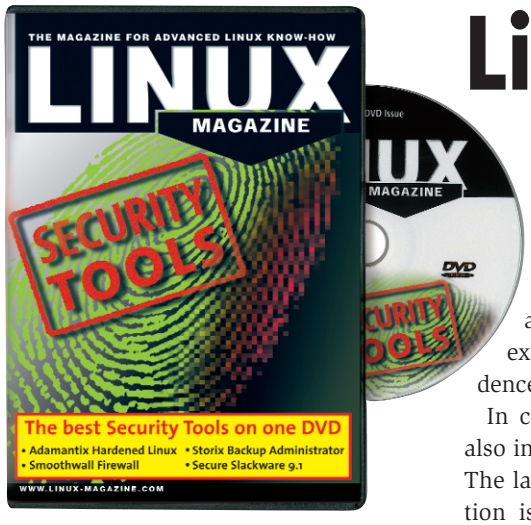

Linux Magazine DVD

This months DVD sees a host of security related applications. We start by having the Adamantix Installation.

This is followed up with Smoothwall Express 2.0. Smoothwall has a large following. This firewall can protect a local network from outside attack, while interfering as little as possible with user activities.

Storix Personal is also on the DVD. This will work as the full Administrator version for 30 days before reverting back to the personal version.

Storix System Backup Administrator (SBA) is a graphical interface for administration of various types of Linux system backups. SBA was designed not only to backup data files to a network server, but to also provide the ability to reinstall a complete system from scratch while providing the flexibility needed to restore the backup onto a different hardware environment.

SBA was designed to perform the difficult task of recovering a Linux system that other backup products avoid. Unlike other "bare-metal restore" options, SBA understands your Linux system and configuration. When reinstalling a system, the configuration is then tailored to work with your new hardware configuration. In addition, you can completely re-customize your system during the system installation process, by changing filesystem types, adding software RAID devices, converting to LVM partitions, and much more.

Just hitting the newsfeeds is "The PacketMaster". This is not just a boot and run distribution. It contains a collection of security and forensic utilities so you can examine and, if needed, collect evidence of tampering.

In case that is not enough, we have also included images of Trustix and Fire. The latest Slackware 9.1 Linux distribution is also included with the newest Slackware Administrators Security Toolkit (SAStk) to ensure it is as secure as possible.

Installing Adamantix

The Adamantix Installation DVD has taken the distribution a step closer to its goal of bringing usability to high-security Linux. However, the installation routine is not for the faint-hearted. Before you deploy Adamantix as a VPN router or firewall in a production environment, it makes sense to perform a test installation and get to know the operating system.

Although Adamantix is based on Debian, and has adopted a few approaches from Debian, the installation DVD does its own thing. It does not use the Debian installation program, but instead an installation routine based on Timo's Rescue CD. In other words, you can use the DVD as a rescue medium that automatically recognizes most of your hardware. The DVD also includes a good collection of tools that help you tackle installation problems, such as *fsck*, *parted*, and *memtest86*.

The installation routine comprises a few simple shell scripts which leverage *dialog* to provide a well-organized menu-based interface. The script collection is also available as an Adamantix package. You can look forward to changes in the near future, as soon as the developers complete their task. The long-term goal is to replace the installation routine, and instead use a C++ variant.

If you intend to install Adamantix off the Internet, you should start by installing a minimal Debian Woody on your hard disk, and then refer to the "Installation" box in the Adamantix article.

Step by Step

After booting from the DVD, you can opt to boot the system "normally", that is link in the DVD as a loop. This will mount */var* as *tmpfs* to allow variable data such as logfiles to be written. The alternative is to copy the DVD to a RAM disk. This approach is recommended if you have enough memory. And in this case, "enough" means more than 256

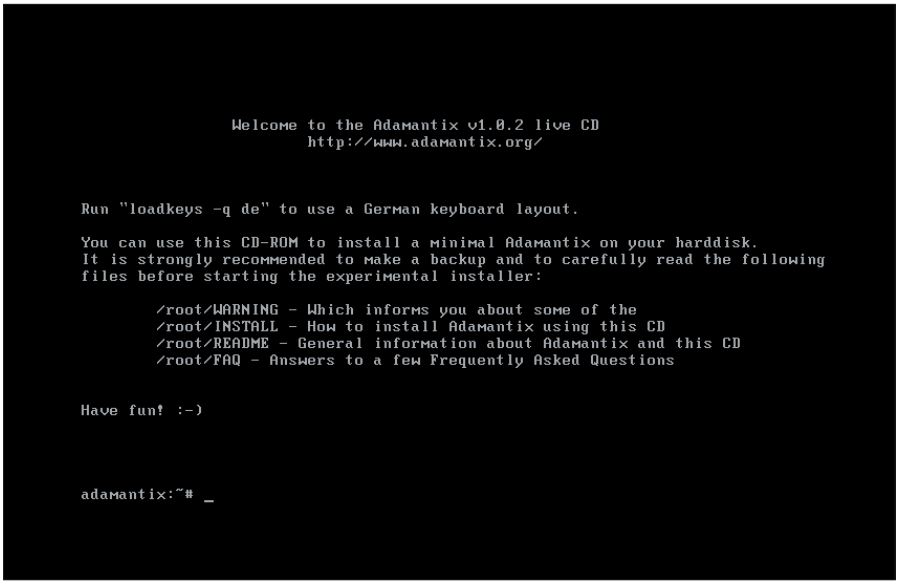

Figure 1: The welcome screen provides useful installation tips.

MBytes as the image takes up 220 MBytes. If you do not have enough RAM, you can expect kernel panic.

The boot process ends with the welcome message shown in Figure 1. After booting you will find yourself in the */root* directory. The directory contains usage notes and a warning: the current version cannot ensure the integrity of installations on your hard disk. According to Peter Busser, the initiator of the Adamantix project, at least one boot block on your hard disk will be overwritten, so you will need to re-configure the boot loader (Grub in this case).

If you are experimenting with Adamantix, we would definitely recommend the use of a test machine. A security-enhanced distribution at the current stage of Adamantix' development is a complex thing. Adamantix explicitly makes no attempt to hide this complexity from the user.

You can enter *adamantix-install* to launch the installer in the shell. The script again warns of the potential danger in Step 1 (see Figure 2) and recommends a backup of your current data. For those of you who do not need international keyboard support, the next step is to partition the hard disk(s). You can opt for the traditional *fdisk* approach, a "user friendly" approach with *cfdisk*, or the easy way out with *parted*. If you have multiple hard disks in your machine, make sure you select the correct disk before you continue.

It is a very good idea to create multiple partitions for the filesystems. The installation tends to grind to a halt if you fail to do so.

After partitioning the disk, an overview of the partitions is displayed. Select *continue* to close the overview. This will actually initialize the swap area(s) you defined. Now go on to specify the partition to be used for the root filesystem (/). As the partitions do not actually contain any filesystems, the next step is to create those filesystems. You can select from the "usual suspects" (Ext2, Ext3, and ReiserFS), or opt for XFS (see Figure 3). The selection of mount-points in the next step is more or less self-explanatory.

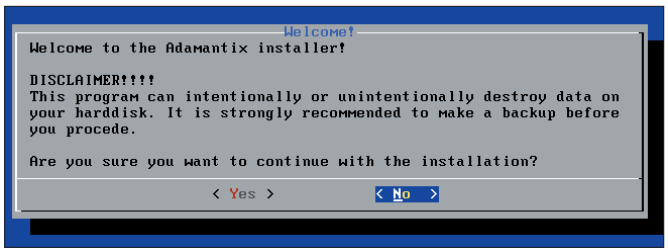

Figure 2: Make sure you take warning seriously, before you launch into the installation.

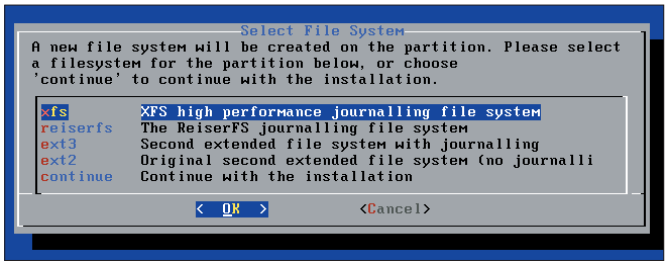

Figure 3: Adamantix is one of only a few distributions that allow you to create an XFS filesystem during the installation phase.

Network Business as Usual

The network configuration that follows is also quite straightforward. You can specify an IP address or opt to use DHCP. The latter option caused a problem on one of our test machines. The NIC did not initialize and the whole installation failed. If you have DHCP, you do not need to enter a default gateway in the next screen. If you specified a static IP, you will also need to supply the IP address of the gateway.

In a similar way, you can either assign a static DNS server address, or use the configuration supplied by your DHCP server. The next step prompts you for the host and domain names.

After configuring the timezone, you are prompted to select the Adamantix mirror which you will be using to download the Adamantix packages. The DVD itself does not contain any Adamantix packages. Instead the most important programs are provided as compressed images. You can download anything else you need from mirror servers, following the traditional Debian approach. Security updates are available from a dedicated server – another Debian-style trait.

The last step in the installation procedure prompts you to specify the location of the boot loader, Grub. Grub simply needs to know where the component that the BIOS calls to boot the system should be written to your disk.

This can be the a boot sector on one of your partitions or the MBR. This completes the installation. If all goes well, your system should fire up an Adamantix environment after rebooting.

Installation Pitfalls

As the installation DVD is still experimental, a few bugs are to be expected. The biggest issue that cropped up during our installation test was the fact that the installation routine was incapable of initializing the Grub boot loader if */boot* occupied a filesystem of its own. The system failed to find the kernel when booted. For this reason, you should avoid swapping */boot* out.

But it would be wrong to assume that a single, large / filesystem would be a better choice. In fact, the installation routine crashes when you try to select the root filesystem. The best approach is to create at least / and */var*, allowing you to work around the problem.

Unfortunately, it is not always easy to recognize installation errors immediately after they occur. On the upside, console 7 (*Alt+F7*) allows you to look under the hood. This quickly reveals most errors. ■

Features

Adamantix: Highly secure but useable Linux distribution.

Smoothwall: Express A Firewall operating system distribution based on Linux.

Storix: A powerful system backup administrator.

The PacketMaster: The latest security distribution with forensic tools.

Trustix: Secure Linux distribution for servers

Fire: A Forensic and Incident Response Environment

Slackware: With the addition of SAStk, this is a secure version of the popular Slackware distribution.

Tripwire: Intrusion detection and integrity checking.

Snort: A network intrusion detection system, capable of performing real-time traffic analysis.