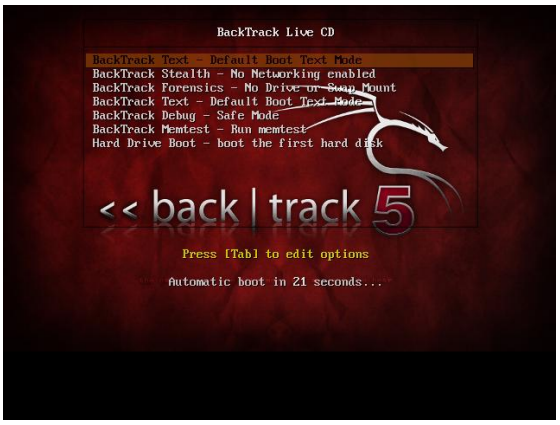
BACKTRACK 5

Pranshu Sharma , Satish Anand Arjunan

BackTrack is a well-known specialized Linux distribution focusing on security tools for penetration testers and security professionals, but it now offers a lot in terms of forensics.

Pros: BackTrack 5 has all the tools you need for testing network security and it is nicely presented.
Cons: Documentation is scarce and often outdated & upgrading from previous release isn't supported.

The advantage of BackTrack 5 (BT5) is that it offers a slew of security and forensic tools on a live DVD, ready to use. It's based on Ubuntu Lucid (10.04 LTS) with Linux kernel 2.6.38 and some patched WiFi drivers to allow injection attacks. You can download the distribution in a GNOME or a KDE version, for 32-bit or 64-bit x86 machines. It's a live DVD ISO file, which you can burn to a DVD or write to a USB stick. On the desktop of the live session, there's an installer icon if you want to install BackTrack permanently. For the first time, the project also has an image for ARM, which you can run on your smartphone or tablet to test the security of a wireless network.



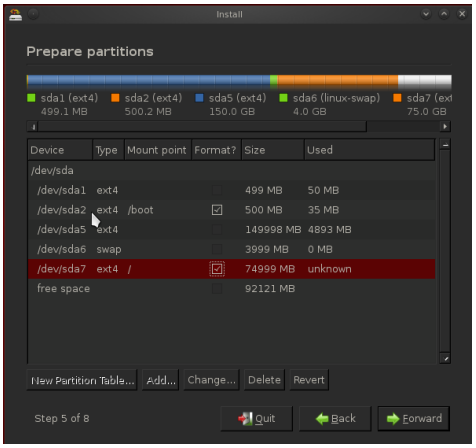
BackTrack 5 allows you to boot into a stealth or a forensics mode. BackTrack's boot menu gives you various options. The default option just starts a live session (a stylish framebuffer console, in which you can start GNOME or KDE with startx), but there's also a stealth mode which boots the distribution without generating any network traffic: you have to enable networking manually later. This is interesting if you want to hide your presence on the network temporarily. Another nice option is the forensics mode, which doesn't automatically mount the computer's drives and also doesn't use any swap space it finds. When forensically investigating a system, this guarantees that you don't accidentally wipe out hidden traces.

BackTrack is filled with a collection of more than 300 open source security tools, which you can find organized in different submenus of the "Backtrack" menu: "Information Gathering", "Vulnerability Assessment", "Exploitation Tools", "Privilege Escalation", "Maintaining Access", "Reverse Engineering", "RFID Tools", "Stress Testing", "Forensics", "Reporting Tools", "Services", and "Miscellaneous". Each submenu is further subdivided into subcategories. The developers have added a nice touch to menu items of command line utilities: when you click on such a menu item, it opens a terminal window with the tool showing its usage, e.g. with the –help option.

This is not a distribution you want to install just to check email and perform other mundane Internet activities, though nothing stops you from using it just for those purposes. It is made available for public download as DVD installation images for both 32- and 64-bit architectures. And there are installation images for KDE and the GNOME desktop environments. Shown below is a screen shot of the boot menu. Unlike other Linux distributions, the system will not boot into a graphical desktop environment, but rather, into a console. You will then have to start the graphical interface by typing **startx** and pressing the enter key. The same is true after installation. The only difference is after installation, the system will boot into a login prompt. The default username that you must use to login is **root** and the password is **toor**. This applies to both the GNOME and KDE editions.

Because it is based on Ubuntu Desktop, the installation process is the same as that of any Ubuntu Desktop edition, although the latest edition uses an older form of the Ubuntu Desktop graphical installer. (BackTrack 5 is based on Ubuntu Desktop 10.04 LTS.) The only problem I have detected with the installer, as revealed by several comments here, is that it can be almost impossible to install the boot loader on a separate partition, when attempting to set up a dual-boot system with another distribution or operating system.

Shown here is a screen shot of the Advanced Partitioning Tool of the KDE edition.



As stated earlier, you could still use BackTrack for some regular computing activities, even though it was not really designed for such. For example, with Firefox installed out of the box, you could use it to surf the Web just as you would on any other desktop distribution. The very latest edition (Firefox 14) is even installed. And because the guys responsible for this distribution take security issues very seriously, the Firefox installed comes pre-loaded with add-ons that offer additional security when you are busy surfing.

Aside from Firefox and a handful of desktop accessories and system utilities, almost every application installed out of the box is designed for a specific pentesting activity. Rather than go through what would be a very long list of installed applications, the following screen shots should give you an idea of what BackTrack 5 has to offer. Note that all the screen shops were taken from a test installation of the KDE edition.

*This one shows applications in the **Information Gathering** > **Wireless Analysis** > **WLAN Analysis** category.*

*Applications in the **Vulnerability Assessment** > **Network Assessment** > **VoIP Fuzzers** category.*

*Applications in the **Exploitation Tools** > **Physical Exploitation** category.*

The list of applications in the Physical Exploitation subcategory is new to BackTrack 5, making their first appearance in BackTrack 5 R3.

*Applications in the **Privilege Escalation** > **Spoofing Attacks** > **VoIP Spoofing** category.*

*Applications in the **Maintaining Access > OS Backdoors** category.*

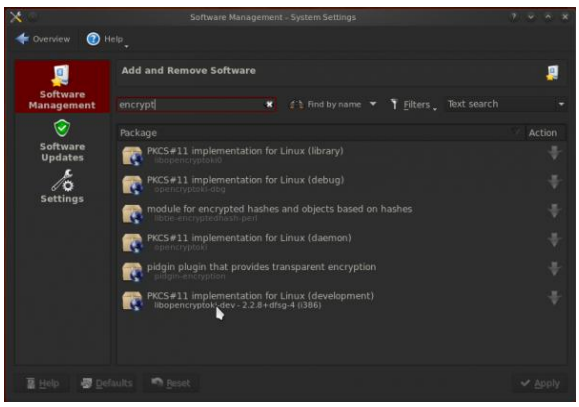
*Applications in the **Reverse Engineering** category.*

*Applications in the **RFID Tools > RFID Frosch** category.*

*Applications in the **Stress Testing > Network Stress Testing** category.*

*Applications in the **Forensics > Forensic Analysis Tools** category.*

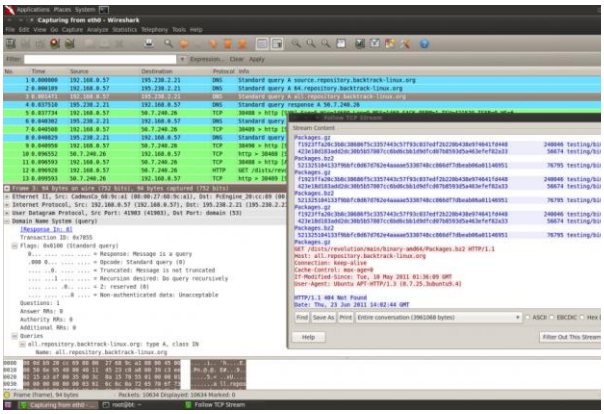
Though it is intended for users with more than a passing knowledge of managing and navigating a Linux system, all the graphical management applications that you will find on regular desktop distributions are also available on BackTrack. For example, in the KDE edition, installing and managing applications can be accomplished via the software manager module of KDE's System Settings.



Because BackTrack 5 is based on Ubuntu 10.04 LTS, all the applications available in the repository of that edition of Ubuntu are also installable on it. So you will still find packages for OpenOffice 3.2, when they are not available in the very latest edition of Ubuntu.

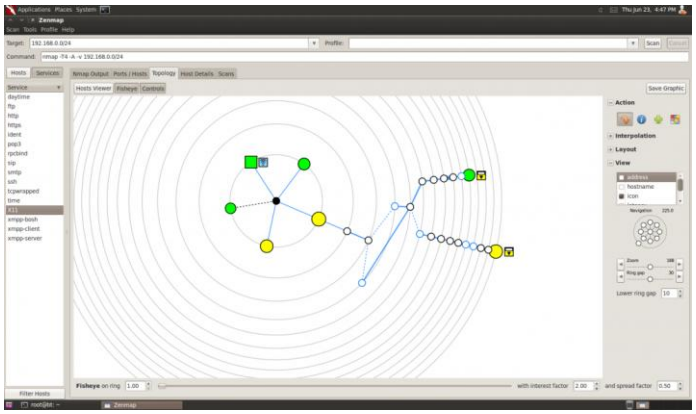
BackTrack is filled with a collection of more than 300 open source security tools, which you can find organized in different submenus of the "Backtrack" menu: "Information Gathering", "Vulnerability Assessment", "Exploitation Tools", "Privilege Escalation", "Maintaining Access", "Reverse Engineering", "RFID Tools", "Stress Testing", "Forensics", "Reporting Tools", "Services", and "Miscellaneous". Each submenu is further subdivided into subcategories. The developers have added a nice touch to menu items of commandline utilities: when you click on such a menu item, it opens a terminal window with the tool showing its usage, e.g. with the –help option.

Sniff a network with Wireshark



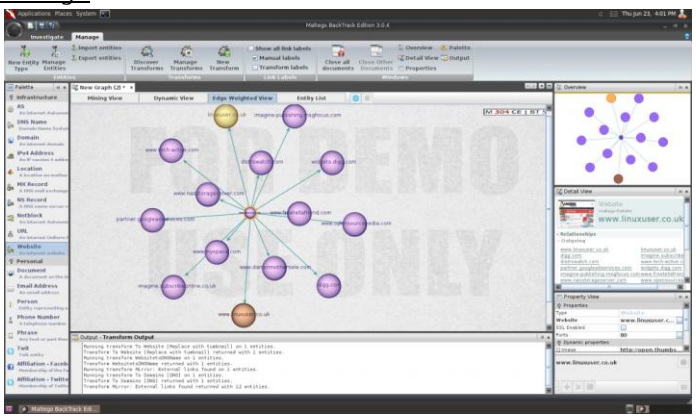
BT5′s software collection is really a security professional's dream. It has all you need to pentest a network, such as the exploit framework Metasploit, the network scanner Nmap, the network analyzer Wireshark, the browser exploitation framework BeEF, the information gathering tool Maltego, and so on. One disadvantage of BT5 is that you can't upgrade to it from BT4, which is a pity if you have installed and configured a BT4 installation in the past. Moreover, some interesting tools like Pyrit, which uses your GPU's processing power to accelerate WPA password cracking, and the vulnerability scanner OpenVAS have been dropped in BT5, although they can be installed manually.

Scan all hosts on a network with Zenmap



The bad thing about BackTrack is the documentation. It's scarce, fragmentary, and often outdated. Many tips and tutorials we found on the BackTrack website and its wiki were for older versions and didn't work on BT5, and other documents didn't spell out which version they were talking about. However, there are also some extremely detailed and very good documents on the website, and obviously documentation is a work in progress, so depending on what you need your mileage may vary.

Find all information you can about a website with Maltego



BackTrack is also more about the tools than about the distribution, so the lack of consistent documentation shouldn't be such a big problem. Moreover, BT5 is really Ubuntu 10.04 under the hood, so most of the documentation about the latter applies. BackTrack is sponsored by the company Offensive Security, and they offer a "Penetration testing With BackTrack" course if you want to train your penetration testing skills. Upon completion of this course, you are ready to take a security challenge in an unfamiliar lab, and after successful completion you receive the Offensive Security Certified Professional (OSCP) certification.

ACKNOWLEDGEMENT

The author likes to thank Sir Linus Torevald for designing and developing Linux and for making it open source. Also, special thanks to Mati Aharoni, Devon Kearns and the Offensive Security team for developing Backtrack and facilitating user friendly pentesting platform.

REFERENCES

[1] www.linuxuser.co.uk
[2] www.linuxbsdos.com