A reader wrote,

>From time to time I receive news bulletins pertaining to patches to Cisco's IOS and/or attacks. However, once a patch is implemented, how can we test it actually solved the problem? The client for whom the work gets done gives us a period of 'down time' within which to test. Since I have signed many NDAs with Cisco, is there a site / person / newsletter or anything else that actually describes the procedures that hackers use to attack the IOS and the routers.<

There are many firms, including AtomicTangerine, which can carry out penetration tests which will include verifying that patches are up to date and functioning. Just be sure that you obtain contractual confirmation that the firm does not hire criminal hackers. The last thing you need is to have untrustworthy people testing your security.

However, I think that testing individual patches is less important than the fundamental underpinnings of good information security:

* keeping security policies and architecture consistent with current needs by periodically re-evaluating the security architecture, including policy and procedure, facilities security, hiring / management / firing practices, perimeter security, and data transmission security;

* maintaining security as an integral part of corporate culture through effective awareness programs;

* monitoring current vulnerabilities by subscribing to vendor and CERT-CC bulletins;

* maintaining a sound intrusion-detection capability and rapid response to attacks and intrusions.

Sources of attack scripts include books, articles, USENET newsgroups and Web sites.

AMAZON.COM lists many books if you enter keyword "hackers"; unfortunately, some of these books are written by criminal hackers, and I hate to give them a penny. You might want to support security professionals by buying books from people who don't boast about breaking the law, but I know that the criminals do provide detailed attack scripts.

One of the most important attack/vulnerability USENET groups is BugTraq, which is described as "a full disclosure moderated mailing list for the *detailed* discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them." Its archives are at <http://www.securityfocus.com/bugtraq/archive>. Although some posters use pseudonyms, BugTraq is a serious list mostly supported by security professionals.

If you do visit criminal-hacker Web sites, may I suggest that you restrict cookie-exchange and that you bar active content (ActiveX, Java) while browsing there?
Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit <http://www.atomictangerine.com>.

Copyright © 2000 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.