;login:
THE MAGAZINE OF USENIX & SAGE
November 2001 • Volume 26 • Number 7

Special Focus Issue: Security
Guest Editor: Rik Farrow

inside:

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

in this issue

by Rik Farrow

Rik Farrow provides UNIX and Internet security consulting and training. He is the author of *UNIX System Security* and *System Administrator's Guide to System V*.

rik@spirit.com

This has been a summer of disasters. Natural ones, like hurricanes, droughts, and tornados. National ones, most incredibly the suicide bombings. The dot-com revolution has become the dot-bomb devolution. And for security, an embarassment of automated attacks against IIS servers, making a travesty of claims for security.

While some things, like nature, fanatics, and the stock market, are not under anyone's control, other things are. Computer and network security relies most on simplicity – if a service is not run, it can't be exploited. When you read this issue of *;login:*, please keep this in mind. It should be easy, because you will find this being said more than once.

I am very excited about this issue. More people contributed articles and summaries than we could fit into our pages. For those of you who could not attend the Tenth USENIX Security Symposium this August in D.C., I recommend the summaries. Reading them is the next best thing to having been there. We had more people volunteer to write summaries than we had sessions to summarize, and I thank all who contributed their time and energy in taking notes and writing them up for us.

The articles have been divided into three groups: Forensics, Intrusion Detection, and Best Practices. Keith Jones, of Foundstone, contributed two articles based on his experience working on live systems with hacking tools installed. I appreciated reading both of these articles, but especially liked Keith's description of knark, and techniques for defending against tools like it, as well as an excellent description of how loadable kernel modules work as almost undetectable rootkits.

Brad Powell, of Sun Microsystems, writes about another aspect of forensics, detecting trojaned commands. In some ways, what Brad describes are simple tools for collecting checksums using MD5. What he barely touches on is the amount of work that went into this project, which includes a database of MD5 checksums – one for every binary that Sun has shipped. During a Sun BoF at the conference, I heard that Caspar Dik had spent many hours loading all the Sun distribution CDs into drives so that all distributions and patches could be added to the database. I would love to see all vendors provide both a database like Sun's, as well as an easy-to-use interface for checking the authenticity of files. I also want to thank Brad, and his companions at Sun, for actually completing something that many of us have wished for.

In the Intrusion Detection section, we have three articles from people who have implemented ID systems using open source software. Jon Lasser talks about using snort in an environment where, even with carefully trimmed rulesets, he was seeing tens of thousands alerts each day. Peter Van Epp writes about the uses of Argus, a tool for recording IP header information. Peter talks enthusiastically about many of the practical uses he has found for the gigabytes of Argus data that he has collected. In addition Sven Dietrich covers a different angle of IDS: survivability, which is the ability of a distributed ID system to continue running in the face of determined adversaries, even when the adversaries are insiders.

The final section borrows from the experience of three gentlemen who work in the open environments of universities and research institutes. Oscar Bonilla, of Galileo University in Guatemala, describes how necessity forced him to design a firewall that fits on a floppy disk. Remember what I wrote earlier, about not running unnecessary

services? Oscar shows you how to do this in the extreme case of a practically diskless server.

David Brumley, of Stanford University, and Abe Singer, of the San Diego Supercomputing Center, describe the best practices that have made their sites more secure and more easy to manage. David focuses on several very practical issues, with simplifying configurations high on the list. Abe describes how the San Diego Supercomputer Center has terminated the use of plaintext passwords in network services entering SDSC. Both explain their successes and failures, and extol the power of having management buy-in when it comes to getting anything done. I especially liked the psychological techniques that Abe suggests for getting troublesome researchers to migrate to new, more secure, tools and protocols.

Due to length restrictions, articles by Erin Kenneally, Paco Hope, and Ofir Arkin will appear in later issues of *;login:*. I truly wish we could have fit everything into this one issue, but we ran out of available pages.

As you read the summaries, think about the implications touched on by the special evening session about the SDMI challenge.

A group of researchers decided to investigate proposed techniques for protecting some intellectual property – in this case, music owned by corporations and distributed on CDs. The researchers were successful in reverse engineering and countering most, perhaps all, of the six techniques used to watermark music or protect the contents track. But when it came time to present their paper, they were threatened with a lawsuit, based on the Digital Millenium Copyright Act (DMCA). It was only with the support of USENIX and the Electronic Freedom Foundation that they were able to present the results of their research.

As in the case of Slylarov, who was arrested after explaining the extremely lame job Adobe had done to protect copyrighted information used in their e-Books (XOR-ing a constant against the bytestream), the DMCA seeks to prevent researchers from pointing out that the emperor has no clothes. Imagine a world where you can only report dangerous defects in automobiles to the manufacturer. This is the world that DMCA expouses, where it is illegal to discuss mechanisms used to protect copyrights. (See *http://lwn.net/2001/0726/bigpage.php3* regarding the Skylarov case).

In the wake of the attacks on the World Trade Center and the Pentagon, the same old voices are crying out for new limitations on encryption, and less restrictions on the right to search, to incarcerate, and generally, to trample on the US Bill of Rights. This trend toward a corporate state – one that focuses on corporate rights instead of citizen rights – began before the suicide bombings.

I would much rather live in a world made secure through correctly designed software and encryption without backdoors, than in a police state where it is illegal to share a thought privately, disagree with the government, or even test whether the software that is supposed to be secure is really doing anything at all. We are living in a most frightening time, and it is not only terrorists I am frightened of.