The cadets gained a deep understanding of how to apply the firewall and how technologies and policies interact.

encountered among the leaders and managers currently responsible for our nation's critical information infrastructure.

What the cadets did not say was also encouraging. They were engrossed in the minutiae of network configuration and security for weeks. They discovered that one of the most effective tools in the arsenal was the host-based firewall, but they also understood that the key to defensive success is not the firewall per se. Rather, it is a deep understanding of how to apply the firewall and how technologies and policies interact. This thinking beyond how to use a specific package is another indicator of the value of this exercise.

Finally, even those on the Red Team—professional security auditors—had interesting impressions. Although some had been tasked to conduct penetration exercises before, the exercises typically had a limited scope and took place over extended periods. In the cyberdefense exercise, they had greater freedom in choosing an attack, and the entire attack took only one week. The compressed schedule gave them a different perspective of a network attack. According to the Red Team leader, an NSA representative, "We probably learned about as much as [the cadets] did."

And the victor is...

USMA became the first owner of the NSA Information Assurance Director's Trophy. The decision was close, but the trophy was awarded to the USMA team because of its ability to keep the required services running as well as its prevention and detection of penetrations. In reality, the contest had no losers. This may sound trite, but all participants learned so much that the exercise became a win-win competition.

DESIGNING A TRAINING EXERCISE

The cyberdefense exercise took a great deal of time and effort on the part of many organizations, but the educational benefits were off the scale. We saw impressive and steady growth in the cadets throughout the exercise, and by the end of the week, the USMA network was essentially secure from attack.

All the Red Team organizations gave generously of their personnel, equipment, and financial resources—which makes this exercise unique in some ways. Although the resources to duplicate it may be out of reach for many programs, others can still benefit from smaller exercises. We recommend basing any similar exercise on five key principles:

Make it a culminating experience. The exercise took place near the end of each cadet's undergraduate study of computer science. Because information assurance pulls together many fields from within and outside computer science, it is a natural medium through which students can draw on their entire education and apply it in a practical way.

Let the students own it. The cadets were exposed to situations they had never seen or even expected to see. They had to understand what was happening, determine how to fix it, and then actually implement the corrective action. They discovered the hard way how to plan and coordinate reactions to attacks. Their ability to do this of their own accord later in the exercise proves that they received an education beyond the normal classroom experience.

In an exercise of this magnitude, the students must have the responsibility for running and securing the network; they must also be able to control most aspects of the exercise. Giving them this kind of control is risky, but without a sense of ownership, the students will tend to quit when faced with a thorny problem. Keep instructors in a facilitating role only.

Pick a meaningful adversary. Matching wits with professional minds is a great incentive for students to perform well. It is one thing to be told why something you did was wrong. It is quite another to discover that you've been outwitted and have to clean up the resulting mess. Tremendous learning goes on when students have to scramble to determine what is happening in the network they are responsible for.

Incorporate some form of competition. Competition is an irreplaceable motivator. An exercise like this is difficult and frustrating. Students need something besides a grade to motivate them to spend a spring weekend in a hot, stuffy laboratory. CDX involved two kinds of competition. In addition to the obvious competition between the service academies for the best defense, there was also an adversarial competition between the Red Team and the cadets. This competition played on the well-established athletic rivalry between the service academies, but lower-key competition can still be effective. Even an exercise between two teams from the same school can be a sufficient motivator.

Have a network sandbox. The exercise must place restrictions on what students can and cannot do, and these restrictions must be enforced. Otherwise, collateral damage to a live network or the Internet will cause real problems for everyone. Having a network sandbox—an isolated area where the