CIO CORNER

This new column will focus on secure computing, providing tools and tips for those in the information security trenches. Each issue, we'll evaluate new technologies (primarily in the open source space) and discuss ways to integrate them into your organization.

We want to hear from you! Got a great utility or "magic" script that's saved you hours of tedious keyboard pounding? Something new we haven't heard about? Let us know at ciocorner@sandstorm.net.

Knoppix Rocks!

Knoppix is a Debian-based Linux distribution, neatly packaged on a bootable Live-CD. Unlike other distributions, it doesn't require a lengthy installation to become useful. Just boot from the disc and you've got a full-featured operating system, ready to go.

In fact, Knoppix was designed to be self-contained. It won't modify your hard drive or otherwise interfere with existing OS installations unless you tell it to. The only exception is swap space, which is used if an appropriate partition is found during startup (though this feature can be disabled). Instead, a RAM disk is created during bootup, and is used for home directories, config files, logs, etc. By default, disk partitions are mounted "read-only" (but can of course be re-mounted "writable" through the command line). Coupled with tools and utilities found on the disc, this makes Knoppix an ideal option for data recovery or forensic investigation of a PC.

The Knoppix distribution provides a wide assortment of open source applications. It's a complete desktop system, with all of the things we've come to expect on the desktop: office applications, web browsers, instant messaging, multi-media apps, etc. What's more, there are several choices of applications in each category. For example, if you're looking for a word processor you'll find OpenOffice.org, AbiWord and KWrite. There are over 1700MB of similar choices on the disc, made possible by the compressed filesystem used by Knoppix.

The Live-CD concept isn't new, and isn't unique to Knoppix. Linux distributions have been offering live discs for years. But you don't have to be first to be popular. The project has gained its strong following because the creator, Klaus Knopper, did it right. It's a one size fits all sort of project. There are so many applications on the disc that nearly everyone finds it useful.

Every PC and help desk technician should have a Knoppix disc in their CD wallet, if only for the data recovery aspects of the system. Network and security engineers will find the diagnostic and penetration tools such as Ethereal, Nessus and Nmap to be invaluable. It's even great as a simple workstation – and doesn't require licensing fees.

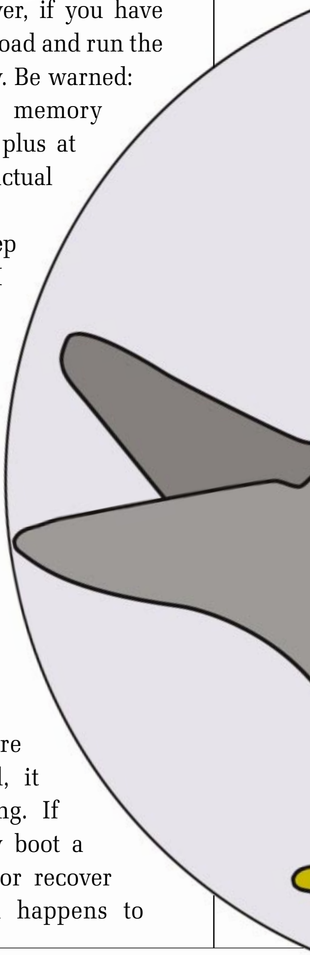
Knoppix is completely customizable. Although not for the faint of heart, any aspect of the system can be modified. Several projects have formed around the net, offering custom-made Live-CDs based on Knoppix, with their own distinct objectives. For example, Knoppix-STD (security tools distribution) focuses primarily on tools useful to the security professional. Another noteworthy project is Morphix, which takes a modular approach to the construction of the distribution. Instructions for the re-mastering process are available on knoppix.net. Additionally, software developers can use Knoppix as the basis for their own Live-CD demonstration.

These examples are fantastic for people who already know how to use the tools, but what about regular people? The real strength of Knoppix is that it lowers the entrance requirement to Linux. All you have to do is boot off the CD. If you don't like it, you can just take it out of the drive and go about your day. If you do like the system, but screw it up while trying to figure it out, just reboot – it'll be ok.

There are some realities of running an entire OS from a CD that you'll have to accept. Because Knoppix uses on-the-fly decompression, the system has a tendency to become unresponsive at times, while the drive spins-up to access something new. However, if you have RAM to spare, you can load and run the entire image to memory. Be warned: this requires a lot of memory (the entire image size, plus at least 128MB to run actual applications).

It is important to keep in mind that the RAM disk will be cleared when the system is powered off. Data created during a session that you wish to preserve must be copied to another system or written to disk. Another option would be to mount a remote volume on top of the "knoppix" users' home directory.

While the hardware auto-detection is good, it won't detect everything. If your goal is to quickly boot a system to fix a drive or recover data, and the system happens to



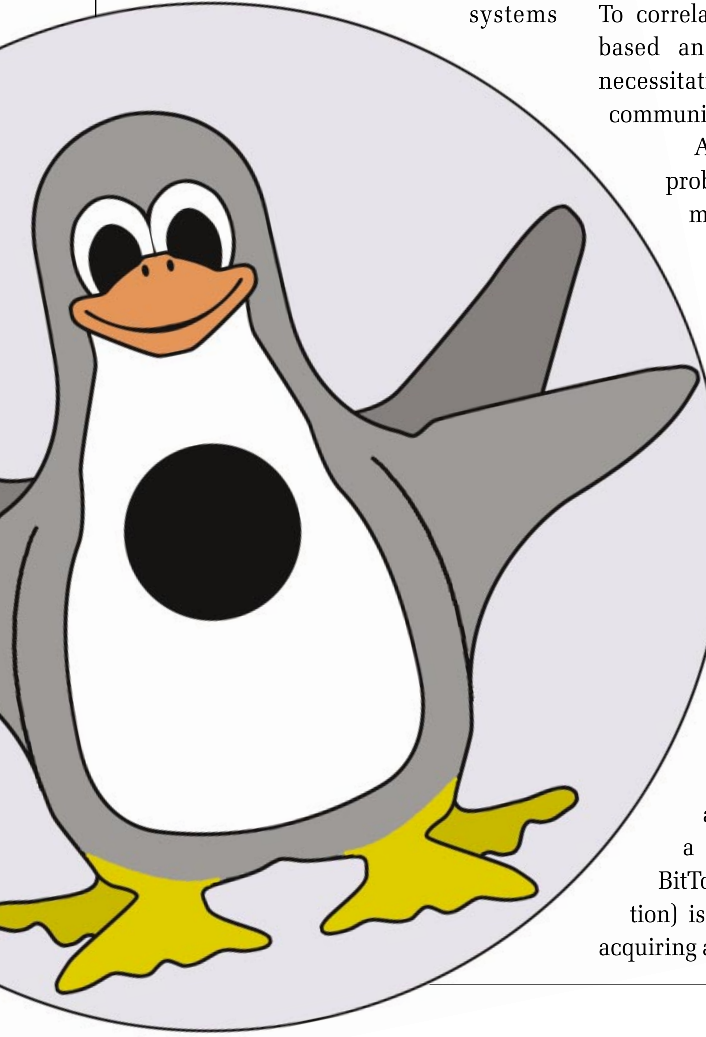
contain some critical piece of hardware that is unsupported, you've immediately forsaken the "quick" component of your plan. The remastering process takes quite a bit of time, and diagnosing driver problems may be more trouble than its worth.

From a security standpoint, Live-CD distributions like Knoppix make for an excellent addition to an administrator's toolkit. But the wide availability and ease of use of systems like this should serve as a reminder of the importance of physical and network security. An attacker may be able to use such a system to bypass host-based security restrictions, even recover passwords and other critical data from a PC's hard drive. Tools like Ettercap can wreak havoc on a LAN. What's more, a Knoppix session is almost impossible to detect using host-based forensic techniques (remember: Knoppix doesn't touch the hard drive). To correlate such a session, network-based analysis would be required, necessitating surveillance of host communication.

Again, this isn't a new problem. Your network isn't any more or less secure because Knoppix exists, and someone might use it to do something bad. Security measures should already be in place to defeat these kinds of attacks. It does however tend to defeat the argument that such attacks are unlikely since they require a high level of technical savvy.

Downloading Knoppix is a bandwidth intensive endeavor, as the iso is about 700MB. While traditional file transfer methods are available (http or ftp from a collection of mirror sites), BitTorrent (a peer-to-peer application) is usually the best method of acquiring a new release. Also, discs may be purchased and shipped via postal mail from a variety of online retailers.

The recent popularity and press coverage of this system stem from the project's fundamental characteristic: it's incredibly useful. After using it for awhile, you might even find it fun (check out Frozen Bubble in the games folder). Knoppix rocks! CDM



REFERENCES:

- http://www.knoppix.org/
- http://www.knoppix.net/
- http://www.openoffice.org/
- http://www.abisource.com/
- http://kate.kde.org/
- http://www.ethereal.com/
- http://www.nessus.org/
- http://www.insecure.org/nmap/
- http://www.knoppix-std.org/
- http://morphix.sf.net/
- http://ettercap.sf.net/

Walker Whitehouse *is CIO of Sandstorm Enterprises and* **Mike Yamamoto** *is a Network Systems Engineer at Sandstorm. Sandstorm Enterprises develops aggressive software products for network monitoring, network forensics analysis, and security auditing including telephone scanning, penetration testing, and vulnerability assessment.*