Kernel 2.6 rootkits and the quest for Linux security

BREAKING IN AND KEEPING OUT

Your Linux system may not be so airtight after all. To understand the threats, you need to think like an intruder. We'll show you what the intruders are thinking now about the Linux 2.6 kernel. **BY JOE CASAD**

Of all the most devilish creations in the history of cyber crime, the rootkit is perhaps the most ingenious. A rootkit is a bundle of tools for the network intruder. An attacker who gains access to a computer can upload the rootkit and use the tools to gain control of the system. One interesting aspect of a rootkit is its ability to cover the intruder's tracks. Doctored-up versions of common monitoring utilities such as netstat and ps hide any sign of the attack.

Many, many rootkits were copied onto many computers around the world. But eventually, developers and security specialists grew wise to the ways of user space rootkits. Experts learned to detect the intruder's presence by looking behind the standard Unix tools for evidence of changes. But rather than giving up, the intruders went on to something new. The kernel rootkit is a new generation of intrusion tool that weaves itself into the Linux system at a very deep level – below the reach of any userland detection tools. Armed with the kernel rootkit, the intruders again gained the upper hand – at least temporarily.

The Linux 2.6 kernel implemented several changes that made it much more difficult to create a kernel rootkit for Linux. But is the battle really over? In this month's cover story, security expert Amir Alsbih shows why you still need to worry about kernel rootkits in the Linux 2.6 kernel. Our leadoff article, "Secret Weapon: Rootkits for Linux kernel 2.6" offers a practical look at how a kernel 2.6 rootkit could work and what it would look like.

Lest you think that all the innovations are coming from the black hats, we also take a look at the two leading Mandatory Access Control (MAC) security systems for Linux. With AppArmor and SELinux, an intruder who exploits a vulnerability to gain access to a Linux computer may never have the necessary privileges to get started with taking control. Security expert Ralf Spenneberg shows how to protect your system with AppArmor, which is sponsored by Novell, and SELinux, the tool of choice for Red Hat systems. To top off this look at Linux intrusion security, in our final article, spokesmen for Novell and Red Hat square off on the costs and benefits of AppArmor and SELinux.

We hope you enjoy this month's cover story on rootkits and Linux security. ■

COVER STORY

How to Write a Rootkit 22
AppArmor 30
SELinux 36
AppArmor vs. SELinux 40