International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Kali Overpowering Backtrack

Laxman Vishnoi
M.Tech(I.T.) Student,I.T.M. College
India

Dr. Vivek Shrivastava
Asst. Prof. (I.T.), I.T.M. College
India

Abstract –

Pentesting – It is a process to imitate all ways used by hackers to compromise a system. But with the diference its is purely ethical in deed so as to know in prior how a machine can suffer security breach attack. In this paper we will look after how kali linux overpowered backtrack in such a short span of time. Backtrack and Kali linux are two powerful and yet very common choices for the purpose of penetration testing. Kali linux declared its presence in 2013 and now has covered much market than its predecessors. Kali is often known as an offshoot of backtrack. Backtrack has been in presence since 2007. We will highlight all the reasons behind formation of kali linux and why it become so popular than backtrack, which was first or may say a default choice for all before release of kali.

Keywords - Hacking, Hacker, Ethical Hacking, Penetration Testing, Information Security.

I. A BRIEF ON BACKTRACK AND KALI

BackTrack Linux, is a specialized distribution of penetration testing tools, has long been a favourite of security specialists and IT pros.

Kali linux is Debian based (Debian Wheezy) by Offensive security. Actually according to them it is a mix between everything and not much as declared on website.

Cyber Security, the most concerned topic and the most concerned area in today's online world[3]. The vast number of complaints were received about hacking acts. People around there, using internet medium for most of their sort of stuff including business, communication, fun have a fear of being observed or hacked by malicious users.

II. WHY SWITCHED?

So the first big change was platform -- from Ubuntu to Debian. Debian-compliant packages and Filesystem Hierarchy Standard (FHS) compliance were two main reasons that put effort into this decision: "What this means is that instead of having to navigate through the /pentest tree, you will be able to call any tool from anywhere on the system as every application is included in the system path."

Fig. 1 A still of Kali

Kali Linux is so different that the researchers and technical team at Offensive Security thought that to solve the 'inherent problems' of BackTrack the authors needed a complete re-write. The main issue with BackTrack v1-v5 was that it was a an ache for dependencies. Here was the problem: too many pentesting tools embedded within BackTrack all struggled to co-exist within the dependencies. Many pentesting and security tools where not regularly updated by their creators so the result was that trying to update the entire OS often caused conflicts and tools would simply stop working, crash or even cause other tools to crash. A fine example is Ettercap which was not updated for a very long time.

Here are some of the highlights of Kali:

- More than 300 penetration testing tools involved and still funded by Offensive Security
- ARMEL and ARMHF support, including for these arm devices: rk3306 mk/ss808, Raspberry Pi, ODROID U2/X2, and Samsung Chromebook
- Fully customizable
- Multilingual support
- Free of use

III. EVOLUTION OF KALI

The figure below describes how kali is being evoluted. Knoppix is a classic distro with a loyal community. Over time the Knoppix project was forked into WHoppix (yes the WH are meant to be capitalized) that was then re-forked into WHAX. WHAX was then re-branded and streamlined into the BackTrack that we all used.

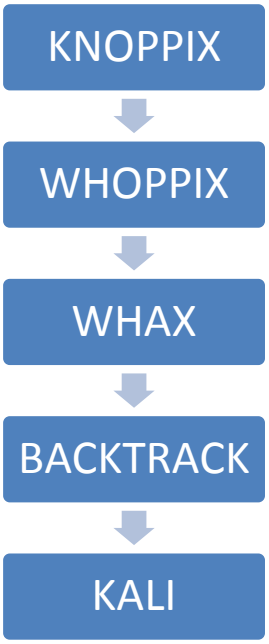

Fig. 2 Evolution of kali

The new Kali Linux offers a smoother, easier penetration testing experience, making it more accessible to IT generalists as well as security specialists. The new infrastructure incorporates Debian development standards to provide a more familiar environment for IT administrators. The result is a more robust solution that can be updated more easily. Users can also customize the operating system to tailor it to their needs and preferences.

V. SOME MORE FEATURES

Kali Linux has been improved over Backtrack in many ways. Backtrack was kind of "Ubuntu + security tools placed in the /pentest directory". And due to this, to run any security tool first the user had to navigate to the pentest directory. This made updates difficult too, since the tools were not real installations that could be updated from synaptic. Kali linux has everything installed like packages that can be updated from repositories. Kali Linux is based on Debian and is a complete distro in itself. To run any tool just type the command at the terminal and it would run. Also there is no more need to type the startx command at boot, like in backtrack. Kali is a free, open source, and robust Linux Distribution that makes security auditing ready for the enterprise. It is the natural evolution of the BackTrack platform, which has been hugely popular among Metasploit users. This is why the Metasploit team here at Rapid7 was more than happy to join the Kali Linux project as an official contributor. We re-engineered Metasploit to fully integrate into the Kali Linux repositories and resolved some of the issues that may have caused some of you headaches with updates, databases, and general stability on BackTrack in the past.

It can be easily installed inside a virtualizer like Virtualbox. Infact I use it inside virtualbox only. Kali linux needs to run as root, and therefore its very secure to run it inside a virtual environment, or from a live media.

Backtrack had both a gnome and kde version available for download. However kali linux comes only in the gnome based build. However other desktops like xfce, kde can be easily installed from synaptic.

Kali linux is configured to run as root. Even after installation to hard drive, it runs as root. This is necessary because many security tools like wireshark, nmap need to run as root.

IV. Emergency Self Destruction of LUKS in KALI

Being penetration testers, we often need to travel with sensitive data stored on our laptops. Of course, we use full disk encryption wherever possible, including our Kali Linux machines, which tend to contain the most of sensitive and confidential information. and setting up full disk encryption with Kali becomes simple process. The Kali installer includes a straightforward process for setting up encrypted partitions with LVM and LUKS. Once encrypted, the Kali operating system requires a password at boot time to allow the OS to boot and decrypt your drive, thus protecting this data in case your laptop is stolen.

VI. CONCLUSION

Kali Linux is a new open source distribution that facilitates penetration testing. Whereas BackTrack was built on Ubuntu, Kali is built from scratch and constructed on Debian and is FHS-compliant. Kali also has improved software repositories that are synchronized with the Debian repositories so it makes it easier to keep it updated, apply patches and add new tools. 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 customize your desktop environment to use Gnome(default), KDE, LXDE, XFCE or whatever you prefer.

The development of Kali Linux was funded by Offensive Security. Offensive Security is a security training and penetration testing consulting firm that has been a creator, supporter and maintainer of BackTrack since the beginning. For years they have offered their popular Penetration Testing with BackTrack (PWB) class, but with the introduction of Kali Linux, that class name will likely change.

Like its predecessor, Kali Linux is completely free and always will be. Offensive Security is committed to supporting the open source community with the ongoing development of Kali Linux. The development tree and all sources are available for those who wish to tweak and rebuild packages. Kali Linux is available immediately for download from http://www.kali.org/downloads/.

REFERENCES

[1] Internet Crime Complaint Centre link: www.ic3.gov

[2] Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min; "Software vunerability Discovery Techniques : A Survey" IEEE Conference Publication, DOI : 10.1109/MINES.2012.202, Page(s) 152-156, 2012

[3] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI : 10.1147/sj.403.0769, Page(s): 769-780

[4] Bradley, Rubin "Computer Security Education and Research : Handle with care" IEEE Conference Publication, DOI : 10.1109/MSP.2006.146, Page(s): 56-59

[5] Wilbanks "When Black Hats are really white" IEEE Conference Publication, DOI : 10.1109/MITP.2008.146, Page(s): 64

[6] Robinson, S. "*Art of Penetration Testing"* Security of Distributed Control Systems, 2005. The IEE Seminar on Date of Conference: 2 Nov. 2005. Page(s): 71 – 76.

[7] Budiarto, R.,Sureswaran Ramadass "*Development of penetration testing model for increasing network security*" Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on Date of Conference: 19-23 April 2004, Page(s): 563 - 564.

.