

Using LiveCDs to solve everyday problems

Computer forensics as a speciality has grown hand-in-hand with computer crime. As in all walks of life, as criminals have grown more sophisticated so have the methods used to investigate the crimes they commit.

However, the field of computer forensics has more to offer than just the investigation of crime. There are a surprising number of commonplace situations where forensic techniques can be useful. For example, what happens when the password to the root or administrator account of a computer is lost? Someone will need to break into that machine and reset the password in order that normal administrative tasks can be performed. The techniques used to break into a machine are part of the forensic specialist's toolkit, along with auditing tools, intrusion detection tools, and tools that allow data to be rescued from machines that will not boot.

It may come as something of a surprise to learn that many of the forensic tools in use today have not come from large corporate software houses linked to intelligence and police services but have come from the open source community. Although the open source community is sometimes characterised as being composed of anti-establishment hackers, it has a long history of producing leading security experts. The open source development model is such that security flaws are there in the source code for all to see and fix and this provides a wealth of security experience in the community. In particular Linux itself has become a widely used forensic tool through increasing use of bootable CDs, also known as LiveCDs. More recently, Pendrive Linux makes it possible to install a portable Linux operating system on a flash drive or USB key as an alternative to a LiveCD.

1 What is a LiveCD?

A LiveCD (or LiveDistro) is an operating system installed on a CD in such a way that it can be used to boot a computer into that operating system without any installation onto the hard drive of that computer being necessary. The majority of LiveCDs feature the Linux operating system along with a collection of software applications and work on computers with an x86 architecture, for example all IBM-PC compatible and more recent Apple Macintosh computers. LiveCDs are useful for showcasing the Linux operating system and selected software without installing onto the hard drive of a computer. They are also seeing increasing use as a way of booting a computer that cannot be booted from its own hard drive.

This could be because the operating system on the computer has suffered a catastrophic failure or perhaps because the machine has been compromised. Once the computer has been booted into the environment provided by the LiveCD then data recovery or system cracking tools can be used to rescue data or to repair the installed operating system.

There are a huge number of LiveCDs available, all of which are targeted at specific markets or groups of users. In addition to the various specialisms to be found amongst IT professionals there are LiveCDs aimed at the games and entertainment market, for educational use, targeting those requiring heightened privacy or those who wish to turn their computer into a media centre capable of playing multiple media formats.

2 A range of LiveCDs

There are many LiveCDs available each targeting a specific audience and a specific purpose. Examples include:

Ubuntu - an introduction to open source for the end user Ubuntu is a Linux distribution that has seen a huge surge in popularity over the last few years. It is based on Debian but has a frequent, predictable 6 month release cycle and a Long Term Support (LTS) version provides three years support on the desktop, and five years on the server. The project invests a great deal of effort in its desktop environment. Although Ubuntu is primarily used as an operating system installed on a computer's hard drive, the standard installation CD also acts as a LiveCD, allowing anyone to try Ubuntu out with the minimum of effort. It is also possible to run it from a USB memory stick. The LiveCDs available from Ubuntu are especially interesting as they are available for PCs and newer Macs with x86 architecture, and there is also a version for 64 bit computers. Several variants of Ubuntu exist including Edubuntu which is aimed at educational use.

Knoppix - general purpose and comprehensive Knoppix is an established and well known LiveCD based on Debian GNU/Linux and released under the GNU General Public License (GPL). Its fullest version, which comes as a DVD rather than a CD, comes with a host of open source software programs, from industry strength server programs such as the Apache web server, the MySQL database, and the PHP scripting language, to applications targeted at the end user, such as office suites and a range of email clients. It also offers a choice of desktop environments such as KDE and GNOME. All of the 2700+ software packages that come installed

on the Knoppix DVD require no further downloading, installation or configuration; the smaller CD version has just over 1000 packages. Although Knoppix is not targeted directly at the specialised field of forensics, it nonetheless comes with utilities for data recovery and system repair for a range of operating systems. It is possible to create your own customized version of Knoppix, a process known as remastering.

Helix 3 Pro - specifically aimed at forensic users Helix is a CD-based suite of tools targeted at the forensics field, including a bootable Linux environment that allows a computer to be investigated independently of its own operating system. It is produced by e-Fense Inc, a company specialising in incident response and forensic analysis, and is made available as a downloadable ISO image that can be used to burn a Helix CD. Despite containing some open source software, it is not clear that the entire Helix CD is covered by open source licences, as some of the tools on it are produced by e-Fense themselves. The Helix CD is only available to paid members of the e-Fense forum.

Dyne:bolic - specifically aimed at media creators Dyne:bolic is a Linux-based LiveCD featuring pre-installed applications for audio-visual creativity including Blender, a fully-featured open source 3D rendering package. Dyne:bolic also includes software to allow multiple computers to be operated remotely from a main workstation over a network, allowing you to distribute your workload over a number of machines. Dyne:bolic's creators promote its use as a tool to free creators from what they see as oppressive interference from large organisations.

3 The use of LiveCDs to solve everyday problems

Detailed forensic examination by professional forensic experts is undoubtedly one use of LiveCDs but they also offer opportunities for the less specialised IT professional and indeed the end user. There are many everyday problems that can be easily solved by using one of the many LiveCDs available today. Some examples of these include:

- Forgetting the Windows administrator password. This is such a common occurrence that many LiveCDs specifically cater for this situation. Instead of having to have detailed system administration knowledge of how to break in to a Windows machine and reset the administrator password, all the forgetful owner needs is a few moments with a LiveCD and it is taken care of.
- Rescuing data from a compromised machine. When a machine has been compromised it is often unsafe or inadvisable to boot that machine into its own operating system. This could be because it has had many of its system programs replaced and so local tools are unsafe, or perhaps because it is launching attacks against other machines across a network. In this situation it can be a life saver to be able to boot the machine safely and then be able to copy valuable data from the hard disk either to a removable storage or to another network device.
- Restoring deleted files. Many LiveCDs come with utilities to easily restore previously deleted files. In fact these utilities can even recover files and complete partitions that have been damaged or formatted. If a repartitioning operation runs into difficulties then being able to restore a partition that has been reformatted may save the machine from a complete reinstall.
- Virus checking. If a machine has been infected by a virus the safest option is to boot the infected machine from a LiveCD and clean the machine whilst its local operating system is not running. This situation ensures that no infected files are in use when the virus scanning is performed. Some LiveCDs are completely dedicated to scanning for and disinfecting viruses. Many LiveCDs, such as Knoppix, provide the Clam Antivirus virus scanner.
- Using a computer privately. As long as a user has the ability to reboot the computer, a LiveCD can be a powerful tool for using a computer without leaving traces. As all data is held in memory rather than being written to the hard drive, when a computer booted from a LiveCD is switched off, all traces of the user session disappear.

4 Further reading

Links

- Pendrive Linux <http://www.pendrivelinux.com>
- Knoppix <http://www.knoppix.com/>
- Helix <http://www.e-fense.com/helix3pro.php>
- Ubuntu <http://www.ubuntulinux.org/>
- Dyne:bolic <http://dynebolic.org/>

- A comprehensive list of LiveCDs <http://www.livedcdlist.com/>

Related information from OSS Watch

- Top tips for selecting Open Source Software
- Is open source software insecure? An introduction to the issues

Author: Elena Blanco

© 2005-2010 University of Oxford

This document is licensed under the licence:

<http://creativecommons.org/licenses/by-sa/2.0/uk/>

For further information on OSS Watch, the Open Source Advisory Service, see <http://www.oss-watch.ac.uk/>