In this series of articles, I’m summarizing key insights from my colleague Peter Stephenson’s work on computer forensics. In the last article, I introduced some reasons for testing one’s own security system.

Testing should begin with vulnerability assessment. Collect information about your own system such as access-control parameters, firewall settings, logging, and – much more difficult – observations of actual human behavior by system operators and other members of the production team. This phase of the work is known as assessment. Next, compare the actual configuration and performance with mandated standards and procedures and identity discrepancies. This process is known as auditing the security of the system; future columns will look at auditing in more detail. With information in hand about where security is not conforming to your own standards, you can choose which problems to correct and also the sequence for remediation that reflects your priorities and resources.

At the technical level, one of the most valuable sources of information on which vulnerabilities may be relevant to your systems is the Common Vulnerabilities and Exposures (CVE) database run by MITRE Corporation. The ICAT Metabase from the Computer Security Laboratory at the National Institute of Standards and Technology provides an excellent human interface into the CVE database; you can specify your operating system, data range, type of vulnerability and so on and instantly get a list of vulnerabilities to check in your environment. Such assessments and scans save time and money; they can allow even non-expert personnel to contribute to security assessments at low cost. The CVE / ICAT system is helpful in training security personnel and in motivating interest in the task of keeping systems strong. Assessments and vulnerability scans can also provide baseline data to help spot changes in systems after real attacks have succeeded, thus speeding up the repair process by allowing immediate attention to damaged components.

On the other hand, scanning for weakness is necessary but not sufficient for maintaining good security. Many vulnerability scanners identify problems but cannot resolve them. Worse, out-of-date assessment products may provide an incorrect evaluation of the current state of system security. Finally, some scanners can be applied externally by potential attackers, providing the enemy with valuable insights for future exploitation.

Stephenson points out that scanning for vulnerabilities and assessing procedural failures are low-cost approaches to tightening up security, but neither confronts reality directly. In contrast, red-team attacks force you to face the facts of success and failure. Active testing simulates or actually carries out system attacks. These tests can be intrusive and even dangerous. However, they provide excellent diagnosis of weakness, particularly for network perimeter tests.

In the next article in this series, I’ll look at some management aspects of active red-team security tests.

* * *
For further reading:

CVE http://cve.mitre.org/

ICAT Metabase http://icat.nist.gov/icat.cfm


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 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.