

KNOPPPIX HACKS™

Includes
Knoppix on
CD-ROM

*100 Industrial-Strength
Tips & Tools*



O'REILLY®

Kyle Rankin

HACK
#46

Check for Root Kits

Use your Knoppix CD as a safe "known good" system for scanning your Linux install for root kits.

The root user on a Unix system has always held a bit of mystique. The power to create and destroy user accounts on a whim has gone to many system administrators's heads. System administrators aren't the only ones who seek the power of root, however. Attackers have long sought to exploit the security holes in a system to illegally gain root access.

A *root kit* is a system of scripts that uses a security exploit to help an attacker obtain and maintain root access on a system. These scripts often clear logs and replace important system binaries, such as *ps*, *find*, and *su*, among others, with modified versions to further hide his tracks.

A single root kit is as damaging as a single lie. Just as Baltasar Gracian said, "A single lie destroys a whole reputation of integrity," a single root kit destroys a whole system's integrity. If an attacker has root access, he has free reign to your system. The result is that you can't trust the information in your system. Processes might be hidden, files might be hidden, and even kernel modules might be hidden. Programs like the *chkrootkit* can scan system binaries for root kits, but when *chkrootkit* is run from inside a rooted system, even it might be fooled.

Advantages to Scanning with Knoppix

If you are unsure whether your system is compromised, the solution is to scan for root kits from a system that is known to be clean. There are advantages to scanning a system for root kits with Knoppix:

- Knoppix runs from read-only media. As long as Klaus Knopper's system doesn't get rooted, once a CD image is known to be clean, there is no way it can be compromised later. This means that even if the version of *ps* and *find* are compromised on your system, Knoppix's versions are fine.
- Your OS is powered down. This means that any hidden kernel modules or hidden processes are no longer running, so you are able to scan the system when it is frozen in time. Also, this means that no processes are running that can potentially detect that you are scanning the system.

There are, however, a few limitations when using *chkrootkit* with Knoppix. Knoppix is running *chkrootkit* from a system that has been rebooted, so *chkrootkit* can scan only files on the system, not anything in memory. Also, *chkrootkit* is a signature-based scanner. That means that it looks for certain

fingerprints popular root kits are known to have. If an attacker wants to evade detection, she could simply change the root kit so that its signature differs from the one on *chkrootkit*.

Got Root?

Using Knoppix to scan a system for root kits is pretty straightforward. Identify and mount the partitions you want to scan by clicking the hard-drive icons on your desktop. You don't need to mount the partitions as read/write for scanning. Once you have identified the partition to scan, open a terminal and type:

```
knoppix@tty0[knoppix]$ sudo chkrootkit -r /mnt/hda1
ROOTDIR is `/mnt/hda1/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not infected
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
. . .
Searching for suspicious files and dirs, it may take a while...
/mnt/hda2/usr/lib/j2re1.4.2/.systemPrefs
/mnt/hda2/usr/lib/j2re1.4.2/.systemPrefs/.system.lock
/mnt/hda2/usr/lib/j2re1.4.2/.systemPrefs/.systemRootModFile
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
. . .
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... nothing deleted
```

Replace */mnt/hda1* with the path to your mounted partition. Scan the output for any warnings, worms, or root kits. Be careful for false positives, particularly when *chkrootkit* is searching for suspicious files and directories. Files are considered suspicious if they have a large number of system calls. Certain

files (in my experience, Java plug-ins in particular) trigger this scan. If you are unsure, simply double-check the suspicious files for any strange code.

If you do find a root kit on your system, consider all of the files on the system suspect. **Back up important data and configuration files to audit later [Hack #47]**, and reinstall your system. You can never fully trust a system that has had root compromised, so a reinstall is the safest option.