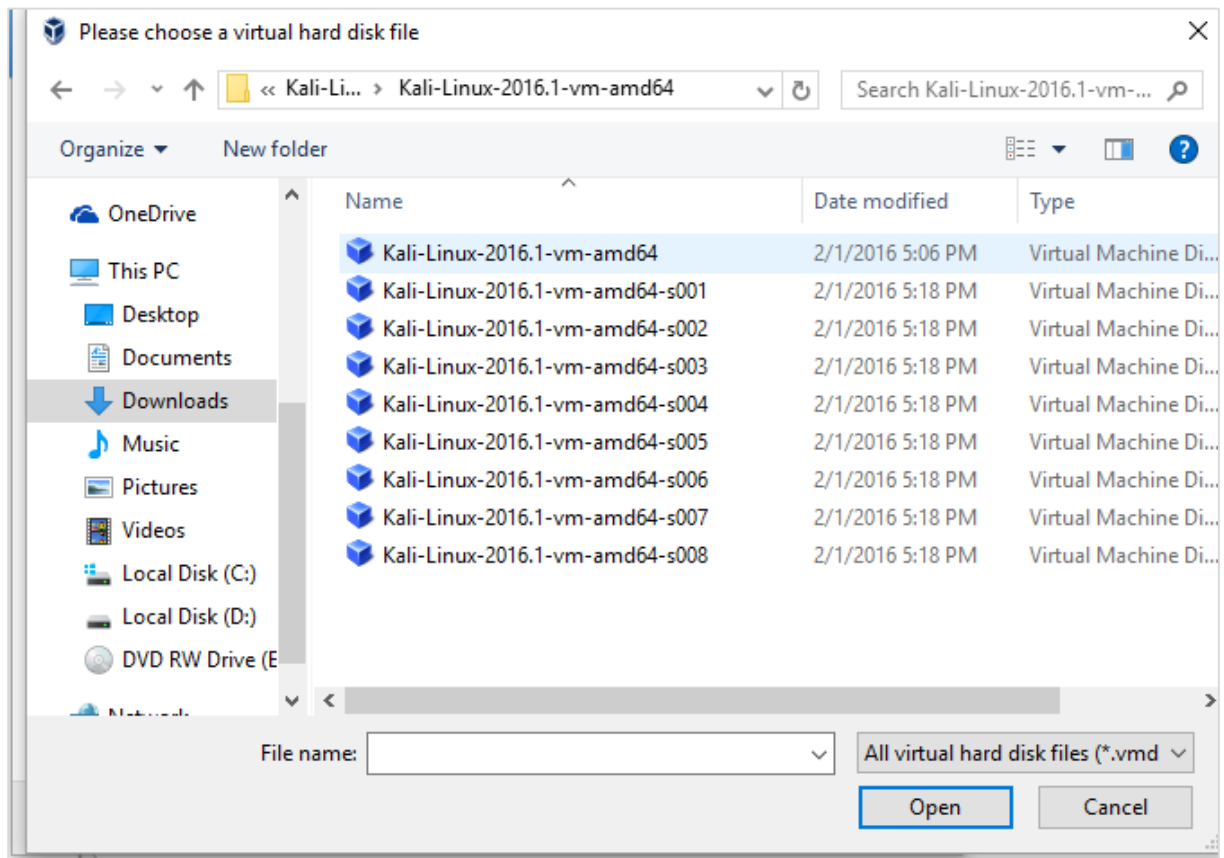
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

Go to the official website and download prebuilt Kali Linux VirtualBox images.

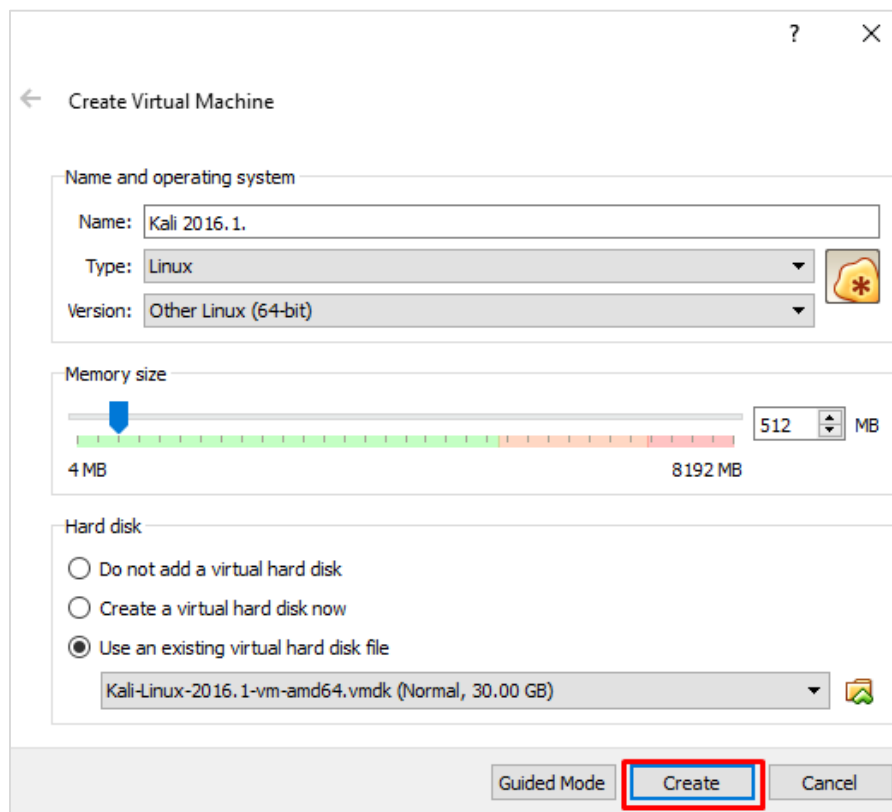
Next, open VirtualBox Manager and go to Machine -> New.



Go to the location where Kali Linux has been downloaded and choose a virtual hard disk file.



The next screen will prompt you to create a virtual machine. Click the **Create** button, as shown in the following screenshot.



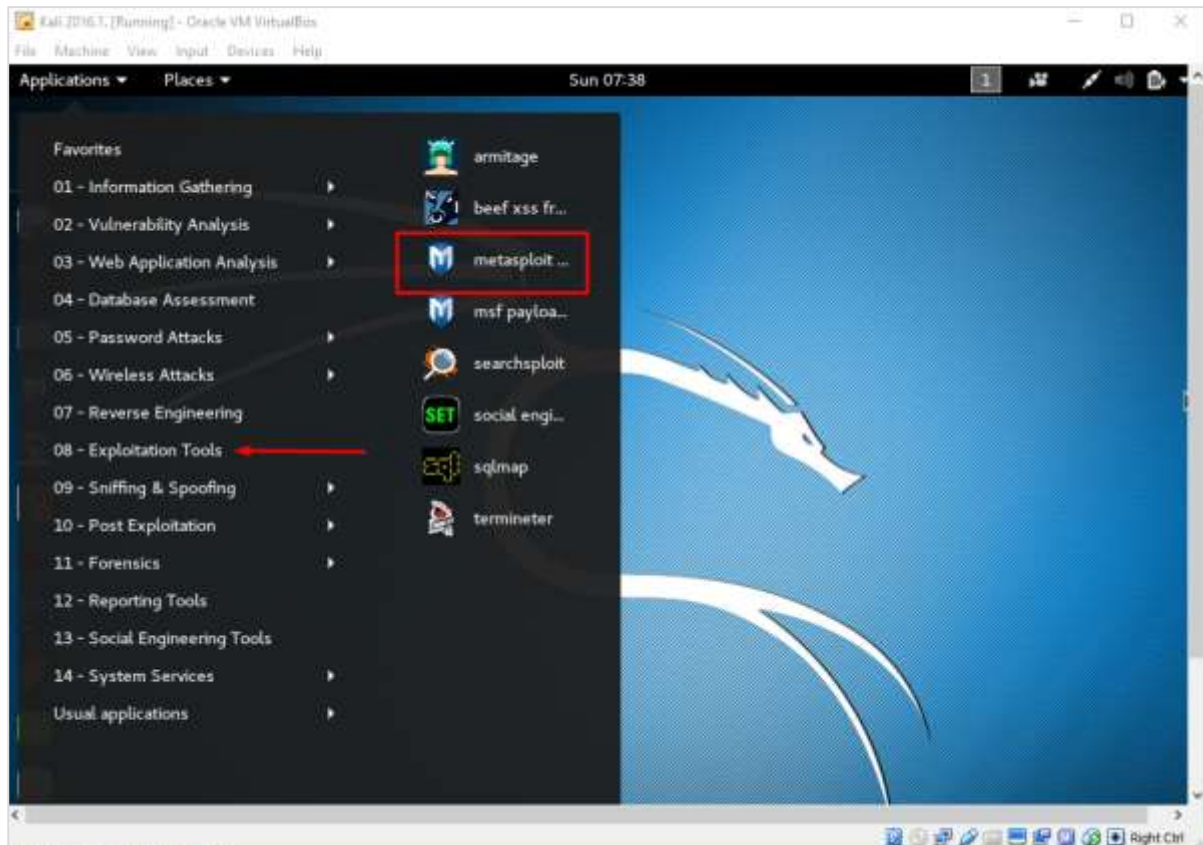
Now, you can start Kali OS. Your default username will be **root** and your password will be **toor**.



3. Metasploit – Basic Commands

In this chapter, we will discuss some basic commands that are frequently used in Metasploit.

First of all, open the Metasploit console in Kali. You can do so by following the path: Applications -> Exploitation Tools -> Metasploit.



Once you open the Metasploit console, you will get to see the following screen. Highlighted in red underline is the version of Metasploit.

```

Terminal
File Edit View Search Terminal Help
  .---.  ;@          @@ ;  .---.
  "  @@@@@"', '@@          @@@@@"', '@@@@@"
  '-. @@@@@@@@@@@@@@@@  @@@@@@@@@@@@@@@@@ @;
     \. @@@@@@@@@@@@@@@@  @@@@@@@@@@@@@@@@@'
      "  --'. @@@@  -.@      @  '-.  '---"
          | @@@@ @@@@      @
          | @@@ @@      @@
          \. @@@@      @@
           ', @@      @
           ( 3 C )      /|___ \ Metasploit!
           ;@' . ___ * '  \|--- \|
           '(. , .... "/

```

Easy phishing: Set up email templates, landing pages and listeners in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

```

      =[ metasploit v4.11.8- ]
+ -- --=[ 1519 exploits - 880 auxiliary - 259 post ]
+ -- --=[ 437 payloads - 38 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

Help Command

If you type the **help** command on the console, it will show you a list of core commands in Metasploit along with their description.

```

--==[ 437 payloads - 38 encoders - 8 nops ]
+ --==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > help

=====
Core Commands
=====

Command      Description
-----
?            Help menu
advanced     Displays advanced options for one or more modules
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
edit         Edit the current module with $VISUAL or $EDITOR
exit         Exit the console
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
info         Displays information about one or more modules
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
kill         Kill a job
load         Load a framework plugin
loadpath     Searches for and loads modules from a path

```

End of ebook preview
If you liked what you saw...
Buy it from our store @ **<https://store.tutorialspoint.com>**