Looking for signs of a network attack

CAT AND MOUSE

If you think your systems are too obscure for an attacker to worry about, think again. Today's intruders are happy for any victim. **BY JOE CASAD**

Are your doors locked? Is you data safe? In the beginning, the first network intruders were just playing around. They slipped in just to prove they could – as an intellectual challenge or maybe a chance to feel brave.

Times have changed, though, and if you care about security, you'd better change with them. Today's systems hold critical information with a cash value – credit card numbers, medical records, email addresses. And the system itself can become a tool of the intruder. Cyber-criminals employ sophisticated techniques to commandeer perfectly ordinary computers for forwarding spam and launching denial of service attacks. And the teenage vandals? They are still out there also. To stay ahead of them all, you'll need to know what they know – and you'll need to know how to look for their tracks. We'll show you what to look for in this month's Detecting Intruders cover story.

An intruder who breaches network security always wants to create a hidden opening to get back in. These secret entrances, which are known as *backdoors*, come in many disguises. We lead off this month's issue with a look at some common backdoor techniques. We'll also show you how to look for signs of an attack using the versatile admin tool lsof. Then we'll look at iWatch – a promising tool that uses the Linux kernel's Inotify interface to monitor your directories and send warning of unauthorized access in real-time. In our final article of this month's set, we'll introduce you to BackTrack, a Linux live distro with a formidable collection of tools for simulating a network attack.

If you want to learn to think like an intruder, or even if you are just looking for some simple techniques for self defense, read on for expert advice on intrusion detection. We hope you enjoy this month's Linux Magazine cover story. ■

COVER STORY

Backdoors 22
Detecting Intruders with lsof ... 29
iWatch 34
BackTrack 36