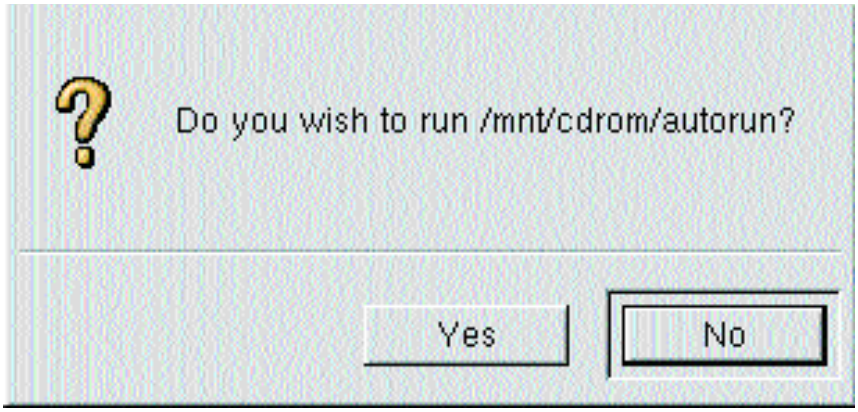
SECURITY

If you acquire a current Linux distribution, you will rightly expect it to have the latest software. We've taken a look at the versions of a few selected packages.

Security				
-	SuSE Linux 7.2 Personal	SuSE Linux 7.2 Professional	Red Hat Linux 7.1 Deluxe Edition	Red Hat Linux 7.1 Professional Edition
Up-to-dateness				
Auto-update?	yes, automatic or manual selection	yes, manual and automatic selection	for a charge, choice of scope	for a charge, choice of scope
Base: Kernel	2.4.4	2.4.4	2.4.2	2.4.2
Base: Glibc	2.2.2	2.2.2	2.2.2	2.2.2
Base: X11	4.0.3	4.0.3	4.0.3	4.0.3
Base: KDE	2.1.1	2.1.1	2.1.1	2.1.1
Base: Gnome	1.4.0.1	1.4.0.1	1.2.4	1.2.4
Programming: gcc	2.95.3	2.95.3	2.96	2.96
Programming: lPer	5.6.0	5.6.0	5.6.0	5.6.0
Programming: Python	2.0	2.0	1.5.2	1.5.2
Programming: Java JDK	1.1.8	1.1.8v1	?	?
Server: Apache	1.3.19	1.3.19	1.3.19	1.3.19
Server: WuFTP	-	2.6.0	2.6.1	2.6.1
Server: Sendmail	8.11.3	8.11.3	8.11.2	8.11.2
Server: Samba	-	2.2.0	2.0.7	2.0.7
Server: Bind	-	9.1.2	9.1.0	9.1.0
Bug found / Advisory on				
Man-S Heap Overflow	No / 29.05.	No / 29.05.	No / 21.05.	No / 21.05.
NEdit Temp File Creation	- / -	No / 19.04.	No / 08.05.	No / 08.05.
Samba TMP Symbolic Link	- / -	No / -	yes / 14.05.	yes / 14.05
Ntpd Buffer Overflow	- / -	No / 09.04.	No / 08.04.	No / 08.04.
Linux sysctl() Kernel Reading	No / 17.05.	No / 17.05.	No / 16.04.	No / 16.04.
Bind 8 Transaction Signatures Buffer Overflow		- / -	No / 31.01.	No / 29.01.
Secure configuration				
Security profiles	4	4	3	3
Firewall configuration	Pre-configured	Sample configuration	Gui-Tool	Gui-Tool
Unnecessary on pure client?	No	No	rpc.statd	rpc.statd
Security-Scanner	No	Saint, Nessus, Nmap	none	none
Intrusion Detection System	No	Snort, Tripwire, AIDE	Tripwire	Tripwire
IpSEC, VPN	No	FreeSWAN	No	No
Other special features?	Crypro file system	Crypro-FS, Amavis, Kerberos	Kerberos	Kerberos
Assessment	++	++	+	+

The viability of programs is also closely linked with their security. If a loophole is discovered, it must be closed, and this usually happens by means of an upgrade to a new version. Our test therefore also includes six randomly selected security loopholes that cropped up in recent months. We ask whether the version in the distribution displays these loopholes and whether the manufacturer has published an advisory in this respect.

We also expect a secure configuration, in which there is a choice of several security profiles, as well as support for the configuration of a firewall and a few security tools.



Gnome only executes the Autorun file from the CD on Red Hat after a confirmation – but in Red Hat's KDE installation this prompt is missing and thus opens a security loophole

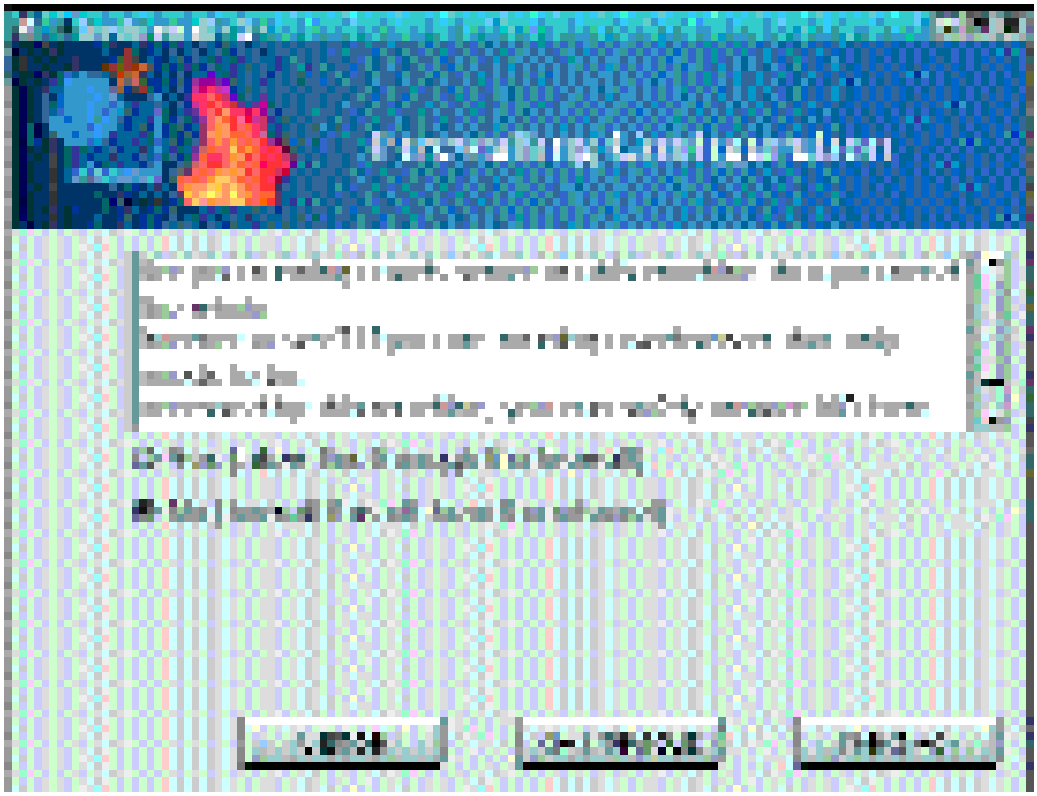
SuSE Linux 7.2 Personal

The ultimate security measure is to have no services running and SuSE Linux 7.2 Personal achieves this with aplomb; because no services are running it is perfectly secure. It does come equipped with Sendmail and Apache but these are switched off by default. Otherwise the trimmed down version is on a par with the Professional version.

SuSE Linux 7.2 Professional

The test SuSE Linux 7.2 Professional also passed our checklist of current security loopholes with flying

Mandrake Linux 8.0 Power Pack	Mandrake Linux 8.0 Pro Suite	Caldera Open Linux Workstation 3.1	Caldera Open Linux Server 3.1	Progeny Debian 1.0
Yes	Yes	Yes	Yes	Yes, but no choice
2.4.3 / 2.2.19	2.4.3 / 2.2.19	2.4.2-11	2.4.2-11	2.2.18 default, 2.4.2 can be installed later
2.2.2	2.2.2	2.2.1	2.2.1	2.2.1
4.0.3	4.0.3	4.0.2	4.0.2	3.3.6/4.0.2
2.1.1	2.1.1	2.1	2.1	2.0
1.2	1.2	-	-	1.2.4
2.96	2.96	2.95.2	2.95.2	2.95.2
5.6	5.6	5.6.0	5.6.0	5.005_03
2.0-9	2.0-9	1.5.2	1.5.2	1.5.2
1.3	1.3	1.3	1.3	-
1.3.19	1.3.19	1.3.19	1.3.19	1.3.9
2.6.1	2.6.1	-	2.6.1	Bsd-ftpd 0.3.2
8.11.3	8.11.3	8.11.1	8.11.1	postfix 2000531
2.0.7	2.0.7	2.0.8	2.0.8	2.0.7
9.1.1	9.1.1	-	8.2.3	8.2.3
No / -	No / -	yes / -	yes / -	No / -
yes / 25.04.	yes / 25.04.	yes / -	yes / -	- / 27.04.
yes / 21.05.	yes / 21.05.	No / 18.05.	No / 18.05.	yes / 09.05.
No / -	No / -	No / 06.04.	No / 06.04.	No / 09.04.
No / -	No / -	No / 03.04.	No / 03.04.	yes / 16.04.
No / 29.01.	yes / 29.01.	yes / 29.01.	No / 29.01.	No / 29.01.
6	6	No	Server profiles	No
Gui-Tool	Gui-Tool	Webmin	Webmin	No
No	No	No	No	No
-	-	none	none	none
Portsentry	Portsentry	none	Tripwire, Portsentry	none
FreeSWAN	FreeSWAN	No	No	No
-	-	supports Volution	supports Volution	-
++	++	0	0	+



Two simple security mechanisms are provided by Mandrake for the beginner: Three complete security stages and a firewall which can be configured via simple prompts

colours. The online update makes it easier to play in security updates as soon as they appear. In SuSE's software fund, security-conscious users can also find cryptographic solutions as well as monitoring and security tools, while the network manual offers an introduction to problems.

Red Hat 7.1 Professional and Deluxe

Apart from the Samba version 2.0.7, all other system utilities are sufficiently current, so only one of our test loopholes actually exists. It is also very easy to keep the system up to date using the online update via the Red Hat Network, but at just under 20 dollars per month, this is very expensive. The firewall configuration gave a positive impression during the installation. Here the user can choose between three profiles or manually open individual utilities or ports.

Red Hat installs an auto-mounter for the local X11 user. This monitors the CD or DVD drive and mounts the media if they are in the drive when you log in or if they are inserted later. After that, *autorun* is searched for and prompted under Gnome as to whether it is to be executed. Under KDE there is no such prompt with Red Hat, and *autorun* is executed with user rights.

This opens up a security loophole: The fact that CD burners and self-burned CDs are so common means a Trojan Horse or a worm could easily be introduced. The user doesn't even have the option of checking a suspect CD safely. The problem can be corrected by removing the entry for *autorun* from the autostart group of KDE.

Mandrake 8.0 Power Pack/Pro Suite Edition

In Mandrake the kernel is installed in version 2.4.3;

Progeny Debian 1.0: conclusion

Anyone who uses Debian will soon learn what goes on behind the scenes of a Linux system. And Progeny does not change this much. Even if the installation routine, with the appropriate hardware, ensures that one can achieve a working system considerably quicker than with dpkg, one should not expect the comfort and looks of the graphical installers from other distributors. On the other hand, when it comes to the updates for Debian packages, apt-get is still unrivalled as a command line tool.

The new Progeny configuration tools embedded in the Gnome Control Center ensure that even Debian newbies can soon deal with a range of standard configuration tasks, but here again other distributors are ahead in many respects.

Since Progeny is a distribution tailored for the American market, installers should be familiar with the American keyboard layout.

but there is also the option of a kernel 2.2.19. The main new functions and modules of the 2.4.4 kernel, though, are already integrated in Mandrake in kernel 2.4.3.

Samba is only installed in version 2.0.7, although for some time now a corrected version 2.0.9 together with the current 2.2.0 would have been available. And there is also room for improvement with the installed Apache version 1.3.19, as version 1.3.20 has come out.

Mandrake is a bit negligent in the fact that an installed utility is basically activated automatically. There is only a brief warning message and to compliance with the security updates.

Caldera Open Linux 3.1 Workstation/Server

Of the six security bugs tested, three slipped into the latest version of Caldera. By the time we closed for press there had been no advisory from Caldera on the "Man -S Heap Overflow" for any of their Linux versions.

But Caldera is using version *man-1.5h1*, which has the aforementioned bug. The test command then also leads to a segmentation fault:

```
$ man -S `perl -e 'print ":" x 100'` ls

Segmentation fault
```

It's a similar picture with the "NEdit Temporary File Creation" – no advisory, but the shaky version 5.1.1. A little test shows how simple it is to exploit the loophole. User A makes a symlink in */tmp* named *~x*, which points to */home/B/target*. User B then opens the file */tmp/x* with *nedit* and changes a large amount of text, without backing up the file. Nedit now tries to create an incremental backup - but unfortunately this lands in */home/B/target*. The old content of *target* is thereby overwritten.

Caldera delivers version 2.0.8 of Samba, but this does not correct the "Samba TMP file Symbolic Link" bug. In this case there is in fact an advisory, but it did not come out until after the *Creation Date* of the RPM archive. We can only hope for an update soon.

Calling up *lsof -i* shows that Caldera is very cautious with the services started. The only unusual things are the *slpd* (SLP Service Agent) and the *calserver*, part of the *Cameleo* package from Caldera. The server variant is equipped with additional security programs such as Tripwire.

Progeny Debian 1.0

Since Progeny is based on Debian 2.2, not all the packages out of the box are quite dew-fresh. At *http://archive.progeny.com/progeny/updates/newton/* or at the nearest Debian mirror there are always updated packages available (including for Gnome 1.4). Debian is also famous for providing security updates extremely quickly. Anyone using the graphical package manager front-end, only has the option of updating all the packages at a single stroke.

An update to the 2.4 kernel, also supplied, boils down to manual work. Progeny supplies neither a selection option during the installation, nor an explicit introduction in the manual. ■