[](https://pentestmag.com/)

The only magazine devoted exclusively to penetration testing.

By [rafal\_szymkiewicz](https://pentestmag.com/author/rafal_szymkiewicz/) June 10, 2014

**A Brief Introduction to Kali Linux**

This is a brief article which have the goal to introduce the reader to the awesome world of Kali Linux. This is not an exaustive introduction to this Operating System (OS), but its purpose is just to give an idea of the many possibilities provided by this Linux OS which is born as Pen Testing distro but can be used in several others ways.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created, that is how Oensive Security Ltd. denes their own project. Kali Linux is a Linux Distribution, which is a branch of Debian, but with several specialties. As already reported, Kali Linux is an OS mainly designed for Pen Testing, it is an open source software having numerous Pen Testing tools, more than 300.

Kali Linux is not a general use Linux distribution but it’s designed to be single user, where the default user is superuser (root). It is not recommended for Linux beginners since you’re running as root and it is easy to make a trouble in yor OS if you are not careful.

Is Back Track (BT) the Kali father ?

Many Pen Tester have been using BT for several years in order to perform their security activities. BT is alse an open source Linux based OS having a security toolset. BT made performing a security assessment in a easy way since all of the common tools that you needed were packaged into this distro and ready to be available immediately. If you need to see a complete list of all security tools belonging to BT you have to just run “dpkg list” on it. BT made it easy to create a new VM from the downloaded ISO, perform the assessment, then either archive that VM for future reference or delete it when done to remove the evidence. The latest version of BT is version 5 release 3 and it came out on August 13, 2012.

Since, already said, Pen Tester professionist have been relying on the BT for several years to help them perform their assessments, the industry has been waiting for the next major release of BT but the developers have gone in a new direction by creating Kali Linux.

Kali Linux is similar to BT but it lays a new foundation and makes substan-tial improvements that will allow it to be even more useful to Pen Testers in the coming years. Whereas BT was built on Ubuntu, Kali is (re)built from scratch and constructed on Debian. Kali also has software repositories that are syn-chronized with the Debian repositories so it permits easy updateding, patches applying and new tools adding. It is also easy to customize your own Kali Linux so that it contains only the packages and features that are required. You can also choose your desktop environment by using Gnome (default), KDE, LXDE, XFCE or the kind of desktop which you prefer.

Installation

One can install Kali Linux in the hard drive, or run from a Live CD, or a Live USB. Kali installation is out of the purpose of this introduction, if the reader wants to get a complete installation guide he can see the specic Kali web site.

Pen Testing

As said, Kali is the Linux OS distro dedicated to Pen Tester professionist. It has several free tools and among that you can nd software for the following activities:

password recovery; forensic analysis;

web application testing.

Companies

Kali is an awesome OS developed for both people and organizations that need to accomplish security testing but have not enought resources (time and money) to maintain a specic hardware infrastructure. The tools are preinstalled, main-tained, updated, and congured in order to work together where appropriate, in this way few resources are necessary to maintain an updated environment.

The most advance tools, developed for professional Pen Testers, includes the activities reported in the following:

password cracking; wireless sni‑ng;  
network scanning; social hacking.

Computer Forensics

As already reported, Kali could be also used by Forensics analyzers since it provides a characteristic method which does not touch the internal hard drive, does not auto mount any removable media, and allows a potentially compro-mised system to be analyzed with a great detail, along with tools to track the information gathered.

Information Technology (IT) departments

Furthermore, IT departments could also be interested about Kali Linux, since with its tools can permit the following activities:

network scanning;

vulnerability assesment; password recovery.

Amateurs

Kali Linux could be useful even for simple users which does not fall into none of the previous groups. Kali is a very amusing OS since it has a lot of tools preinstalled, in this way users can look through a categorized menu the tools of interest, making it easy to search for those softwares which might meet their needs and the can be quickly evaluated. A lot of tools are from the command-line, but others have a GUI which make them easier to use.

Usable Hardware Platforms

As already reported, Kali coul be considered the successor to BT which was released at the end of 2012 and is distributed in a number dierent ways:

you can download an ISO for installing from scratch, dual booting with Windows, live USB installs, and hard disk installs;

VMware images are available for bringing up VM quickly; there’s an AMI available for Amazon EC2.

Kali can be installed either on i386 or x86\_64 processors, as well as a whole host of ARM devices such as Raspberry Pi, HP and Samsung Chromebooks, and even the Galaxy Note tablet.

On monday we are going to start workshops.

If you want to get free workshop teaser with two reliable articles about Kali Linux and Wi Fi DOS Attack , please contact with us.

We’ll send you all details and answer your questions: milena.bobrowska@pentestmag.com