

;login:

THE MAGAZINE OF USENIX & SAGE
February 2003 • volume 28 • number 1

inside:

LETTERS TO THE EDITOR

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

letters to the editor

;login:

EDITORIAL STAFF

EDITOR:

Rob Kolstad kolstad@usenix.org

CONTRIBUTING EDITOR:

Tina Darmohray tmd@usenix.org

MANAGING EDITOR:

Alain Hénon ah@usenix.org

COPY EDITOR:

Steve Gilmartin

TYPESETTER:

Festina Lente

MEMBERSHIP, PUBLICATIONS, AND CONFERENCES

USENIX Association
2560 Ninth Street, Suite 215
Berkeley, CA 94710
Phone: 510 528 8649
FAX: 510 548 5738
Email: office@usenix.org
login@usenix.org
conference@usenix.org
WWW: <http://www.usenix.org>
<http://www.sage.org>

To Robert Haskins:

I found a mistake in your article on stopping spam [*;login*: Vol. 27, No. 4, August 2002, page 48] that can produce serious adverse affects. You state:

“A connection rate throttle will limit the number of connections per second from a given server.”

This is incorrect. It limits the *total* number of connections per second. So one connection from each of three different servers in a second will hit the limit. This means your advice of setting it to three will limit the machine to accepting a total of three connections per second. That will be a performance killer. Don't do that!

Gregory Neil Shapiro

To the Editor:

I am writing to you regarding the description of my article “Active Network Defense: Some Concepts and Techniques” in the “in this issue” section of the December 2002 (Security themed) issue of *;login*:. Unfortunately, the introduction suggests that my article “advocate[s] attacking the immediate surroundings of the attacker.” This was not my intent at all, and I did not advocate that. I was merely “exploring what the possibilities are today.”

Regards,

Sven Dietrich
spock@cert.org

Rik Farrow responds:

I agree that I misconstrued Sven Dietrich's point, that he was exploring possibilities, not actively advocating them. I got carried away. The US government, in the second draft of the document from the administration, named the National Strategy to Secure , actually goes much further than Dietrich does:

The new draft cautions that it can be difficult or even impossible to trace an attack's source. But it warns that the government's response “need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner, including through cyber warfare,” it said.

This comment appeared in an AP Wire story written by Ted Bridis on January 6, 2003 (http://news.yahoo.com/news?tmpl=story2&cid=528&ncid=528&e=3&u=/ap/20030106/ap_on_go_pr_wh/securing_cyberspace). Hopefully, the US response will be limited to “cyber warfare” attacks against any hapless ISP or university involved in an alleged attack.

rik@spirit.com