An up-to-date overview of free software and its makers

Projects on the Move

Things have definitely been on the move over the course of the past month. Again, we picked the best of the bunch for you: the Samhain IDS, Linux on the Linksys WRT54G Wireless Router, and updates for Debian GNU/Linux Woody.

BY MARTIN LOSCHWITZ

Ronald Raefle, visipix.com

I f the KDE developers have kept to their schedule, KDE 3.2 should already be available for downloading from the usual mirror servers by the time this issue reaches you (the planned release date was February 2). The new version will introduce a range of enhancements to the menu system, performance boosts, and interesting new programs. The Plastik theme, which has been the target of many jokes to the effect that its name is the only thing wrong with it, has now been integrated with *kdeartwork*, and helps polish the KDE GUI. The expected integration of KDE and Gnome [1] also holds promise for the more distant future. But let's look at a more serious subject first, intrusion detection.

Samhain

It is becoming increasingly difficult to protect servers against intrusion. As the Debian project compromise and other

THE AUTHOR

Martin Loschwitz is from a small German town called Niederkrüchten and a developer for Debian GNU/Linux. Martin's leisure time is mainly preoccupied with activities in the Debian or GNU community.

attacks on Open Source projects show, vulnerabilities can be fatal. While programs like Apache or sendmail are fairly easy to update on the fly, a kernel update, as required to patch the vulnerabilities mentioned above, can mean rebooting your system. If you multiply this by the number of computers in your network, the going can be really tough. In datacenters that use a range of completely different machines, this means compiling a different kernel for each type of machine.

Kernel security holes are typically local. There is less danger if you do not have local users, or if your local users are trustworthy.

Issues that affect systems for multiuser access, where the user base may not be trustworthy, are far more serious. Administrators with a large number of machines that fit this description will typically be unable to avoid vulnerabilities in the software they use. The risk is much greater if known exploits are in the wild. There is no such thing as total security, or a one hundred percent guarantee of avoiding compromise.

This makes it all the more important to recognize an attack as soon as it occurs. Of course you could use MD5 check-

sums, but checksums are just one of many ways of discovering an intrusion after the event. Continually checking a system for suspicious files is an extremely time-consuming task. This has led developers to concentrate on creating ready-made solutions, so-called file integrity checkers, which belong to the Intrusion Detection System (IDS) category. Tripwire [2] and the free alternative Aide [3] are just two examples.

Samhain [4] an IDS by the Samhain Labs runs on a variety of platforms: Linux, FreeBSD, AIX 4, HP-UX 10.20, Sun's Solaris (2.6 and 2.8), UnixWare 7.1.0, and Alpha/True64.

Samhain is extremely flexible with respect to logging. It can collect logfiles on a central server – useful in larger networks. An encrypted connection is used between the client and the server. Samhain also offers an option for emailing logfiles, using its own mail server to do so, and thus avoiding disruptions caused by external mail servers. You can also save logging data to a PostgreSQL or MySQL database, or use a traditional approach with local, signature-protected files.

Samhain expects you to compile a list of files for it to monitor. The list also

Figure 1: KDE 3.2 is jam-packed with enhancements. The developers have not only considerable increased the program scope, but their are new themes such as Plastik, as shown here.
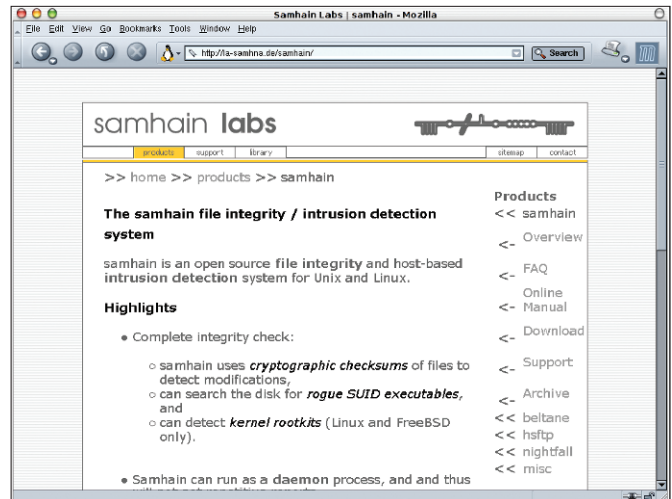

Figure 2: An Intrusion Detection System (IDS) to protect your hosts and networks is a good idea. Samhain recognizes file manipulation and immediately alerts the administrator.

contains file characteristics like SHA1 checksums and timestamps. The program uses a GnuPG signature to protect this file from manipulation.

It goes without saying that an intrusion detection system has to be hardened against attacks. If an attacker were to modify the IDS itself, the whole system would be useless. Samhain uses a GnuPG signed logfile and binaries compiled with a 64 bit key to provide this protection. The key is generated before compiling and included in each email message and logfile entry. If a message does not contain this key, the mail server will discard it.

Samhain can run as a daemon, and will head off into the background when launched. The IDS can also hide its own process to avoid detection. This assumes that an attacker who cannot see the IDS will not attempt to disable it – a kind of "security by obscurity". Samhain even has its own kernel module to remove any trace of its existence.

The Beltane [5] tool, also developed by Samhain Labs, is a Web interface that provides management facilities for Samhain installations in large networks. This does impose a few restrictions, however. For example, you need a database to store your logfiles. Check out the Samhain FAQ [6] or the Beltane website for more details.

No-brain attacks typically leave a few tell-tale signs – panic messages in the kernel logfile are always a cause for concern. But if you require enhanced security, there is no alternative for a file integrity checker.

Linux on the WRT54G

Some of today's hardware boxes have Linux pre-installed by the manufacturer. One of these is the Linksys WRT54G Wireless LAN Router.

Most people are not really interested in the device's firmware, as long as the box works just like the manufacturer promised. At the 20th Chaos Communication Congress (20C3 for short) [7] computer firmware played an important role. Among many topics, talks were held on how to identify a device's firmware. Hardware manufacturers are increasingly leveraging the power of Linux. Sadly, some of them modify the source code without publishing their changes, contravening GPL terms in an attempt to keep the details of their hardware secret. The CCC hackers have now taken it upon themselves to expose any violations of GPL terms.

Fortunately, Linksys is not in breach of the GPL. You can download the source code for the WRT54G firmware from the company's website at [8]. This led hackers to investigate the software shortly after the WRT54G was released. As you all know, the free software community is never satisfied with other people's offerings for very long.

Under the hood it has a MIPS CPU and 4MBytes of flash memory. The device has two external antennae, which cannot be exchanged for more powerful models.

The device has integrated support for 54 MBit/s wireless LAN (aka IEEE 802.11g) and also NAT router functionality to provide Internet access to the wireless network.

There are a few modifications that you can make to the WRT54G without actually modifying the firmware. Of course, uploading your own firmware image is always a risky thing to do. If the Access Point happens to lose power while you are updating its flash memory, the damage could be considerable.

If you do not want to risk replacing the firmware, you can exploit an error in the original firmware (this is only present in older revisions, as of 1.30.7, but not in the 1.41.x series). The Web interface of the configuration program allows you to ping other hosts on the network. The file that provides this functionality, *Ping.asp* accesses the shell command, *ping*, to do so; thus revealing Busybox [9]. In the vulnerable version, you can enter an arbitrary shell command in the IP address field, such as `ps ax > /tmp/ping.log 2 > &1`.

Messing about with the Web interface is slightly cumbersome. So why not use the Web interface to launch a shell? The "Wrt54gtools" [10] by C.J. Collier include both a shell and a telnet daemon that allows you to run commands with your normal shell. This allows users to remove bugs in the WRT54G firmware, such as the one in "ROUTER" mode, which can cause an issue with the WAN/LAN interface. This is easily

resolved using an *iptables* command.

The Web-based configuration interface also provides configuration options for the access point. The *wl_antdiv* and *wl_txant* parameters change the antenna power, and *et0macaddr* changes the MAC address of the access point. If you prefer not to use Web interfaces, you can use the *wl* tool on the router. You can even install the WLAN packet sniffer, Kismet [11].

If you are looking for a solid access point for home or small office use, the WRT54G is a likely candidate. The options you have, thanks to its Linux operating system, and the bug in the Web interface, are many and make the device an attractive proposition.

Updating Woody

The latest version of Debian GNU/Linux (3.1, code named Sarge) will be available some time soon. Unfortunately, users with systems based on the current stable Woody release have had wait patiently in the meantime. Recently, there has been an increase in projects aimed to make that wait as pleasant as possible. A few individual developers have taken up the cause of removing obsolete software from Woody.

The approach is to compile packages from the unstable branch (Sid) for Woody. In comparison with an upgrade to Testing this has the advantage of simply updating a specific program (and its dependencies). Downgrading from Testing to Stable is typically more tricky, and could involve a lot of manual steps.

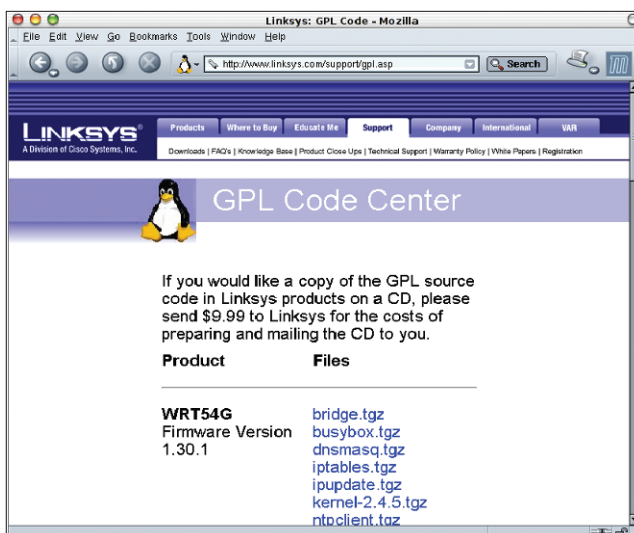The first volunteer to start backporting packages from Unstable to Stable was

Figure 3: Linksys is one of few hardware manufacturers to publish the source code of their modified Linux firmware. This allows experience Linux users to build their own Linux system for the WRT54G WLAN router.

Adrian Bunk. Adrian is a former developer with the Debian project, who left Debian as he was unsatisfied with Debian's release management. Adrian is upholding what has more or less become a tradition of backporting. Users who wanted to install Linux 2.4 on Debian GNU/Linux 2.2 (code name Potato) are probably quite familiar with the name.

The second project was launched by Norbert Tretkowski. The project's name reflects its goals. *http://www.backports.org* [12] provides backports of many unstable packages to Woody. Nearly every major program is represented, from XFree86 4.2, Vim, and Mozilla 1.5 to Apache 2.

The Dependencies Trick

The project is still a good thing. If you want to use apt to add backports to your system, you have to add an entry for each package to */etc/apt/sources.list*. The trick is that there is a *Packages.gz* file for each package in the directory, and this file includes the dependencies for the
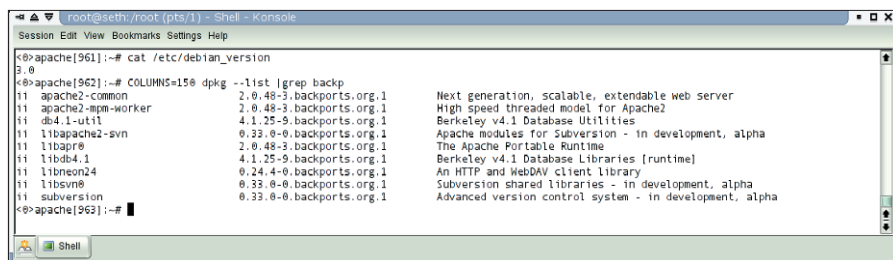
package in question. When you add a package, its dependencies are automatically resolved, without requiring any additional command line wizardry. You should avoid using the *http://www.backports.org* server for downloads, and use one of the numerous mirror servers at [13].

KDE 3 is probably one of the most important updates for desktop users. Version 3.0 appeared about ten days before Woody was released, and did not make it onto the Woody CDs. Fortunately, this is not a major issue, as every KDE mirror will provide current packages for Woody, mainly thanks to Ralf Nolden.

That's all folks...

... for this month at least. If you can recommend a program that you would like to see featured, why not mail me at [14]? I look forward to your comments! ∎

INFO
[1] KDE and GTK+ integration: *http://slashdot.org/article.pl?sid=04/01/10/1750257*
[2] Tripwire: *http://www.tripwire.org/*
[3] Aide: *http://www.cs.tut.fi/~rammer/aide.html*
[4] Samhain: *http://la-samhna.de/samhain/*
[5] Beltane: *http://la-samhna.de/beltane/*
[6] The Samhain FAQ: *http://la-samhna.de/samhain/s_faq.html*
[7] 20C3: *http://www.ccc.de/congress/2003/*
[8] Linksys GPL Download Center: *http://www.linksys.com/support/gpl.asp*
[9] Busybox: *http://www.busybox.net/*
[10] Wrt54gtools: *http://www.seattlewireless.net/index.cgi/Wrt54gTools*
[11] Kismet on the WRT54G: *http://www.seattlewireless.net/index.cgi/LinksysWrt54g#head-2755b98d6bf5b10da8a5d1cff01df93b319e51a6*
[12] Backports for Debian: *http://www.backports.org/*
[13] Backport mirror servers: *http://www.backports.org/mirrors.html*
[14] Tips and suggestions: *projects@linux-magazine.com*

Figure 4: Dpkg provides proof. Thanks to *http://www.backports.org* by Norbert Tretkowski, Apache 2 and Subversion will run on Debian Woody. XFree86 4.2 and Mozilla 1.5 are also available.