Understanding, detecting, and preventing network attacks

INTRUSION STORIES

This month we look into the intruder's toolkit and investigate some prudent counter-measures for detecting and preventing attacks.

BY JOE CASAD

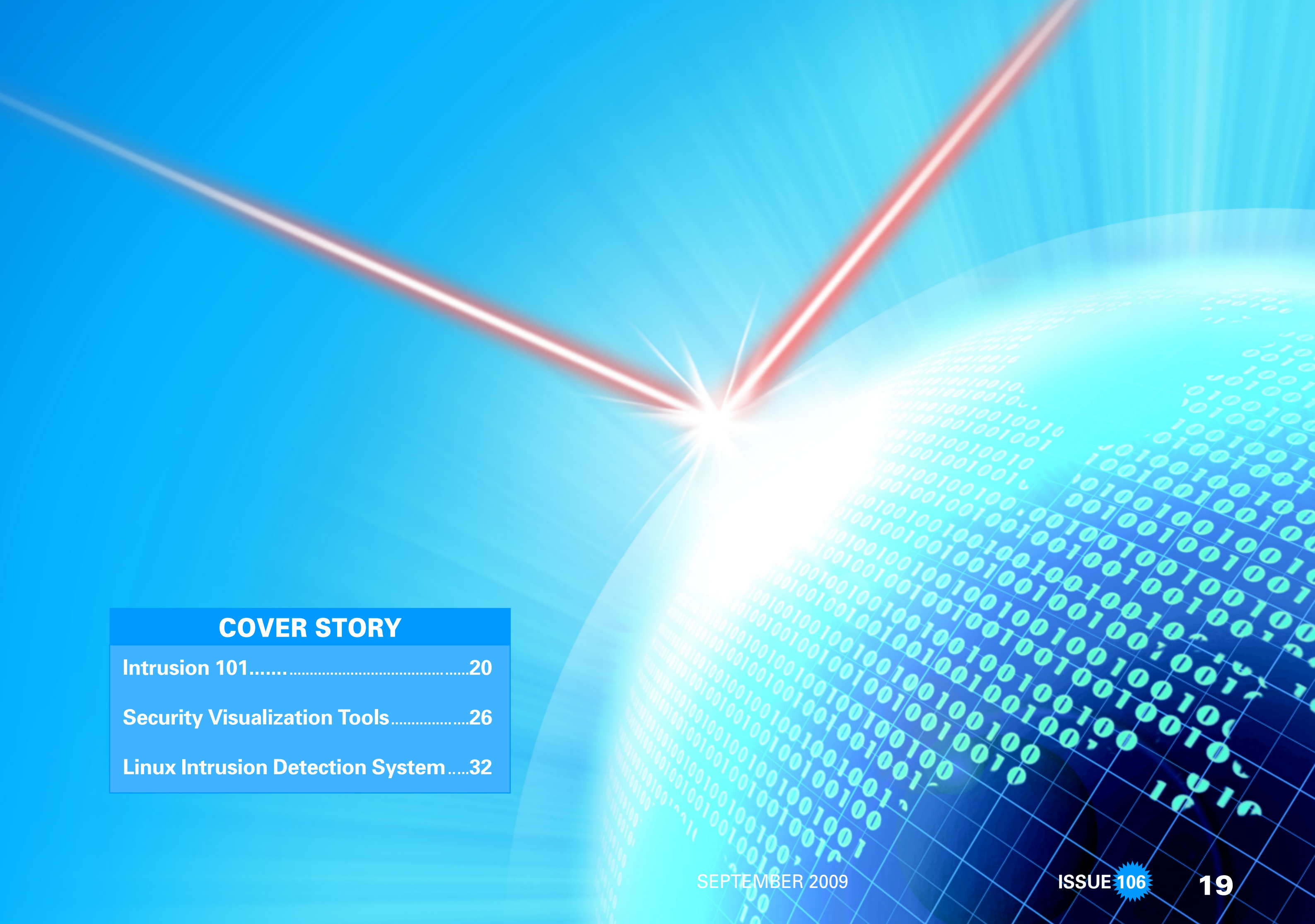
Anyone with an Internet connection has to worry about who might be connecting from the other side. Network intrusion isn't just for pranksters anymore. Spammers, credit pirates, meth addicts, and countless other n'er-do-wells are all looking for a way in. How do you keep them out? Download system updates, make use of the best available tools, and *know your enemy*.

We'll let you handle the system updates, since you probably already understand that yesterday's code is tomorrow's broken window. This month we focus on intrusion techniques and show you some tools for discovering and preventing attacks.

To start off this month's collection, security columnist Kurt Seifried takes a look at some recent intrusion strategies. You'll learn about SQL injection, cross-site request forgery, and HTTP parameter pollution. Next we offer a hands-on look at some tools for visualizing intrusion events. You'll get a chance to play through some real intrusion scenarios using PCAP (Packet Capture) files, and we'll show you how the text-based reports from the Snort intrusion detection system compare with the output of graphical visualization tools such as NetGrok, AfterGlow, Rumint, TNV, and Ethercape.

Finishing up this month's security set is a study of the Linux Intrusion Detection System (LIDS), an alternative to SELinux and AppArmor that provides mandatory access control and several other important security features.

Linux has never been more secure, but the fact is, the threats to your network have never been more profound. If you are looking for new tools and a deeper understanding of the intrusion detection game, keep reading. We're proud to bring you this month's Intrusion Prevention cover story. ■



COVER STORY