Testing security is very difficult. It's not enough to try a few known input conditions on a single installation, fix the problems that are found, and then declare the product secure. Security testing must include challenges to a full range of installations and configurations of a product to give the testers more than a superficial impression of the product's adequacy. In this article, I mention a few laboratories engaged in security testing.

* * *

_ICSA Labs_

When I worked at ICSA Labs throughout the 1990s, one of our most valuable efforts was the construction of an extensive laboratory for testing security products as part of the certification process. ICSA Labs today has a massive installation of hundreds of computers and network devices in many rooms in a small town in Pennsylvania. Staff there continue to subject security products of many kinds to rigorous testing to establish whether the products comply with ICSA Labs standards for certification. George Japak <mailto:gjapak@trusecure.com> is VP of the Technology Research Group at TruSecure and is a primary contact for further information on the work of ICSA Labs.

_NIST CSRC_

The National Institute of Standards and Technology (NIST) runs the Computer Security Resource Center (CSRC) as part of the Computer Security Division (CSD). Vendors will find a wide range of resources at the CSRC Web site. In particular, their security testing program is described as follows (bullets added): “Focus is on working with government and industry to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation and validation; and addresses such areas as:

* development and maintenance of security metrics, security evaluation criteria and evaluation methodologies, tests and test methods;

* security-specific criteria for laboratory accreditation; guidance on the use of evaluated and tested products;

* research to address assurance methods and system-wide security and assessment methodologies;

* security protocol validation activities; and

* appropriate coordination with assessment-related activities of voluntary industry standards
bodies and other assessment regimes.

The Security Testing and Metrics Group is principally responsible for this focus area.”

_DeepNines_

Another lab that has recently been announced is run by DeepNines Technologies. According to their press release in November 2002, the Sleuth9(TM) Cyber Attack Simulation Center in Dallas is focused on their Sleuth9 Security System, a real-time defensive system described in the release as follows: "... an intelligent attack mitigation and intrusion prevention solution that instantly detects and automatically prevents cyber attacks from entering or leaving a network. Sleuth9 resides inline, in front of the router and protects organizations from DoS, DDoS, Port Scans, Trojan horses, propagating worms and viruses, as well as other cyber attacks."

Sue Dark, chief executive officer at DeepNines, said that the new laboratory, "gives companies the ability to configure the security software to their specifications, create live cyber attacks with numerous variations of each attack and then analyze the results."

For more information about DeepNines’s laboratory, contact Jim O’Gara < mailto:jogara@deepnines.com >.

_Norwich University InfoWar Lab_

At Norwich University, my colleague Jason Wallace has been building an interesting cyberwar laboratory for use in data communications, information assurance and computer forensics courses. The InfoWar Laboratory consists physically of three rooms:

* Two contain rack-mounted network equipment such as routers and firewalls and have several workstations where users can engage in learning about appropriate defensive responses to various attack methods;

* The room in the middle serves as a representation of the Internet itself, including such services as DNS servers.

The Norwich lab thus allows a simulation of ordinary communications via the Internet and using the World Wide Web; however, the entire system is insulated from the real Internet so that no harm can be done from our systems to the outside. The systems are equally insulated against attack from the outside world (there is in fact no external access at all to these systems). Readers should note that our entire focus at Norwich is on defensive information assurance and information warfare; attacks are part of the curriculum only as part of this defensive orientation.

Students will be using these labs to practice for the military information warfare games that pit teams from several military academies and colleges against each other and against attacks from crack Red Teams from the National Security Agency. The whole exercise is an exciting and educational experience for all the students and faculty involved. The systems are already proving valuable for extensive computer forensics laboratory classes that are useful for computer science and criminal justice students interested in contributing to the fight against computer crime.
crime. They will also be used in the final hands-on exercises for graduating students in the MSIA (Master of Science in Information Assurance) program at Norwich.

The Norwich InfoWar Lab will also be useful for researchers in the new Norwich University Center for the Study of Counter-Terrorism and CyberCrime under the direction of colleagues COL Tom Aldrich <mailto:taldrich@norwich.edu>, who also welcomes questions from vendors interested in collaboration.

Finally, in addition to supporting students and researchers, Norwich’s lab is available under contract for use by vendors seeking a platform for security testing or interested in contributing hardware and software for our students to learn about. Interested vendors and donors can contact our VP of Technology & Strategic Partnerships, Phil Susmann <mailto:susmann@norwich.edu>

***

For further reading:


ICSA Labs <http://www.icsalabs.com/>

NIST CSRC <http://csrc.nist.gov/index.html>


***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.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.