



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

© 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. KALI LINUX – INSTALLATION & CONFIGURATION	1
Download and Install the Virtual Box	1
Install Kali Linux.....	6
Update Kali.....	8
Laboratory Setup.....	10
2. KALI LINUX – INFORMATION GATHERING TOOLS	14
NMAP and ZenMAP	14
Stealth Scan.....	16
Searchsploit.....	18
DNS Tools	19
LBD Tools.....	21
Hping3	21
3. KALI LINUX – VULNERABILITY ANALYSES TOOLS	23
Cisco Tools.....	23
Cisco Auditing Tool	24
Cisco Global Exploiter	25
BED.....	26

4.	KALI LINUX – WIRELESS ATTACKS	27
	Fern Wifi Cracker	27
	Kismet	32
	GISKismet	36
	Ghost Phisher	39
	Wifite	40
5.	KALI LINUX – WEBSITE PENETRATION TESTING.....	43
	Vega Usage	43
	ZapProxy	48
	Database Tools Usage.....	51
	CMS Scanning Tools.....	54
	SSL Scanning Tools.....	57
	w3af	59
6.	KALI LINUX – EXPLOITATION TOOLS	61
	Metasploit.....	61
	Armitage	64
	BeEF	66
	Linux Exploit Suggester.....	69
7.	KALI LINUX – FORENSICS TOOLS.....	70
	p0f.....	70
	pdf-parser.....	71
	Dumpzilla	72
	DFF	73

8.	KALI LINUX – SOCIAL ENGINEERING	76
	Social Engineering Toolkit Usage	76
9.	KALI LINUX – STRESSING TOOLS	82
	Slowhttptest.....	82
	Inviteflood	84
	laxflood	85
	thc-ssl-dos	86
10.	KALI LINUX – SNIFFING & SPOOFING	87
	Burpsuite.....	87
	mitmproxy.....	90
	Wireshark.....	91
	sslstrip	93
11.	KALI LINUX – PASSWORD CRACKING TOOLS	95
	Hydra.....	95
	Johnny.....	97
	john	99
	Rainbowcrack	100
	SQLdict	100
	hash-identifier	101
12.	KALI LINUX – MAINTAINING ACCESS	102
	Powersploit	102
	Sbd	103
	Webshells.....	104
	Weevely	104
	http-tunnel.....	106

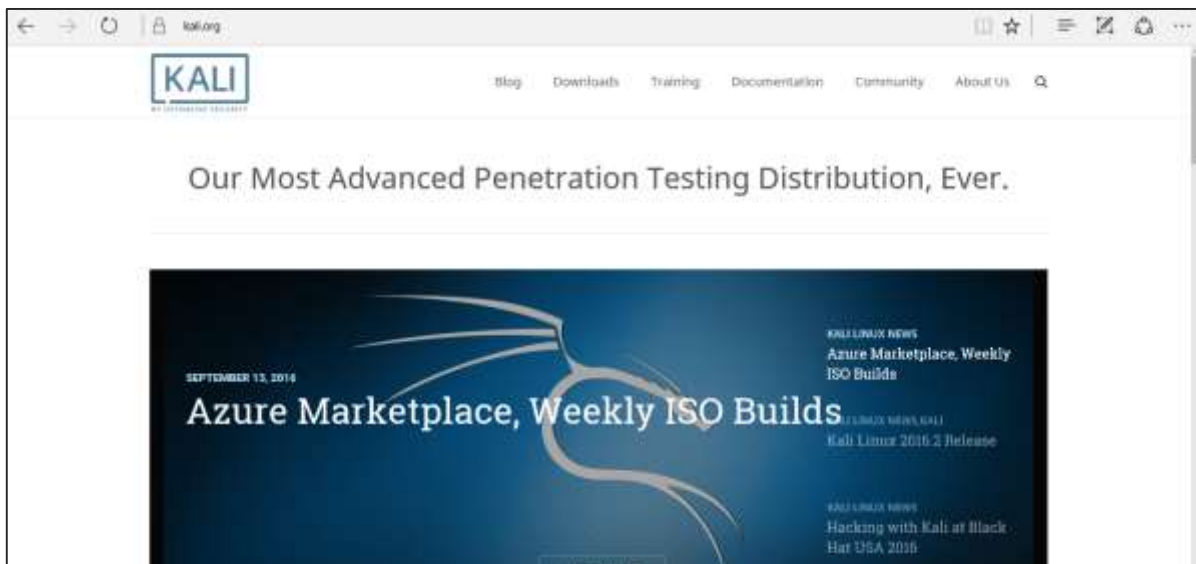
	dns2tcp.....	106
	cryptcat	107
13.	KALI LINUX – REVERSE ENGINEERING.....	108
	OllyDbg.....	108
	dex2jar	109
	jd-gui	110
	apktool.....	111
14.	KALI LINUX – REPORTING TOOLS.....	112
	Dradis	112
	Metagoofil.....	114

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.

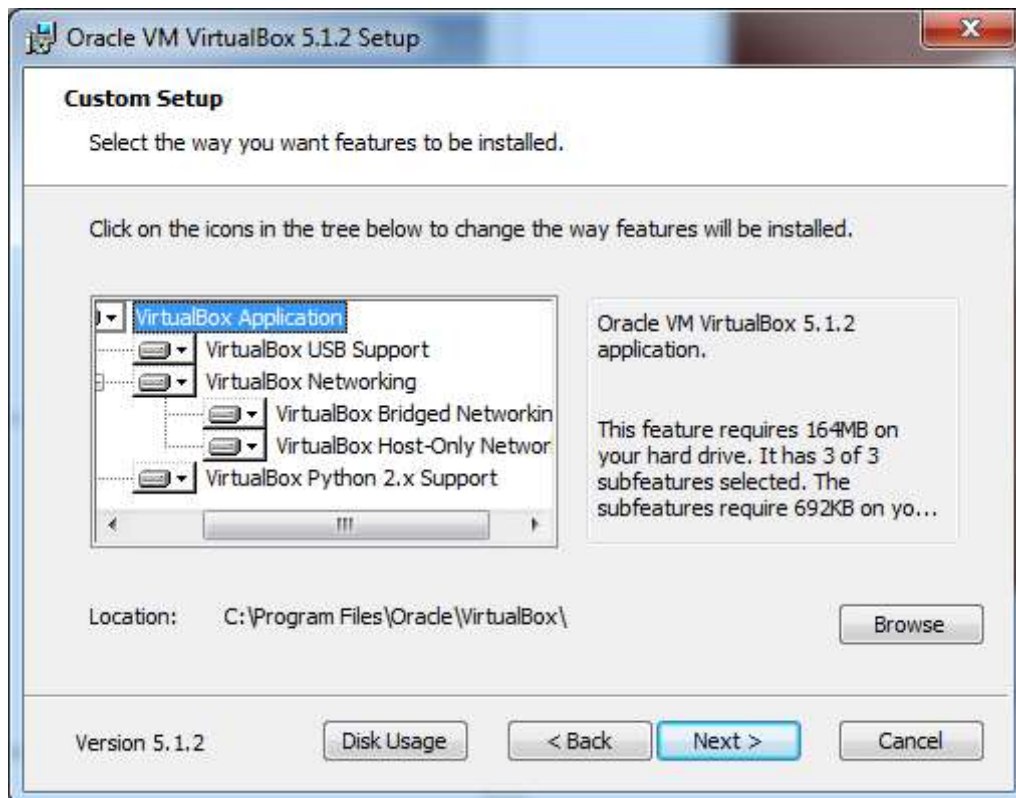


The screenshot shows the 'VirtualBox Download VirtualBox' page. It features a blue header with the 'VirtualBox' logo. Below the header, there is a section titled 'Download VirtualBox' with a sub-section 'VirtualBox binaries'. A red box highlights the first bullet point: 'VirtualBox platform packages. The binaries are released under the terms of the GPL version 2.' Under this, there are four sub-bullets: 'VirtualBox 5.1.2 for Windows hosts', 'VirtualBox 5.1.2 for OS X hosts', 'VirtualBox 5.1.2 for Linux hosts', and 'VirtualBox 5.1.2 for Solaris hosts'. Below this, there is a section for 'VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack' with additional text and links.

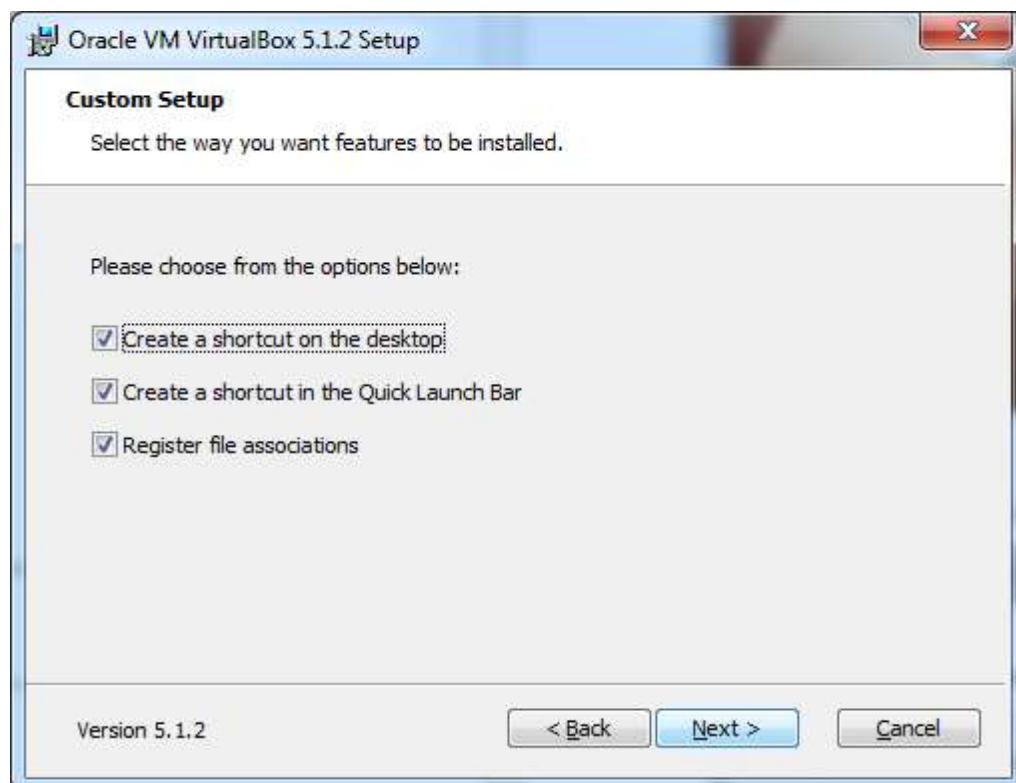
Step 2: Click **Next**.



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**.



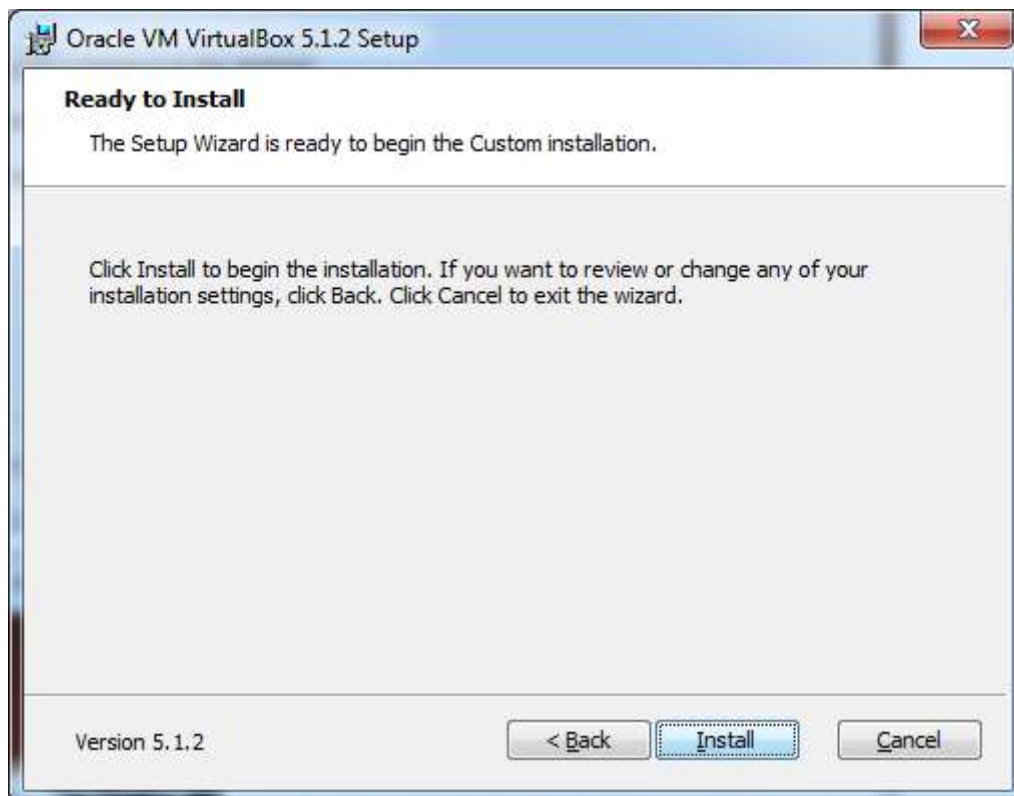
Step 4: Click **Next** and the following **Custom Setup** screenshot pops up. Select the features you want to be installed and click Next.



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



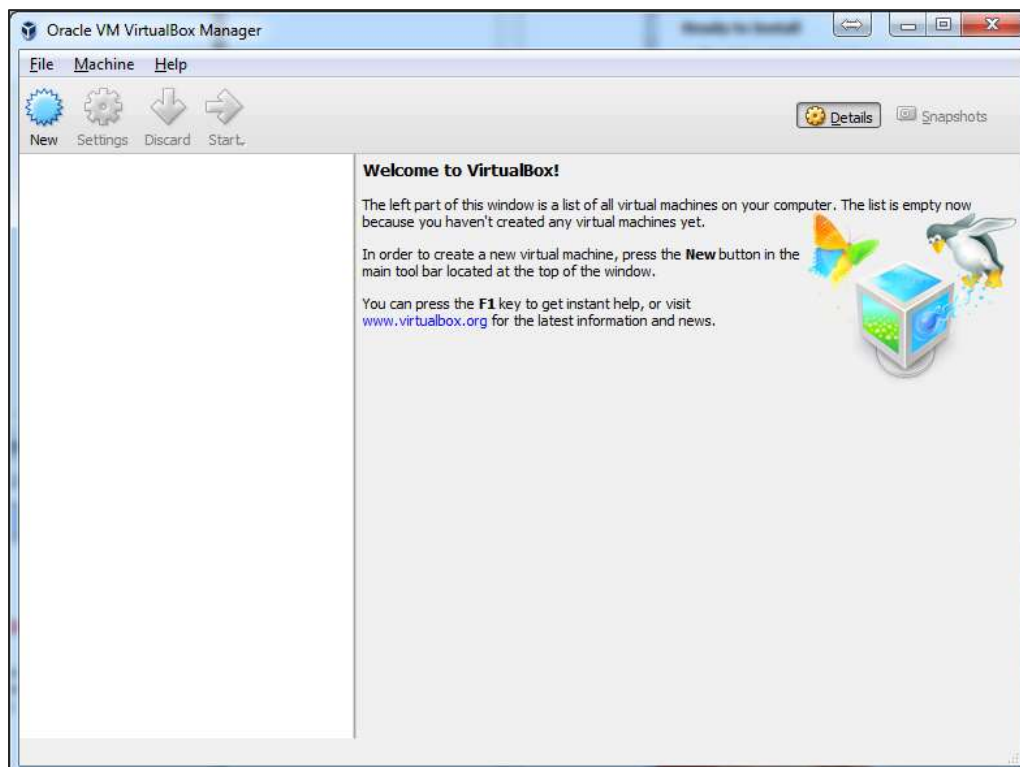
Step 6: The **Ready to Install** screen pops up. Click Install.



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.

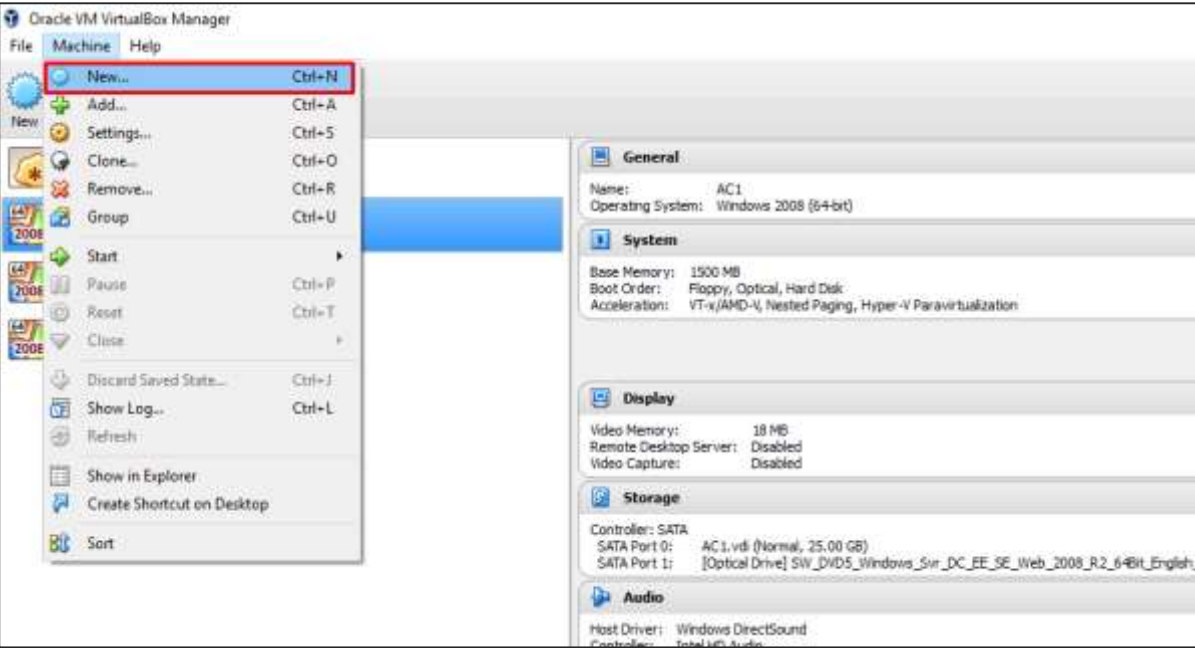
Step 1: Download the Kali Linux package from its official website: <https://www.kali.org/downloads/>



The screenshot shows the website [offensive-security.com/kali-linux-vmware-virtualbox-image-download](https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download). The page features the Offensive Security logo and navigation links for Blog, Courses, Certifications, and Online Labs. Two tabs are visible: "Prebuilt Kali Linux VMware Images" (selected) and "Prebuilt Kali Linux VirtualBox Images". Below the tabs is a table listing available VM images.

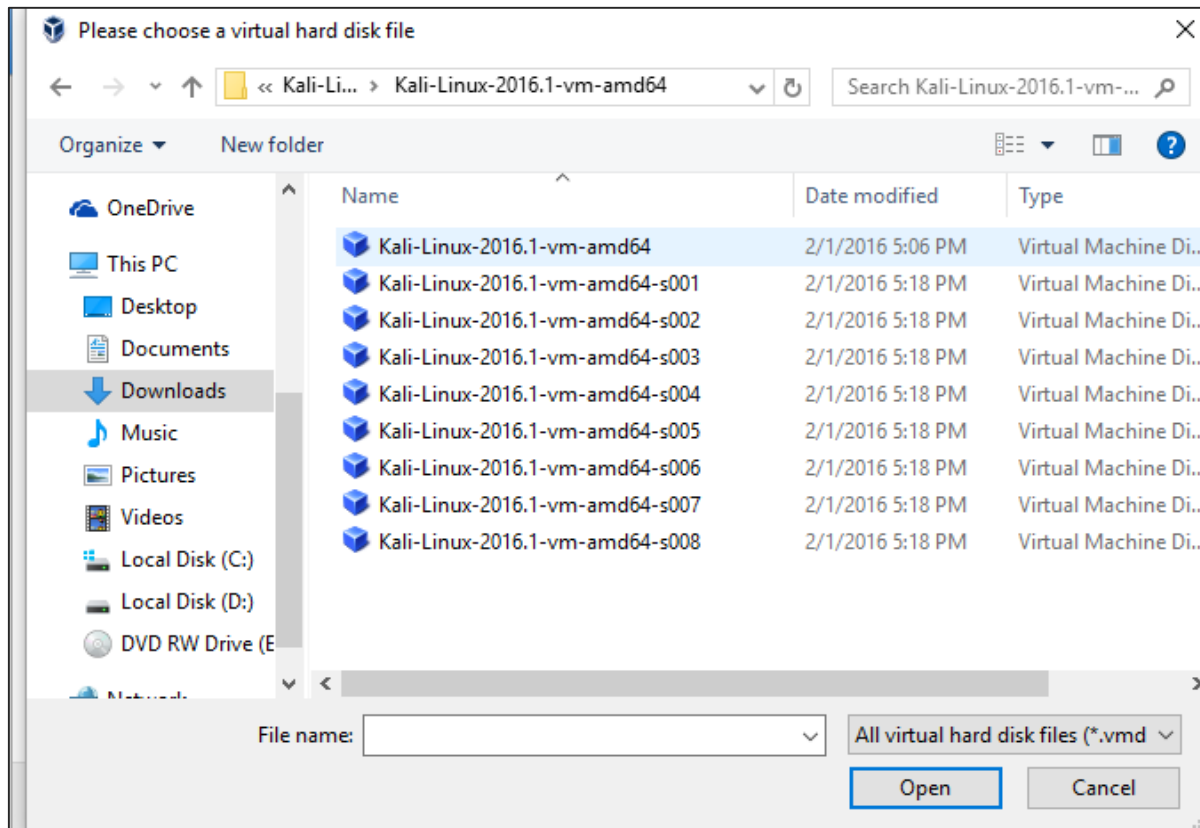
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

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

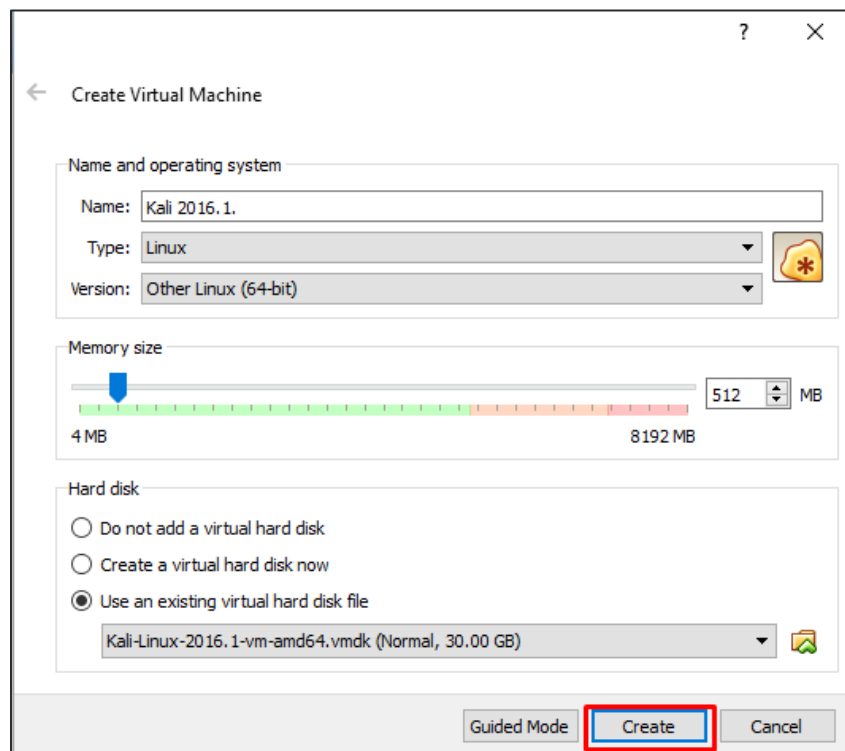


The screenshot shows the Oracle VM VirtualBox Manager interface. The 'File' menu is open, and the 'New...' option is highlighted with a red box. The 'New...' option has the keyboard shortcut 'Ctrl+N'. Other options in the menu include Add..., Settings..., Clone..., Remove..., Group, Start, Pause, Reset, Close, Discard Saved State..., Show Log..., Refresh, Show in Explorer, Create Shortcut on Desktop, and Sort. The right-hand pane shows the configuration for a virtual machine named 'AC1', which is running Windows 2008 (64-bit). The configuration includes details for General, System (1500 MB Base Memory), Display (18 MB Video Memory), Storage (SATA Controller), and Audio (Windows DirectSound).

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



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



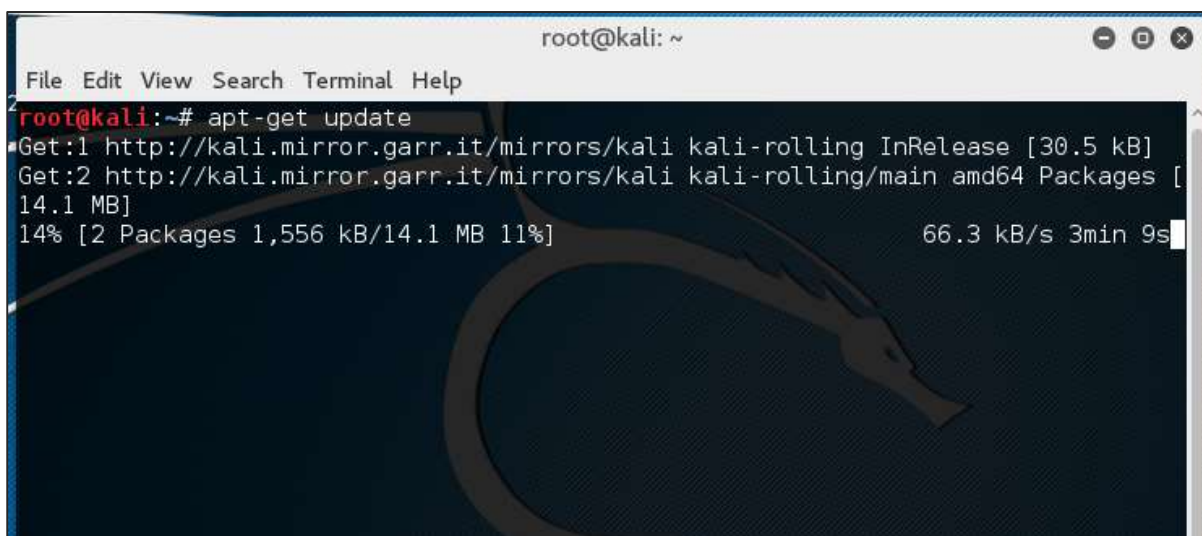
Step 5: Start Kali OS. The default username is **root** and the password is **toor**.



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 girl.2-gdkpixbuf-2.0
 girl.2-gnomedesktop-3.0 girl.2-gst-plugins-base-1.0 girl.2-gstreamer-1.0
 girl.2-ivscriptcroatk-4.0 girl.2-mutter-3.0 girl.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 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 girl1.2-clutter-gst-2.0 girl1.2-evinced-3.0 girl1.2-gtk-3.0
girl1.2-packagekit-glib-1.0 girl1.2-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-ffmpeg5 libavformat-ffmpeg56 libavresample-ffmpeg2 libavutil-ffmpeg54 libbasicusageenvironment0
libbind9-98 libboost-filesystem1.58.0 libboost-python1.58.0 libboost-python1.61.0 libboost-system1.58.0
libboost-thread1.58.0 libcamel-1.2-54 libchronoprint0 libclutter-gst-2.0-0 libcrypto++9v5 libcurl-perl
libcurls-ui-perl libdns100 libdataserver-1.2-21 libexporter-tiny-perl libfft3-single3 libgdic-1.0-9
libglew1.13 libgrilo-0.2-1 libgroupsock1 libgssapi3-heimdal libgtkglext1 libgucharmap-2-90-7
libcrypto4-heimdal libhdb9-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhunspell-1.3-0
libhw509-5-heimdal libicalia libilmbase6v5 libisc95 libisccc90 libisccfg90 libjasper1 libjpeg9
libkdc2-heimdal libkrb5-26-heimdal liblist-moreutils-perl liblivemedia23 libllvm3.7 liblouis9 liblwres90
libnm-glib-vpnl libntdb1 libonig2 libopenexr5v5 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 libtrio3
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.

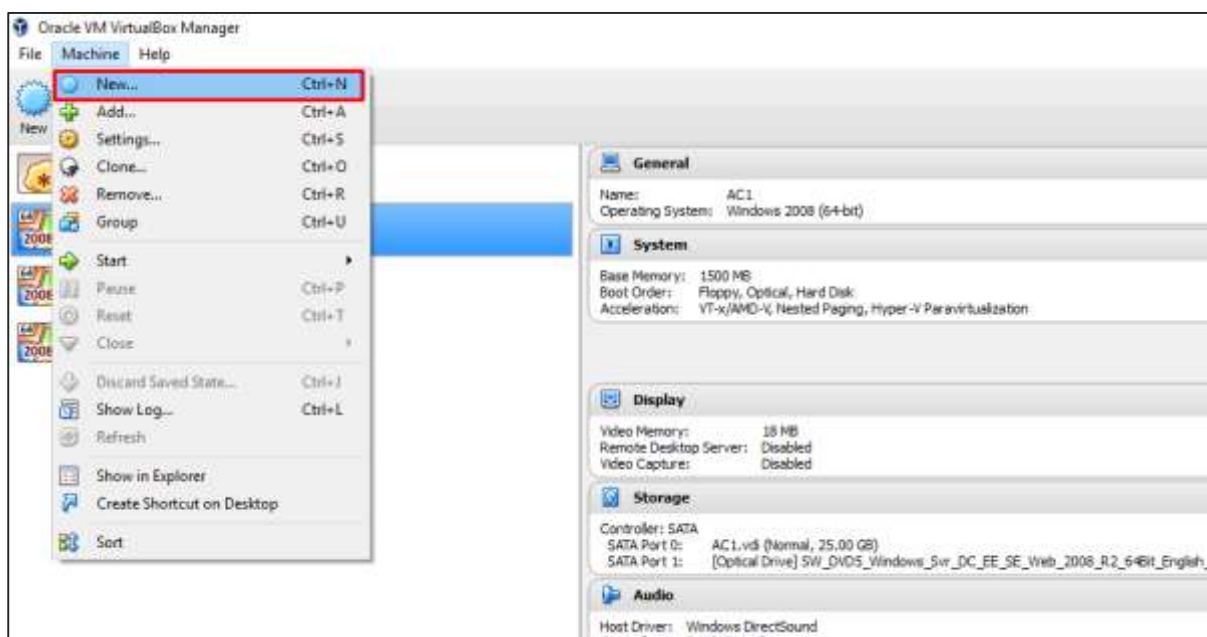
Step 1: Download **Metasploitable**, which is a Linux machine. It can be downloaded from the official webpage of **Rapid7**: <https://information.rapid7.com/metasploitable-download.html?LS=1631875&CS=web>

The screenshot shows the Rapid7 website's download page for Metasploitable. The page features a header with the Rapid7 logo and the text 'Download Metasploitable'. The main heading is 'Metasploitable - Virtual Machine to Test Metasploit'. Below this, there is a sub-heading: 'Download Metasploitable, the intentionally vulnerable target machine for evaluating Metasploit'. The page contains a detailed description of the VM, its purpose, and how to use it. A form is provided for users to fill out to download the VM, with fields for First Name, Last Name, Job Title, Job Level, Company, Work Phone, Work Email, and Country. A 'SUBMIT' button is located at the bottom of the form.

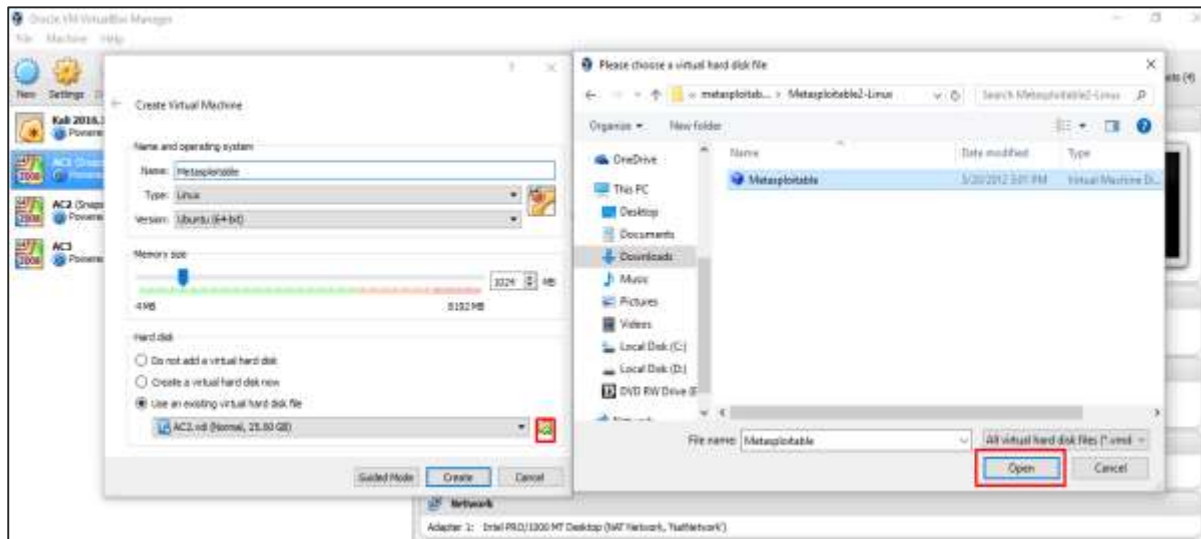
Step 2: Register by supplying your details. After filling the above form, we can download the software.



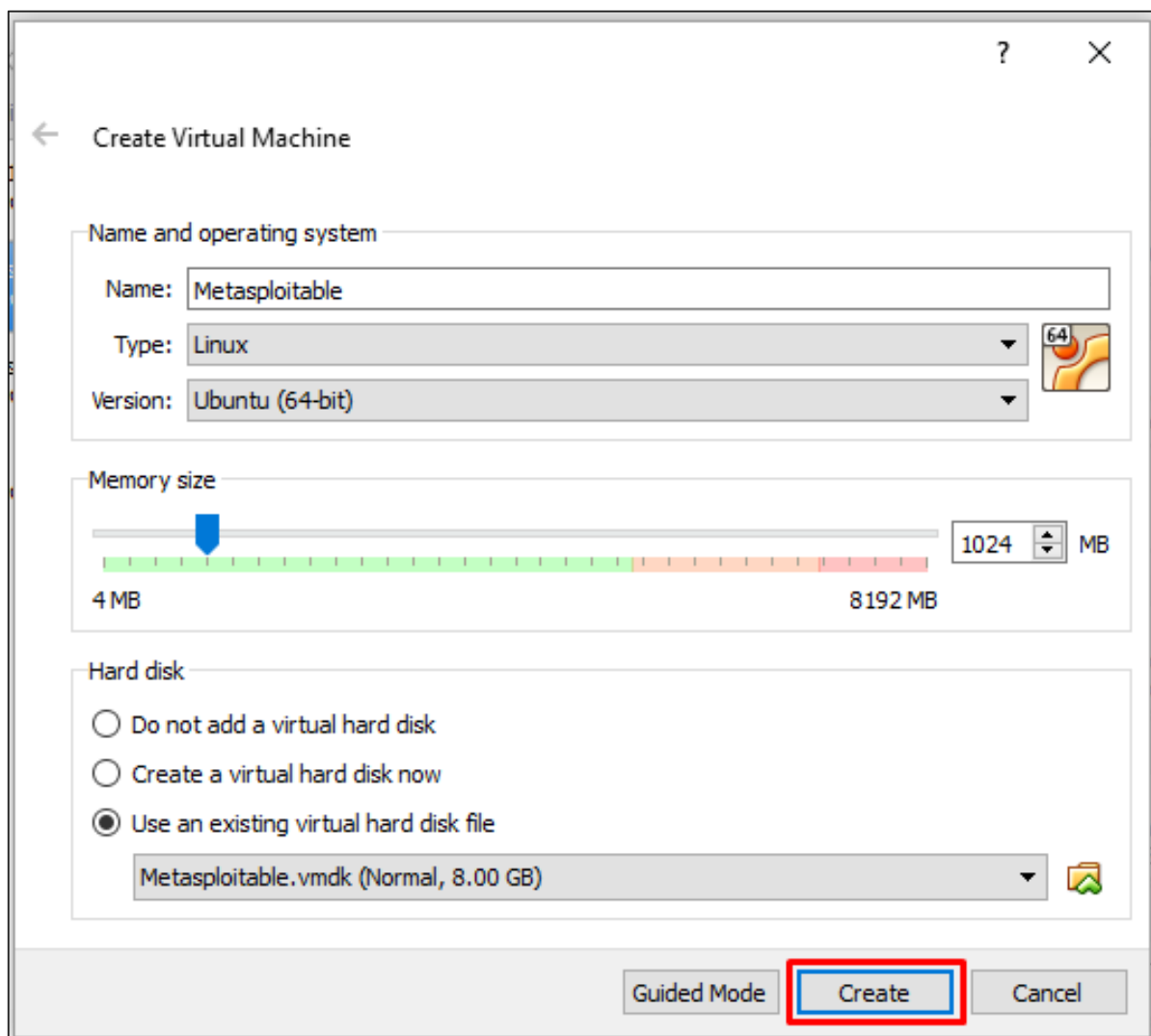
Step 3: Click **VirtualBox** -> **New**.



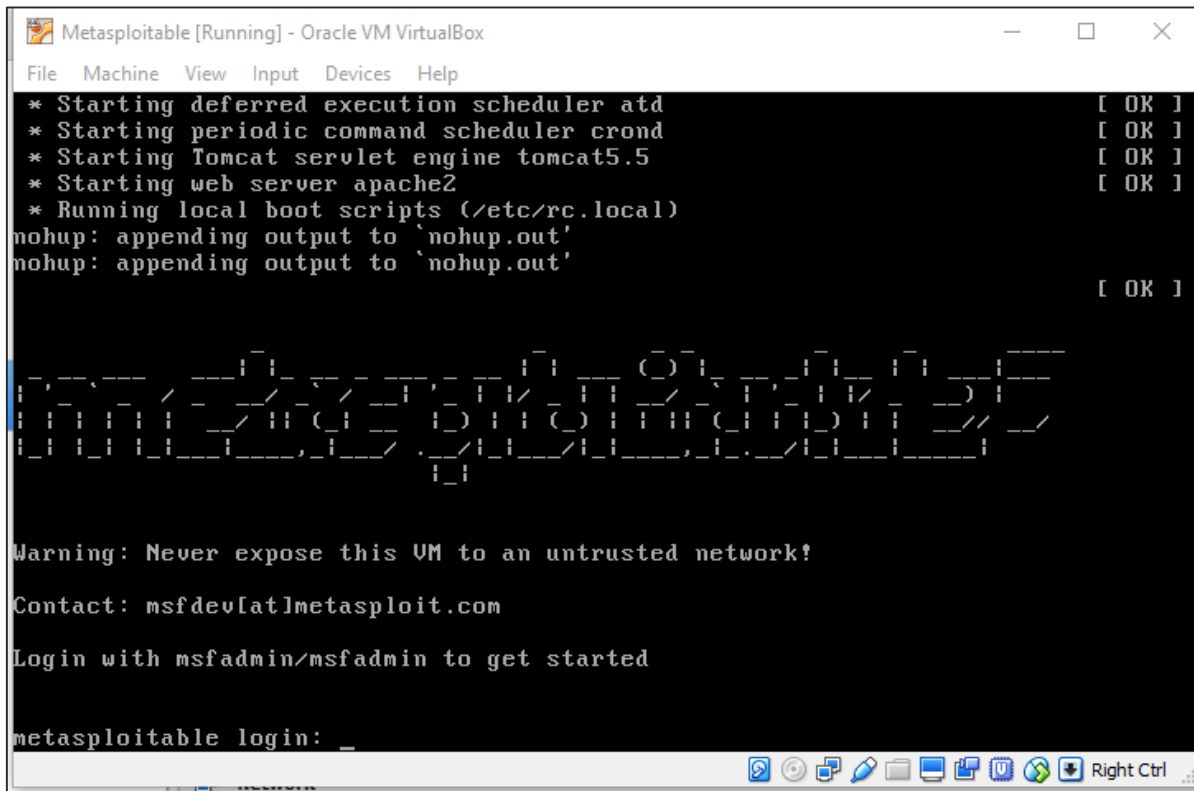
Step 4: Click "Use an existing virtual hard disk file". Browse the file where you have downloaded **Metasploitable** and click **Open**.



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



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



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```

2. Kali Linux – Information Gathering Tools

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

NMAP and ZenMAP

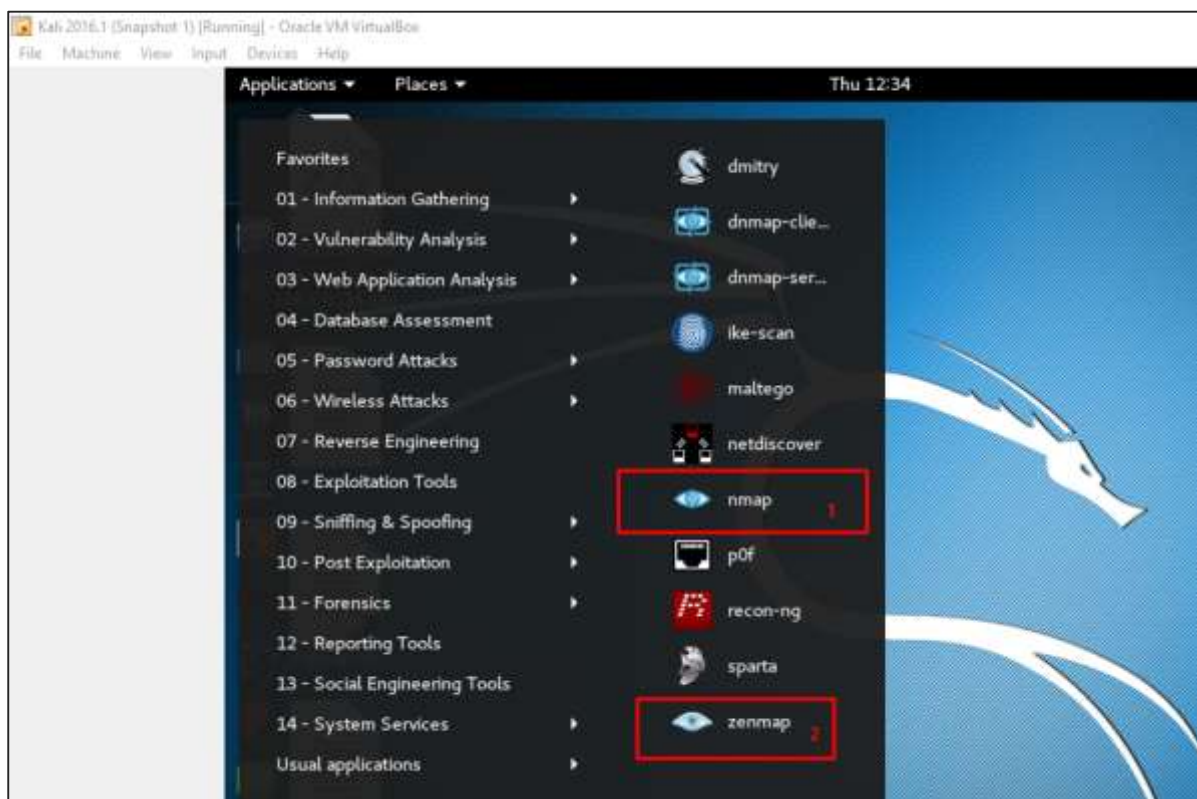
NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

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.

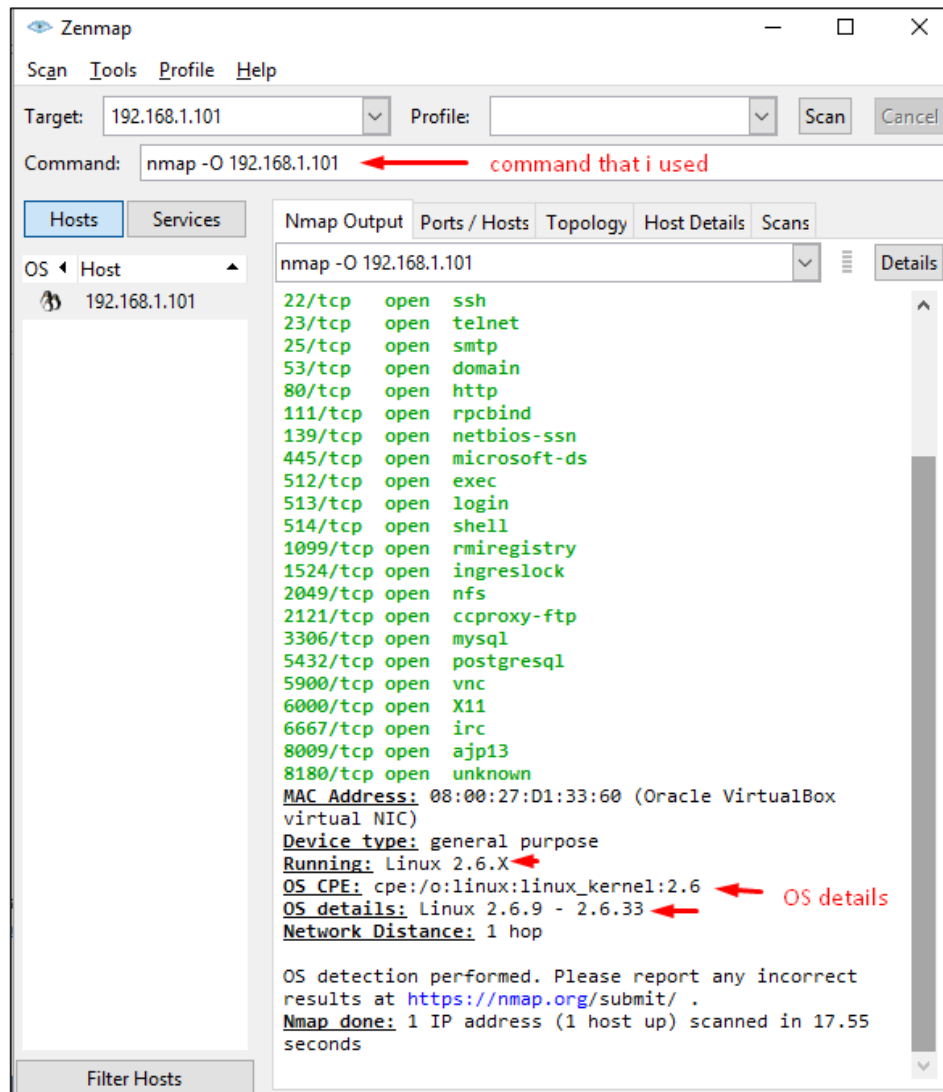


Step 2: The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable "-O". For more information, use this link: <https://nmap.org/book/man-os-detection.html>

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.

Target: 192.168.1.101 Profile: Scan Cancel

Command: nmap -p 1-65535 -T4 192.168.1.101

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 192.168.1.101

nmap -p 1-65535 -T4 192.168.1.101

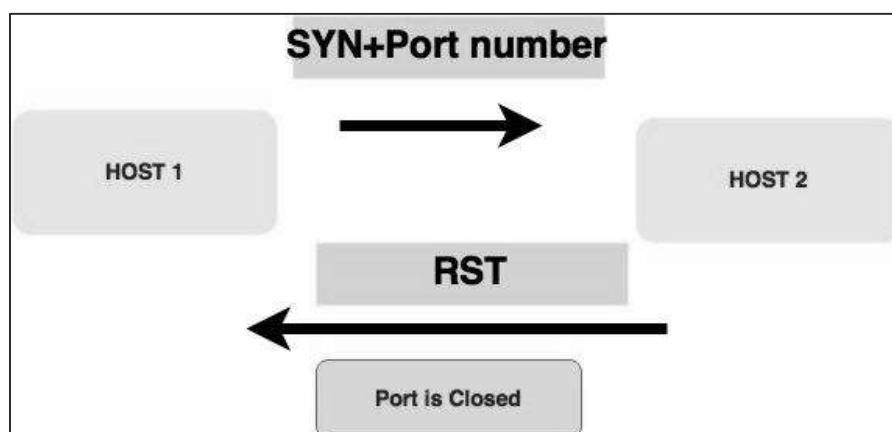
Starting Nmap 7.12 (<https://nmap.org>) at 2016-09-16 18:04 Central European Daylight Time
 Nmap scan report for 192.168.1.101
 Host is up (0.000010s latency).
 Not shown: 65505 closed ports

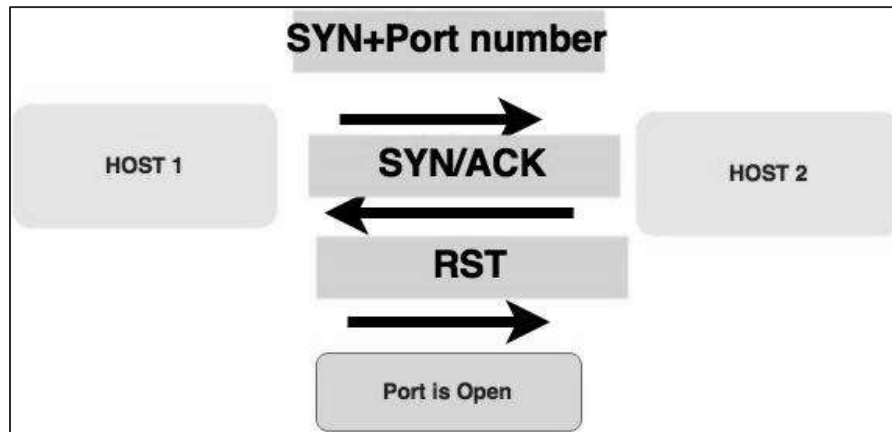
PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
3632/tcp	open	distccd
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
6697/tcp	open	unknown
8009/tcp	open	ajp13
8180/tcp	open	unknown
8787/tcp	open	unknown
48285/tcp	open	unknown
51161/tcp	open	unknown

Filter Hosts

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.

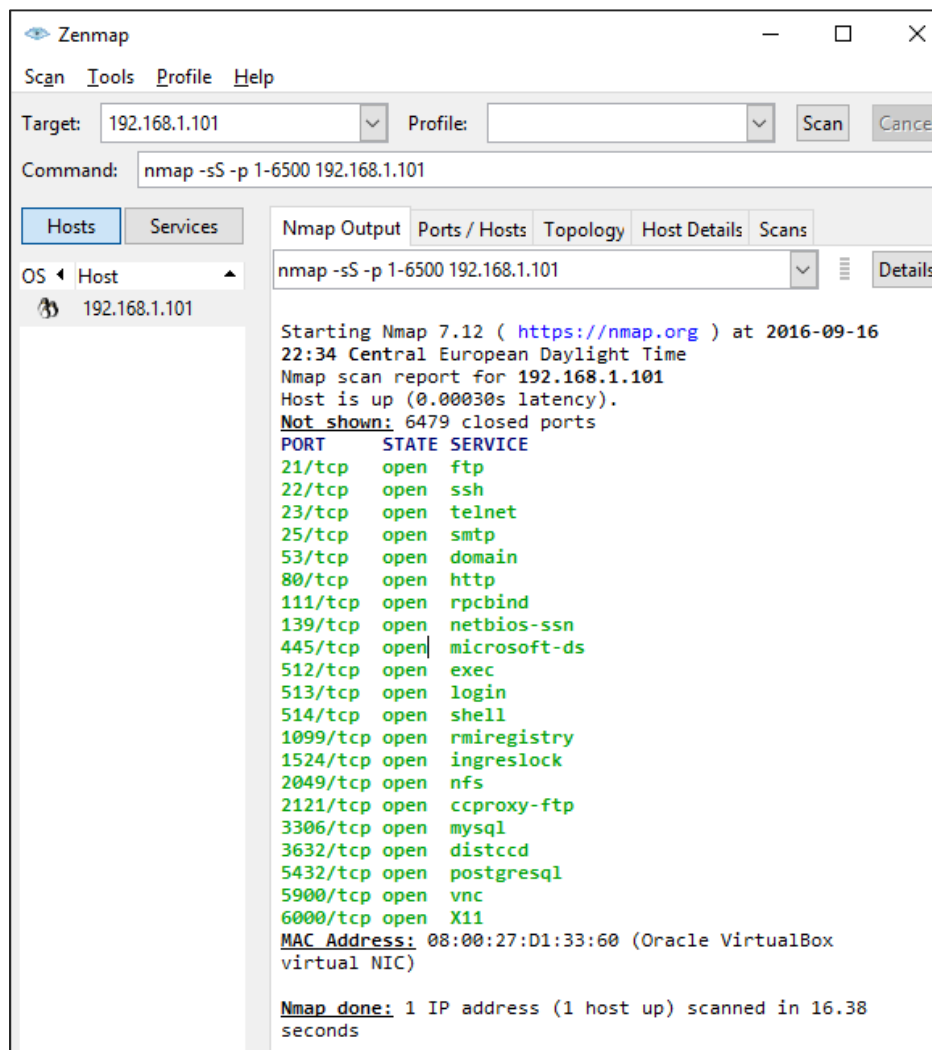




Now to see the SYN scan in practice, use the parameter **-sS** in NMAP. Following is the full command –

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

The following screenshot shows how to use this command:



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