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
Iaxflood ........................................................................................................................................................................... 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
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](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.

![VirtualBox](https://www.virtualbox.org/wiki/Downloads)

**VirtualBox binaries**

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

- **VirtualBox platform packages.** The binaries are released under the terms of the GPL version 2.
  - VirtualBox 5.1.2 for Windows hosts
  - VirtualBox 5.1.2 for Linux hosts
  - VirtualBox 5.1.2 for Solaris hosts

- **VirtualBox 5.1.2 Oracle VM VirtualBox Extension Pack** for all supported platforms

Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP and PKE boot for Intel cards. See this chapter from the User Manual for an introduction to Oracle VM VirtualBox Extension Pack. Binaries are released under the VirtualBox Personal Use and Evaluation License (PVUL). 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](https://www.virtualbox.org/wiki/Downloads). If you are using VirtualBox 4.3.38, please download the extension pack [here](https://www.virtualbox.org/wiki/Downloads).

**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/

<table>
<thead>
<tr>
<th>Image Name</th>
<th>Torrent</th>
<th>Size</th>
<th>Version</th>
<th>SHA1Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kali Linux 64 bit VM</td>
<td>Torrent</td>
<td>2.0G</td>
<td>2016.1</td>
<td>2bd4bf1e77c14c5b5618249ca69a4d623a6f5f2d</td>
</tr>
<tr>
<td>Kali Linux 32 bit VM PAE</td>
<td>Torrent</td>
<td>2.0G</td>
<td>2016.1</td>
<td>c71887a8bbf7ed56a43e7b7c93fd6e450f6759</td>
</tr>
</tbody>
</table>

**Step 2:** Click VirtualBox -> New as shown in the following screenshot.
**Step 3**: Choose the right virtual hard disk file and click Open.

![Image of virtual hard disk file selection]

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

![Create Virtual Machine dialog box]

- Name: Kali 2016.1
- Type: linux
- Version: Other Linux (64-bit)
- Memory size: 4 GB
- Hard disk: Use an existing virtual hard disk file
**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`”.

---

**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](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**.
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:

![Nmap Command Example](image)

**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: