

## **Fact Sheet: NSA/CSS Cyber Defense Exercise – After Exercise**

### **New Strategy of Mitigating vs. Avoiding Vulnerabilities**

The 2010 CDX theme, “Survival Strategies in a Hostile Network Environment,” emphasized a strategy of mitigating vulnerabilities rather than trying to simply avoid them. The rules were deliberately designed so even the best Blue Cell teams would have difficulty keeping the Red Cell out entirely. With careful thought to their network designs and incident response strategy, the teams should have had success in containing the Red Cell and preventing the compromise of critical systems.

The Blue Cell teams designed and built operational networks constrained by a set of “notional budget” rules – the students did not have the resources to take every security measure they might wish. Networks had to include a variety of services: Domain Name Service (DNS), Windows Active Directory, email, web, Instant Messaging or “chat,” file shares, network printers, and (new for 2010) Voice-over-IP telephones.

CDX 2010 staff was dominated by the Red Cell, the “opposition force” of hackers who challenged the student teams. The Red Cell was composed of about 40 individuals from the following organizations:

- NSA
- Army Reserve Information Operations Command (ARIOC)
- Navy Reserves Navy Information Operations Command (NIOC), Ft Meade
- Canadian Forces Information Operations Group (CFIOG)
- Canada’s Communications Security Establishment (CSE)
- AFIT
- NPS

NSA technical experts and experienced NSA Red Team operators led the Red Cell. The Red Cell posed a strong – but fair and impartial – challenge to the participating students. As Red Cell personnel compromised Blue Cell systems, they reported their results to the exercise referees, the “White Cell.”

The White Cell was composed of 20 personnel; about half located at CDX HQ, the other half posted to the participating schools as on-site referees. As with the Red Cell, the White Cell was led by NSA technical experts, but also included personnel from ARIOC, NIOC, and CSE. The White Cell adjudicated the competition, enforced the rules and levied penalties when the Blue Cell teams suffered service outages or compromises of network integrity.

### **New Gray Cell Plays Role as “System Users”**

One innovation in this year’s exercise was the so-called “Gray Cell,” composed of about 12 personnel, with most deployed at the participating schools. Gray Cell personnel

played the role of users on the Blue Cell networks. During the exercise they sent and received email, created and edited documents, browsed the web, used Instant Messaging systems - all the things that real users do. Gray Cell personnel served several purposes:

- generated innocuous traffic on the exercise network, preventing the students from assuming that any traffic they see must be from the Red Cell and therefore hostile;
- emulated untrained users on the network, who make mistakes that compromise network security and facilitate hostile attack; and
- drove the dynamic scenario, the fictionalized events that occur in the course of the exercise and give the students a sense of context for their activities.

### **New Exercise Injects Designed to Complicate Network Defense**

Aside from the daily routine of defending their networks, the students responded to exercise injects. These simulated the tasks that real-world network managers often have to undertake while still maintaining the integrity of their systems. Exercise injects for CDX 2010 included:

- The sudden arrival of additional workstations that needed quick integration into the operational network. Some of these workstations may have been infested with malware or other security vulnerabilities.
- The appearance of an apparently hostile “web crawler” system on the simulated Internet, which could not be blocked but must somehow be dealt with.
- A requirement to perform forensics analysis on a suspicious computer system, supported by notional “intelligence” information disseminated by Gray Cell in the course of the exercise.

### **New “Hack-Back” Event**

The last exercise inject took place at the end of CDX, on Friday afternoon. NSA set up an extra target network at CDX HQ to serve as a “test range” for Red Cell, permitting Red Cell to test attack techniques without tipping its hand to the Blue Cell teams. At the end of CDX 2010, all of the Blue Cell teams were invited to attack this test range in a “capture-the-flag” event lasting several hours. Students attempted to recover marker files representing actionable intelligence. For CDX 2010 this “hack-back” event did not count toward the exercise scoring, but several teams took the opportunity to attack the “target range.” This type of Computer Network Attack (CNA) or Computer Network Defense Response Action (CND-RA) event may be integrated into future CDX’s.