BackTrack 4 – The Definitive Guide

This document is a work in progress.
It is a quick attempt to cover the most commonly asked questions about BackTrack,
in one place. Check on this page frequently for updates.

Introduction

BackTrack is the world's leading penetration testing and information security auditing distribution. With hundreds of tools preinstalled and configured to run out of the box, BackTrack 4 provides a solid Penetration testing platform - from Web application Hacking to RFID auditing – its all working in once place.

Behind the curtains

BackTrack Base

There have been many changes introduced into BackTrack 4 - most notably, our move to an Ubuntu Intrepid base. We now maintain our own full repositories with modified Ubuntu packages in addition to our own penetration testing tools.

Another significant change is the updated kernel version, currently at 2.6.29.4. This new kernel brought an onset of internal changes, which have greatly changed the structure of BackTrack.

BackTrack Kernel

We no longer use lzma enabled squashfs as our live filesystem, which on one hand results in larger ISO size, but on the other hand, frees us from having to maintain our own kernel patches. This is especially painful these days, as squashfs is slowly moving into the mainstream kernel (at the time of this writing).

BackTrack 4 uses squashfs-tools version 4.0 (which is not backward compatible with previous versions), and the inbuilt squashfs kernel module, which is present in 2.6.29.4. AUFS is used as the unification filesystem (aufs2.x).

Several wireless driver injection/optimization patches have been applied to the kernel, as well as a bootsplash patch. These patches can be found in the kernel sources package (/usr/src/linux/patches).

These changes mean that much of what you were used to in BackTrack 2/3 has changed in terms of boot cheatcodes and such, as this kernel shift also means we no longer use the *live-linux* scripts to create our images (we use casper now).

Packages and Repositories

One of the most significant changes introduced in BackTrack 4 are the Debian like repositories available, which are frequently updated with security fixes and new tools. This means that if you choose to install BackTrack to disk, you will be able to get package maintenance and updates by using *apt-get* commands.

Our BackTrack tools are arranged by parent categories. These are the categories that currently exist:

- BackTrack - Enumeration
- BackTrack - Tunneling
- BackTrack - Bruteforce
- BackTrack - Spoofing
- BackTrack - Passwords
- BackTrack - Wireless
- BackTrack - Discovery
- BackTrack - Cisco
- BackTrack – Web Applications
- BackTrack - Forensics
- BackTrack - Fuzzers
- BackTrack - Bluetooth
- BackTrack - Misc
- BackTrack - Sniffers
- BackTrack - VOIP
- BackTrack - Debuggers
- BackTrack - Penetration
- BackTrack - Database
- BackTrack - RFID
- BackTrack – Python

- BackTrack – Drivers
- BackTrack - GPU

Meta packages

A nice feature that arises from the tool categorization, is that we can now support "*BackTrack meta packages*". A meta package is a dummy package which includes several other packages. For example, the meta package "**backtrack-web**" would include all the Web Application penetration testing tools BackTrack has to offer.

Meta Meta Packages

We have two "*meta meta packages*" – **backtrack-world** and **backtrack-desktop**.
backtrack-world contains all the BackTrack meta packages, while **backtrack-desktop** contains **backtrack-world**, **backtrack-networking** and **backtrack-multimedia**. The latter two meta packages are select applications imported from Ubuntu repositories.

Up and running with BackTrack

We've made a short movie called "up and running with BackTrack" – showing some common and not so common features. A good place to start in order to grasp the new changes in BackTrack 4.

http://www.offensive-security.com/videos/backtrack-security-training-video/up-and-running-backtrack.html

Installing BackTrack to Disk

BackTrack 4 (both barebones and full version) now contains a modified Ubiquity installer. The install should be straight and simple. For a video tutorial, check http://www.offensive-security.com/videos/install-backtrack-hard-disk/install-backtrack-hard-disk.html

Updating Backtrack

Keeping BackTrack up to date is relatively simple by using the apt-get commands.

apt-get update synchronizes your package list with our repository.

apt-get upgrade downloads and installs all the updates available.

apt-get dist-upgrade downloads and installs all new upgrades.

Customizing BackTrack

Creating your own Live CD – Method 1

Creating your own flavor of BackTrack is easy.

1. Download and install the bare bones version of BackTrack
2. Use apt-get to install required packages or meta packages.
3. Use remastersys to repackage your installation.

Creating your own Live CD – Method 2

Download the BackTrack 4 iso. Use the customization script to update and modify your build as show here:

http://www.offensive-security.com/blog/backtrack/customising-backtrack-live-cd-the-easy-way/

Installing BackTrack to USB

The easiest method of getting BackTrack4 installed to a USB key is by using the unetbootin utility (resent in BackTrack in /opt/).

Installing BackTrack to USB - Persistent changes

A Video tutorial can be found here:

http://www.offensive-security.com/videos/backtrack-usb-install-video/backtrack-usb-install.html

Working with BackTrack

KDE3 Quirks

BackTrack 4 contains an "imposed" KDE3 repository, alongside the KDE4 Ubuntu Intrepid repositories. Since BackTrack uses KDE3, it's important to remember that KDE3 packages contain a "kde3" postfix, which makes them easily identifiable.

For example, if you wanted to install the program KDE program "kate", you should *apt-get install kate-kde3* (install the KDE3 version of kate) rather than *apt-get install kate*. (install the KDE4 version of kate).

Updating tools manually

Our BackTrack repositories will always strive to keep updated with the latest versions of tools, with the exception of a select few. These "special" tools get updated by their authors very frequently, and often include significant updates. We felt that creating static binaries for these types of tools would not be beneficial and users were better of keeping these tools synched with the SVN versions respectively. The tools include MSF, W3AF, Nikto, etc.

FAQs

- **The Ubiquity Installer gives me a "Language failed with exit code 10" error. What the heck ?**
- Ignore it. Have faith.

- **Why is the ISO so big? It used to be half the size!**
- For a long time we struggled to keep BT under the 700 MB limit. This was always a challenge and a pain in the backside. We decided to bust this barrier for a couple of reasons:

- We no longer use squashfs with LZMA compression – which makes the image size significantly larger.
- A CD is not the ideal media for running BT4 in a live environment. A USB key is much faster and reliable.

- **Why is this build called a "pre-release"? Isn't it stable enough ?**
- This is probably the sturdiest version of BackTrack we've ever come up with. Saying this, some bugs can be really obscure. Only after running an atheros card for 40 straight hours did we notice wireless frame corruptions – which resulted from a faulty patch we applied. It's impossible for us to test every driver and every hardware combination. That why we NEED YOUR INPUT (in the forums).

- **Why oh why did you use Ubuntu as your base?**
- Check this blog post: http://backtrack4.blogspot.com/2009/01/philosophical-thoughts-about-backtrack.html

- **I've installed Backtrack 4 to Hard Disk. How do I log in ??**
- Use the user / pas cmbination for the user you created during the install. Once logged in, type sudo su, and change the root password to your liking. Check this video for more information: http://www.offensive-security.com/videos/backtrack-security-training-video/up-and-running-backtrack.html

Outro
You can find our forums at http://forums.remote-exploit.org.

Feel free to post bugfixes, suggestions, tool requests, etc.

We hope you enjoy this fine release!

Remote Exploit Team