

What the CDX Challenge is:

The Cyber Defense Exercise (CDX) is a four day Information Assurance exercise run by the National Security Agency/Central Security Service (NSA/CSS) to help train federal service academy students in secure network operations. This paper is a collaborative work on the various tools and techniques used and the overall effectiveness of live-attack exercises in teaching information security.

CDX is a computer security competition that was designed to foster education and awareness among future military leaders about the role of Information Assurance (IA) in protecting the nation's critical information systems. Schools were assessed on their ability to maintain network services while detecting and responding to network security intrusions and compromises.

The beginning of CDX:

Designed to fill the CAPSTONE requirement for the United States Military Academy's Information Assurance course in 2001, the Cyber Defense Exercise (CDX) pits teams of cadets from each of the five US service academies against security experts within the Department of Defense. Each team is challenged to design, implement, and manage an operational network of computers. Management of various platforms (Windows, LINUX, Solaris, FreeBSD, etc.) is required and services such as web, email, public key infrastructure, and database sharing must be provided. Students are encouraged to establish architecture, policy, and procedures that invoke a defense-in-depth and defense-in-breadth posture to keep the aggressors at bay. To keep the playing field level, security measures are limited to open source freely available tools. Strategies and techniques employed by the students that were tested on the CDX battlefield have provided industry, academia, and government with valuable lessons. These lessons are related to work in network mapping, port scanning, vulnerability scanning, password integrity checking, network monitoring tools, intrusion detection systems, host-based and network-based firewalls, and layer-two bridges.

As the competition begins, the National Security Agency (NSA) - led Red Force identifies vulnerabilities and launches repeated attacks on each network over a four-day period. Students have the ability to enter into direct cyber combat in an effort to keep services on-line and running. Teams are then evaluated on maintaining services as well as efforts to recover from and prevent future security breaches. The winner is presented the NSA Information



Assurance Director's Trophy.

The CDX has resulted in an intense rivalry between the academies and has become a staple of each academy's information assurance curriculum. The DoD's investment in this project has already reaped extraordinary benefits and the sky is the limit. The CDX should serve as a model for inter-agency programs as there are several players

involved each year whose vision and dedication make this effort a success. In just three years the number of personnel involved in carrying-out and participating in the exercise has grown from approximately 40 to over 300.

<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01245660>

Architecture of a Cyber Defense Competition^{*}

Wayne J. Schepens and John R. James¹

Electrical Engineering and Computer Science Department
United States Military Academy
West Point, NY 10996, U.S.A.