Metasploit

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

Table of Contents

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

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

The recommended OS versions for Metasploit are:

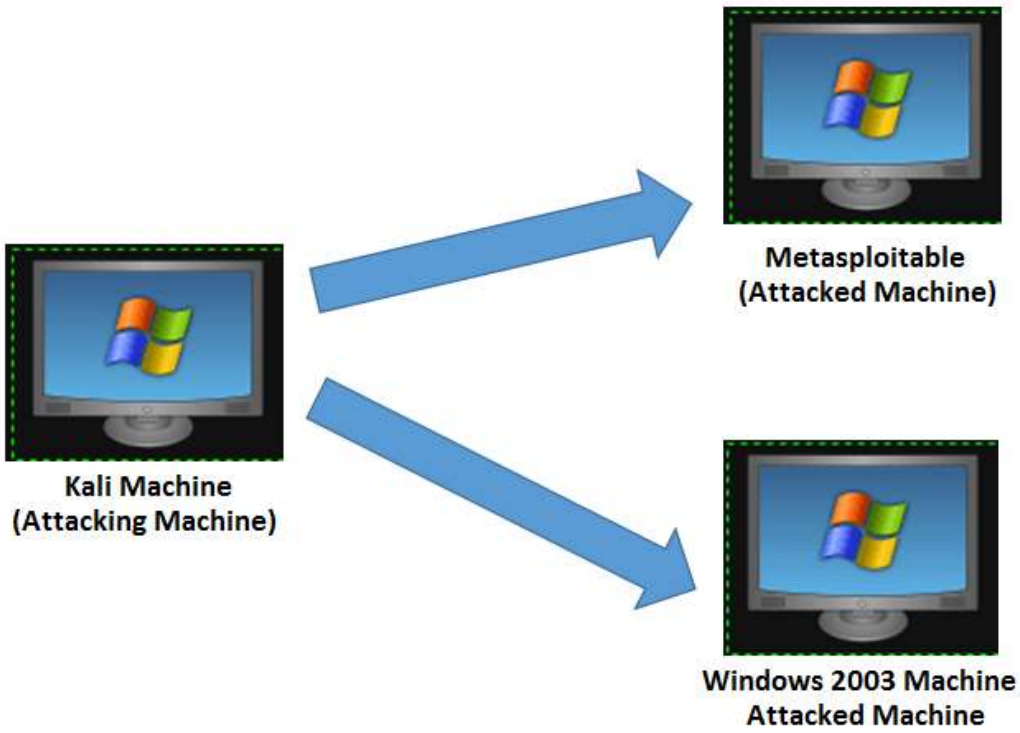
- Kali Linux 2.0 or Upper Versions
- Backtrack 3 and Upper Versions
- Red Hat Enterprise Linux Server 5.10+
- Red Hat Enterprise Linux Server 6.5+
- Red Hat Enterprise Linux Server 7.1+
- Ubuntu Linux 10.04 LTS
- Ubuntu Linux 12.04 LTS
- Ubuntu Linux 14.04 LTS
- Windows Server 2008 R2
- Windows Server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



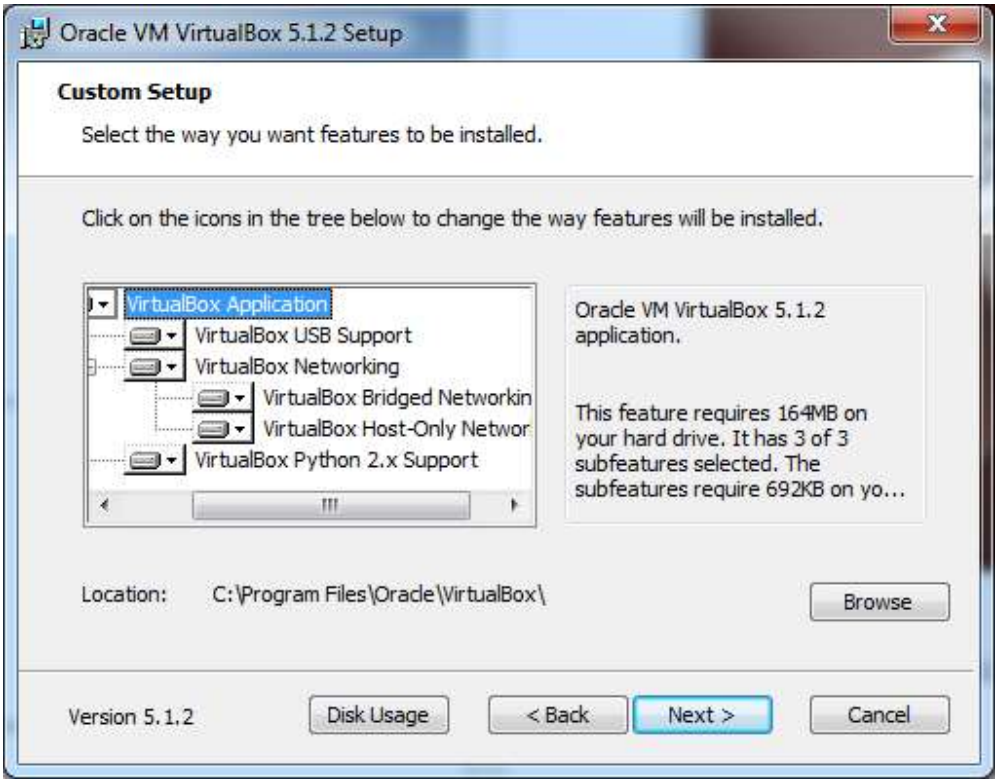
Install Virtual Box

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.

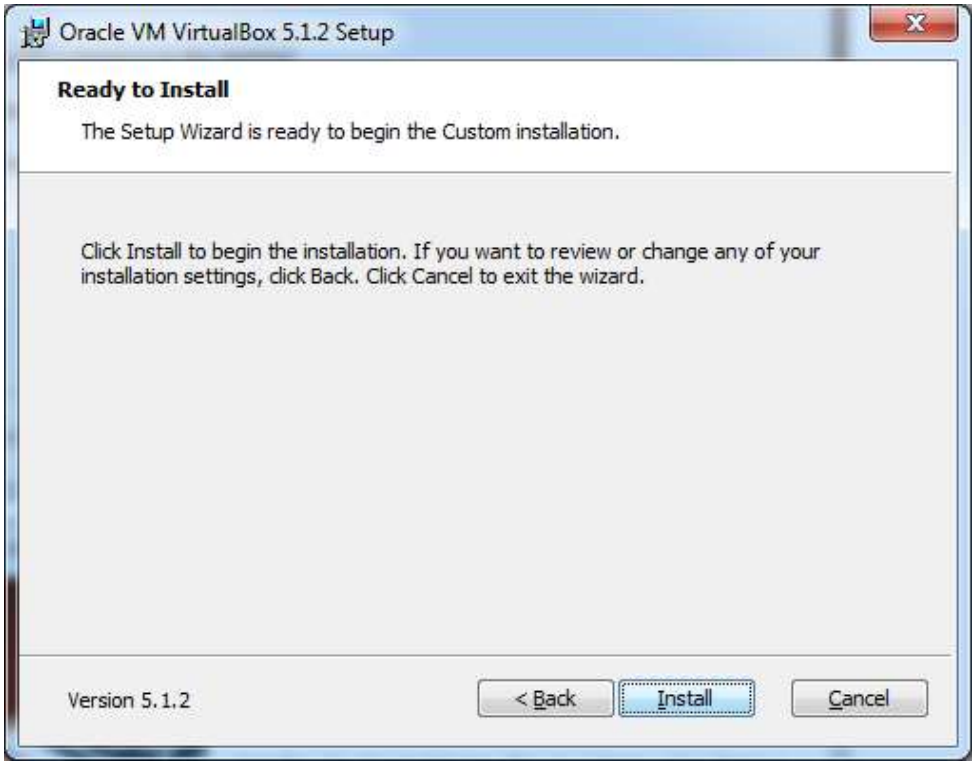
After selecting the appropriate version of Virtual Box, the following screen will appear. Click **Next**.

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



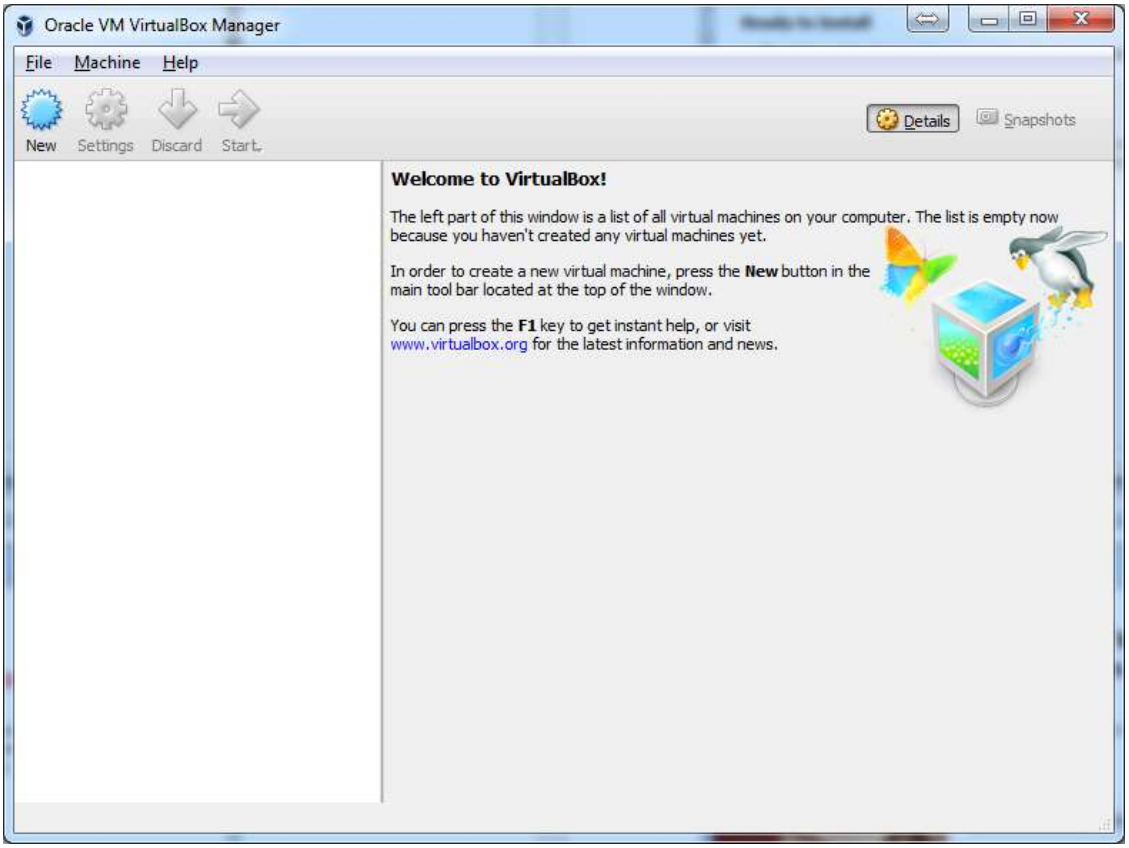
You will get a Warning message before proceeding with the installation.

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.

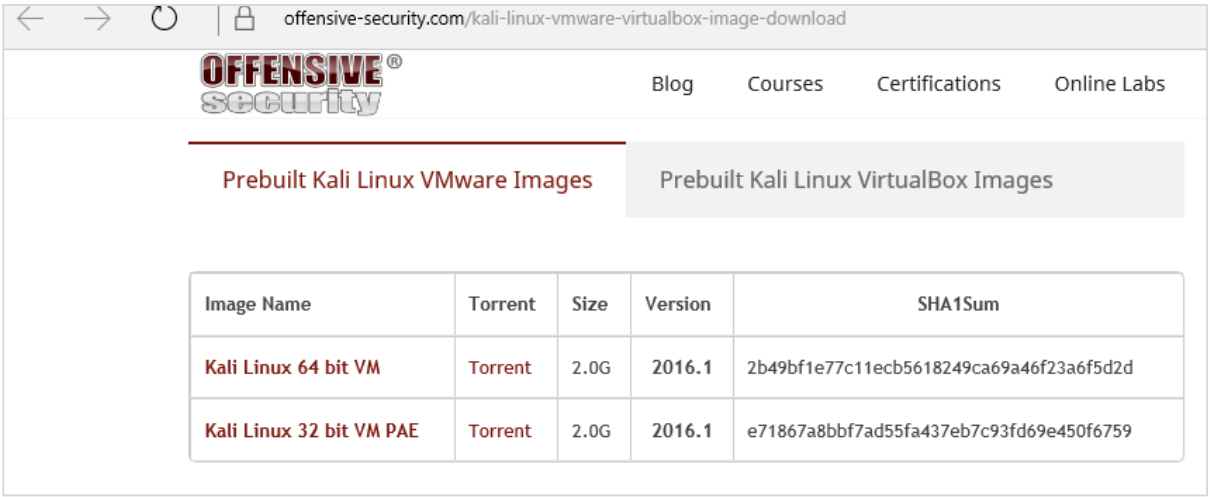
Now, you will be greeted with the opening screen of VirtualBox.



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

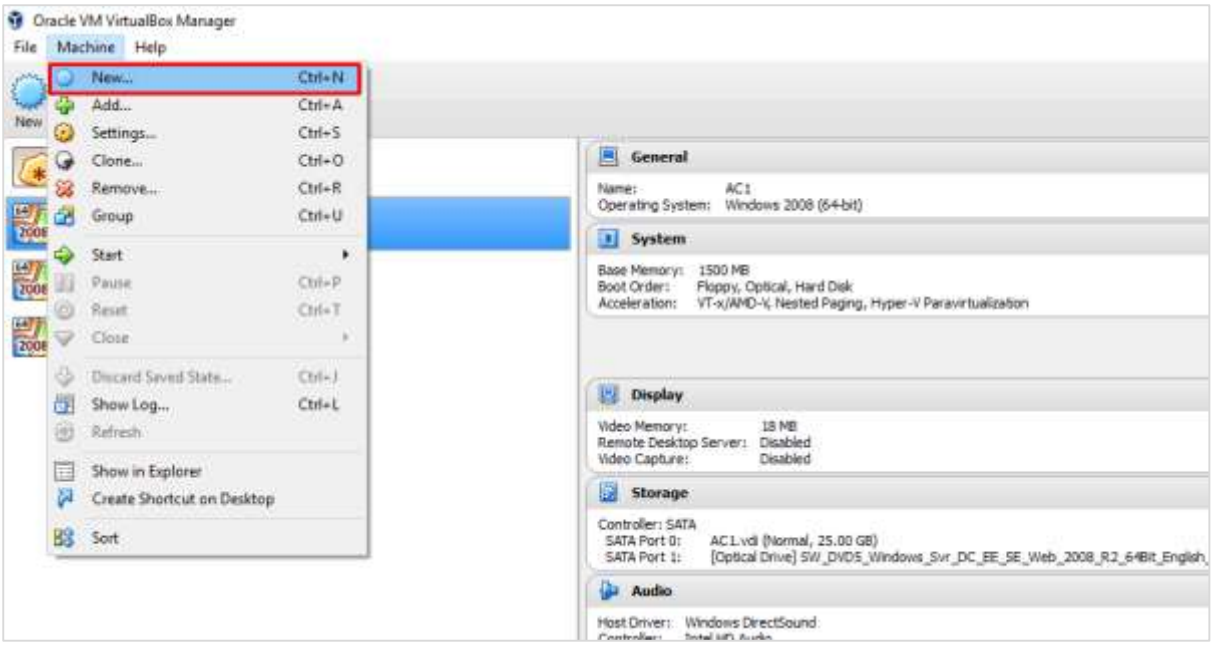
Install Kali Linux

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

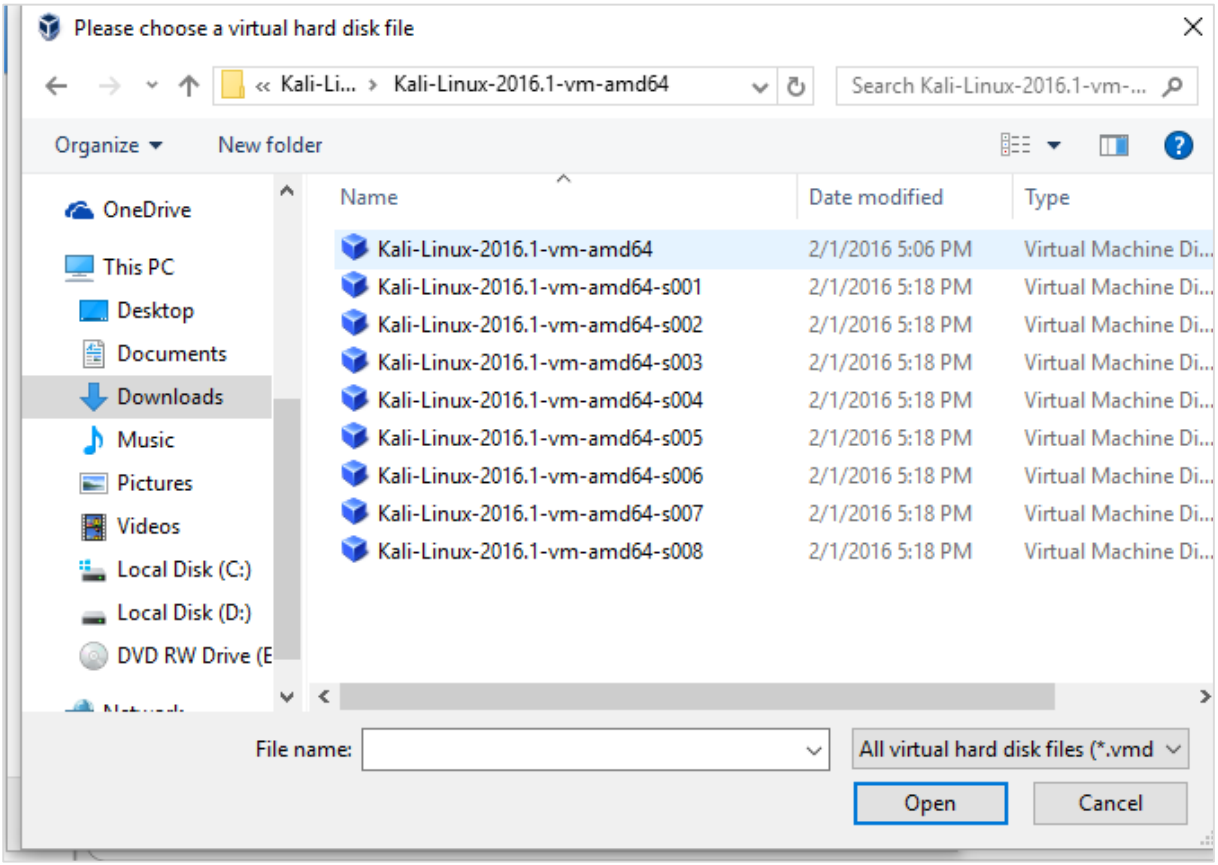


Go to the official website and download prebuilt Kali Linux VirtualBox images.

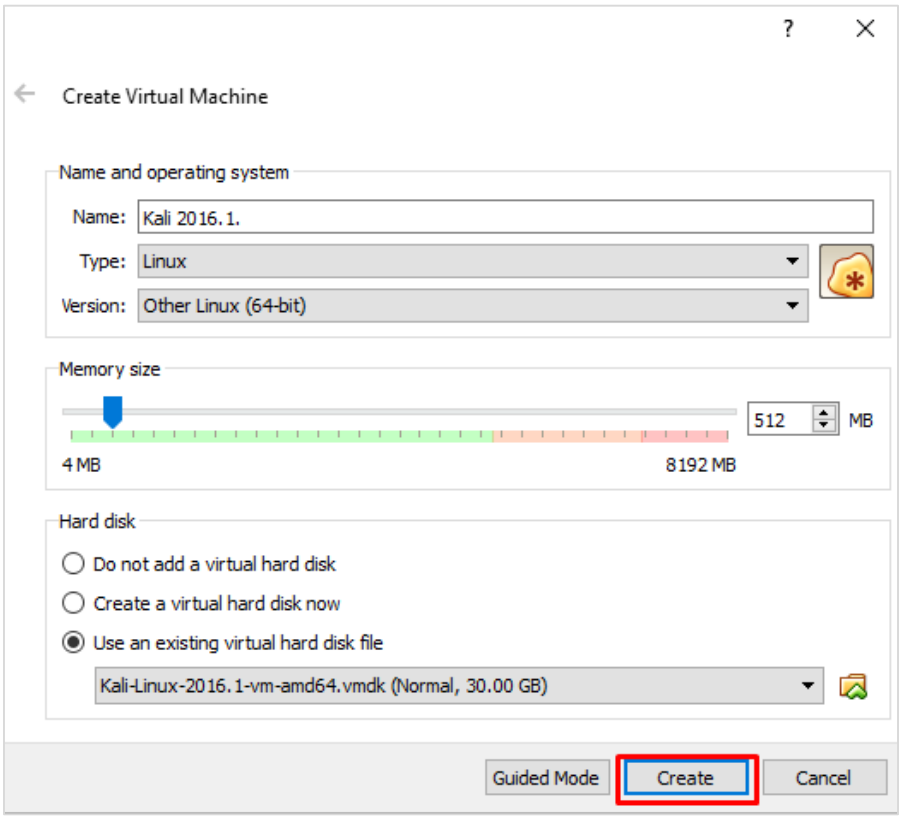
Next, open VirtualBox Manager and go to Machine -> New.



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.

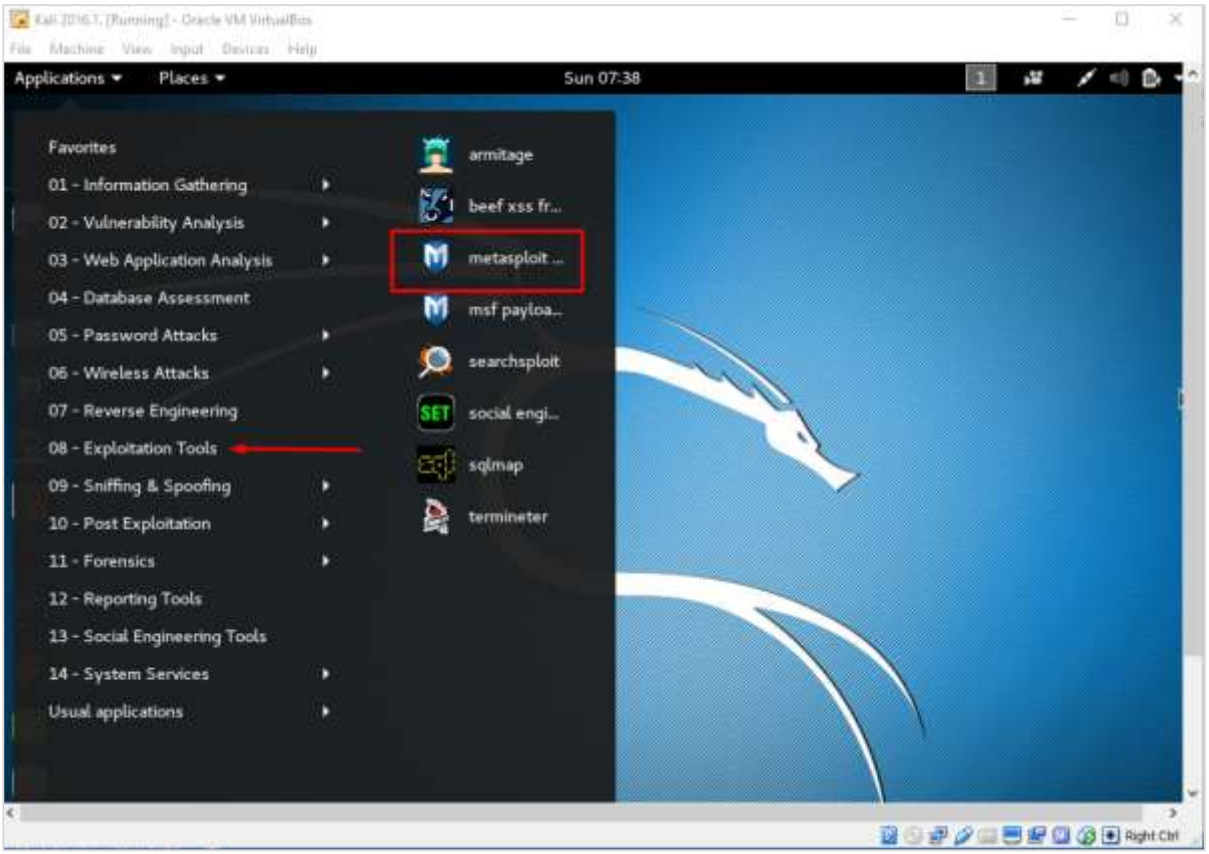


Now, you can start Kali OS. Your default username will be **root** and your password will be **toor**.

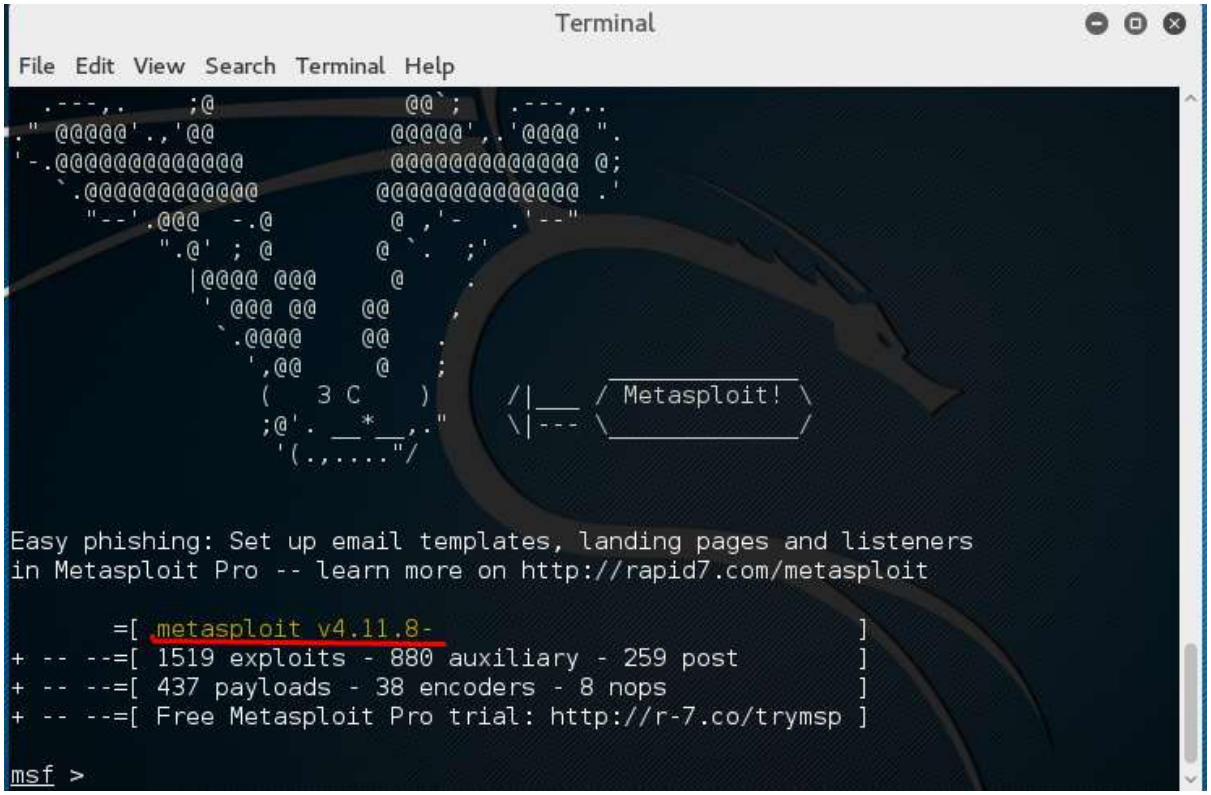
3. Metasploit – Basic Commands

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.



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.