Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

# Cyber Defense Exercise:
## Meeting Learning Objectives thru Competition

Thomas Augustine, *US Naval Academy*, and Ronald C. Dodge JR, *US Military Academy*

***The sixth annual US Service Academies Cyber Defense Exercise proved to be an opportunity to meet pre-planned learning objectives. Rather than focusing on the competition, the planning team designed the exercise to meet objectives which balanced: creativity versus realism, security versus network operations and timely incident reporting. Additional benefits included teaming and leadership opportunities as well as providing an outstanding recruiting tool for Computer Science and Information Technology majors.***

**Index terms – Cyber Defense Exercise, Learning Objectives, Military Academies, National Security Agency, competition**

### I. Introduction

The National Security Agency teamed with the Five US Service Academies and the Air Force Institute of Technology for the sixth annual Cyber Defense Exercise (CDX). This exercise provides an excellent hands-on opportunity for students to practice what they have learned as a Capstone project. In order to maximize the goals of this exercise, faculty and staff members planned well in advance defining both learning objectives and ancillary benefits associated with the exercise. Rather than simply defining enough factors to determine a clear winner to the competition, the exercise planners balanced reality with pre-defined learning objectives to provide an outstanding learning experience. The Cyber Defense Exercise has been written about many times before, focusing on the logistical and experiential facets of the exercise. This paper, however, is the first effort toward documenting the framework used to identify and meet educational goals. The exercise is relevant to Academia in that it illustrates educational goals which extend the Information Assurance curricula, defines means to implement these goals and allows for a measure of success. Government and industry can also benefit using this exercise as a template for hands-on training of system administrators and Information Assurance professionals.

*Major Thomas Augustine, D.CS. is an Assistant Professor in the Computer Science Department at the US Naval Academy, Annapolis MD, thomas.augustine@acm.org*

*Lieutenant Colonel Ronald Dodge Ph.D. is Director, Information Technology & Operations Center, Department of Electrical Engineering and Computer Science, United States Military Academy at West Point, ronald.dodge@usma.edu*

### II. Cyber Defense Exercise

The CDX started as a capstone project for senior Computer Science majors culminating in a competition between the U.S. Military Academy and the Air Force Academy but quickly grew to its current size [1]. Now, this exercise provides a competition between the U.S. Air Force Academy, U.S. Coast Guard Academy, U.S. Merchant Marine Academy, U.S. Military Academy and the U.S. Naval Academy. While this competition pits the undergraduate Academies against each other in operating and securing a network, the graduate Air Force Institute of Technology and Naval Post Graduate Schools are invited to advance the state of technology inherent in the competition yet do not compete for the highly coveted NSA's Information Assurance Directors trophy. This annual exercise provides a means for students to practice what they have learned throughout their information assurance curriculums.

The exercise consists of many participants to include: the students who operate and secure networks at each school; the faculty that teaches the students; the White Cell acting as the exercise controllers and score keepers; and of course the infamous Red Cell acting as the aggressors or network "hackers". Because the exercise started as a capstone project for seniors, all student competitors were in their senior-year and had formal information assurance training. While the seniors continue to lead their team schools, many schools now invite any Computer Science or Information Systems major to compete. The faculty members at each school are an integral part of the CDX planning team. These faculty members are encouraged to teach the information assurance concepts, but required to minimize their support during the exercise. Also part of the planning team, the NSA provides both White Cell and Red Cell members consisting of volunteer network professionals. In order to provide an opportunity for teaming, members of other Department of Defense network security organizations are invited to act as members of the Red and White Cells.

Students receive an exercise directive, providing the ground-rules for the exercise and scoring for the competition. The directive always starts with a scenario which gives the students an opportunity to see how their decisions could affect real-world operations and security. All learning objectives are then weaved into this scenario, providing a realistic reinforcement of information assurance concepts [2].

## III. Learning Objectives

Over the past couple of years, numerous cyber defense competitions have surfaced [3]. Some of these competitions are designed to complement academic experiences while others are designed purely as competitive events. While the students are motivated by the competitive spirit of the CDX, the exercise has been and will continue to be focused on enhancing learning experiences.

In planning the exercise events, many compromises were made. The planning team decided that ultimately if students come out of this exercise with a better appreciation for how their decisions impact the operations and security of the network, then the exercise would be deemed a success. Clearly, the students see this exercise as a competition, as there can be only one winner of the prestigious NSA Information Assurance Directors trophy.

The primary focus of this exercise is student learning through well defined learning objectives. Kolb's Experiential Learning Theory [4] points to four learning styles based on a four-stage learning cycle. This theory recognizes that students learn differently and in order to most effectively retain information must be afforded different teaching methods. These methods include: a concrete experience; observation and reflection; forming abstract concepts; and testing in new situations. Though the CDX is designed to compliment a strong Information Assurance curriculum, this exercise provides an opportunity for students to learn under all four methods, strengthening the overall learning experience. Before and during the exercise, students are encouraged to team together to plan, execute and report Information Assurance concepts as taught in throughout their formal curriculum.

The planning team agreed on five primary goals for the CDX. These objectives included practicing task prioritization while allowing students to creatively practice what they have learned to date about security. The team also defined the need for students to balance the requirement for both network operations and security based on constraints they are likely to see in their future information assurance leadership positions. Other objectives included practicing Department of Defense incident reporting and handling procedures also key to their future leadership opportunities. To develop the components of the exercise we developed three primary areas of consideration to evaluate: design, operate, and manage. Figure 1 shows some tasks identified that we integrated into the exercise.

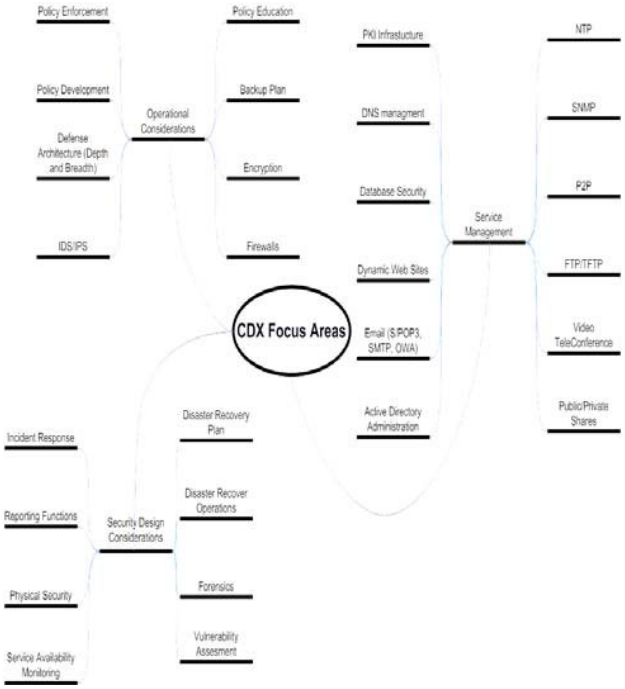


**Figure 1 CDX design considerations**

### *A. Task Prioritization*

Security professionals will generally rate task prioritization as one of the key areas to successful network security. Curriculums can teach a potential priority scheme but in order to instill a true understanding of the challenges associated with endless tasks and limited resources, students must be given the opportunity to practice in exercises like the CDX.

Task prioritization starts immediately upon forming a team and ends only at the close of the exercise. Students must operate and secure multiple network services with limited resources while defending against network attacks and continually reporting accurate status. These requirements provide fertile ground for trial and error. While certainly stressful, each student learns to balance the concurrent requirements of Information Assurance, network operations and limited resources.

*B. Creativity versus Realism*

In defining a competition or an exercise that centers around providing each student with a hands-on demonstration of security practices, the planning team must first ask whether they should reward student creativity which implies a more complete understanding of security practices or whether the ground rules should focus on what the students are likely to see in a year or two after they graduate. This was perhaps the most controversial discussion item among the exercise planners.

Rarely is a system administrator or network security professional able to simply define the perfectly secure network and implement it from scratch. They will have to deal with existing infrastructure and applications; limited budgets; a requirement to balance operational network availability against security concerns; and the reality that users can be the largest obstacle to good security.

Though the planning team wanted to ensure a varied network to add complexity and realism to the student experience, it had to determine how much of the network was to be pre-configured and how much was to be left to the student. While the goal called for securing a varied network, the school faculty noted that they wanted to maximize the security research requirements while minimizing the need for non-security related system administration tasks.

The exercise planning team chose to balance these concerns through the exercise directive which provides the rules by which the exercise and competition was to be administered. The directive dictated the minimum network services that each school was to provide throughout the exercise and the associated operating systems of some of these services. This included a Microsoft 2003 domain controller, a Fedora Core 2 file share server and web server, a Microsoft Exchange server and Microsoft XP clients. Student firewalls were purposely not called out to provide some student latitude. These directives ensured a varied set of platforms and operating systems, however provided leeway on the overall student network architecture by allowing additional servers, hardware or software as required to meet the stated objectives. This helped to simulate a complex network requiring student research from more than a single source, however did not handicap the students creativity in designing a network that can win the competition.

*C. Operations versus Security*

In determining how realistically the exercise was to model the real-world, the exercise planners had to consider whether this was primarily an exercise focusing on security concerns or whether students would also be graded on their ability to manage network operational availability. The planning team decided on a compromise to focus on security for brief outages but penalize students for extended network outages due either to their security decisions or poor network architecture. While there were White Cell exercise controllers located at each school verifying the students actions, it was important to ensure that rules prevented students from gaming the competition simply by unplugging a component that was under preventable attack. This is consistent with real world operations where clients can generally understand small lapses in network service availability to provide better network security but will rarely except extended downtimes. In implementing this concept, the White Cell assessed penalties for each service and for each block of downtime between one and fifteen minutes. After ninety minutes of downtime, competitors were then directed to reconfigure their network using a configuration that was "operational, but non-secure" with help from the White Cell if necessary. Given the high penalties assessed for non-root compromises and the much higher penalties assessed for root-level compromises, this motivated students to keep their networks operational even during potential periods of network attack.

As an extension of the security versus availability discussion, the planning team understood that not every school could provide enough qualified students to administer the network twenty-four hours per day throughout a four-day exercise where many students still have classes and other responsibilities. The planning team took this into consideration by defining a daily schedule of eight core hours where the Red Cell aggressors were active, an additional two hours of planned maintenance down-time and a requirement for all network services to be active throughout the rest of the twenty-four hour period. All network services were validated on a frequent but random basis by using Nagios, an open source host, service and network monitoring program. While a partial solution, manual scoring of services was also required, so future exercises will include custom-made scripts to validate service operations.

Though this exercise is primarily intended to give a hands-on, technical experience to students, we recognize that it can also be used to further demonstrate the importance of non-technical plans and policies. Prior to the exercise students were therefore asked to submit complete network diagrams and contingency plans for the continued operation of the network in an event of a catastrophe. Students were then only allowed to use the hardware and software listed in their network diagrams, forcing them to design back-up servers and plan for the use of software or hardware security solutions. This prior

planning proves to be difficult for some students, yet a strong indicator of whether they fully understand the defense-in-depth security and contingency concepts. Non-technical exercise injects discussed included a loss of primary power, equipment, or personnel, forcing students to either prioritize resources, relocate, restore back-ups or ensure that no one person becomes a single point of failure.

### *D. Accurate and Timely Reporting*

One crucial facet of Department of Defense network security is identifying and reporting potential security breaches. Because of the nature of information sharing requirements among DoD agencies, a vulnerability for one network may provide the weak link necessary to damage other connected networks. As such, the Department of Defense has a well defined process for reporting security incidents in an attempt to control the spread of malware or negative network activity. The CDX models this process, encouraging students to accurately identify and report network status and incidents. Students were required to report the status and security of their network hourly, and provide a consolidated situational report every evening. Students were not allowed to simply provide on-time reporting. Instead, their scoring was based on the accuracy of their reports as compared to the actual logged events of the Red Cell. This requirement actually had the dual purpose. In addition to teaching students a reporting process similar to the one they will see when they graduate, students must hone their skills to identify and characterize possible attacks. While students can be taught the need for accurate reporting, this exercise provides a hands-on, integrated approach to prioritizing operations, security and reporting.

### *E. Ethical Computing*

While the operations and security of the network are key objectives of the CDX, we hope to teach our students more than simply the mechanics of good system administration. In addition, we hope to instill an ethical base, so that they understand the difference between offensive and defensive network surety issues. Many of the defensive skills taught could, with further open source research be turned into offensive actions. The purpose of this exercise is not to teach “hacking” nor teach the students how to use the exploits readily found on the web. Instead, students are taught strong defensive information assurance techniques designed to secure a network against malware or attack. Information Assurance practitioners agree that simply having students sign an ethical computing statement may ensure that students follow the letter of the policy, but does not instill the desired ethical behavior [5]. It would be easy to declare that the students at the US Military Academies can be trusted and that simply asking them to "be ethical" should be good enough. We would argue that the reason these military officers go on to make ethical decisions is that ethics are not just a statement but are incorporated into every course and all training throughout their entire experience. In teaching strong defensive measures students must understand how the network aggressor or attacker will strike and what types of information or systems are at highest risk. To that end, the competitors of the CDX are directed to secure their networks against attack but are strictly forbidden from any aggressive action against another team, the white cell exercise controllers or the red cell network aggressors. This ethical computing concept is then reinforced throughout all Computer Science and Information Assurance coursework in all of the School’s programs. In defining similar Information Assurance exercises or competitions, we recommend that ethical computing be a focus area. Those individuals who act as Red Cell aggressors should be trusted network professionals or senior students, perhaps at the Graduate level, who have demonstrated that they understand and follow ethical computing standards.

## III. EXERCISE INJECTS

In balancing student creativity and realism and in determining a scoring system that provides a definite winner, the planning team chose to add three additional injects to the exercise including a: vulnerability analysis, a forensics exercise and working with a compromised firewall password.

In past exercises, students were given systems builds for each of the required services that they had the choice to use or were allowed to create their own. As noted above, the exercise planning team believed that while students should be encouraged to be creative in their operations and security architectures, some realism was required.

### *A. Malware Implants*

Networks connected to the internet can over time accumulate a large amount of malware, be it viruses, Trojan Horses, spyware or malicious hidden files. Systems also contain unnecessary vulnerable applications and unneeded user accounts as well. In real-world operations, network aggressors or hackers use exploits to enter a system and many have the ability to implant Trojan Horses or hidden files in attempt to gain further access or system information. The planning team realized that in a four day exercise, on a closed-system not open to the internet, malware was not likely to be inherently present. In order to add a factor of realism, the planning team agreed to implant network exploits readily found in the open-source internet. Prior to software delivery, the

Red Cell implanted at least one exploit onto each system to be delivered to the students, mirroring exploits for each school to ensure a fair competition.

These implants served two purposes. First, students could reasonably be expected to find and disable the implants based on vulnerability analysis techniques taught in the classroom. These implants also served a second purpose. Exploits that were not identified by the students prior to the exercise were fair game for use by the Red Cell during the exercise and therefore stratified competitors. Prior to the start of the exercise, students were given the system builds for mandatory use under the directive as pre-configured legacy systems. They were then only told to complete a vulnerability analysis on the domain controller and exchange server with the assumption that students would perform a similar analysis of all provided software. Those schools that completed a strong vulnerability analysis on all provided components had an advantage in deterring Red Cell aggression.

### *B. Forensics Scenario*

In order to keep student interest peaked and provide a diversion through a rather stressful competition, the planning team inserted a forensics scenario mid-way into the exercise. Students were presented with a virtual machine and were told that this machine had been used to commit a crime. Like the popular crime shows, students had to gather computer forensics facts while maintaining positive control of the evidence. The planning team chose not to make this exercise penalty-based but did provide an opportunity for students to improve their overall scores. Students were encouraged to use Sleuth Kit and Autopsy which are a collection of open source Unix-based command-line tools that help detect hidden files and deleted data. White Cell members were permitted to provide hints for a more complete analysis. Students rated this event among their favorite throughout the four days of competition. In addition to providing a fun diversion for students, it provided yet another opportunity to learn and practice security prioritization. If students chose to spend all of their time on this exercise without recapping the day's network security incidents, they endangered their primary graded task of securing their network.

### *C. Compromised Firewall Password*

The CDX focused on injecting realism and forcing students to make rational network security decisions despite emergency conditions. Many administrators assume that by fortifying their perimeter with strong firewall rule sets, they are immune to attack yet we hear stories of many networks that have been compromised using well published exploits. Service Academy Information Assurance curriculums teach network security as a defense-in-depth approach which dispels the myth that a strong perimeter guarantees network security. In order to instill the need for a defense-in-depth approach and allow students to understand the impacts of their security decisions, the White Cell injected a scenario where the firewall password of each student network was compromised. This provided the Red Cell an opportunity to verify the security of each inner-network. Those that had used a defense-in-depth approach were less likely to sustain network damage, while those who did not plan for an internal network penetration were more likely to have a compromised root-password of other systems.

### *D. Peer-to-Peer Identification*

Almost every university student has used peer to peer applications be it chat programs or music distribution systems. While there are certainly legitimate business uses for peer-to-peer applications, they do present a significant security risk which must be factored into the overall network security posture. In meeting goals to make this exercise more realistic, the planning team chose to add peer-to-peer application identification to the exercise agenda. The inject introduced BitTorrent traffic on the network. Students were then allowed to deal with the traffic as they saw fit. Scoring was based on the discovery of peer-to-peer traffic and identification of application protocol, but students were encouraged to provide a mitigation strategy. Based on network policies, some types of peer-to-peer should be blocked while others require security hardening of attached network components and clients.

### *E. Loss of Primary Web Server*

To model a real world outage, students were told that a power outage caused their primary web server to fail and were required to physically remove their primary web server from the network. Those that planned ahead had a mirrored web site or back-up equipment ready for implementation. Scoring of required services continued, motivating students to restore the service. In order to add realism and require students to prioritize actions, this exercise inject was presented at the same time where Red Cell scanning activity was heavy and during a required reporting period. Experienced network professionals will agree that this scenario is quite realistic and occurs on a regular basis.

## IV. Additional Benefits

While there certainly must be a focus on the student, exercise planners understood early in the planning phases, that this exercise could provide additional benefits. Among these benefits, teaming with similar organizations

was high on the list. The CDX provides an excellent opportunity for the US Service Academies to compare information assurance programs while providing a common baseline in education required to compete favorably in the exercise. Faculty members from each Service Academy were integral in the planning of the exercise allowing each an opportunity to share highlights of their information assurance curriculum and incorporate this into the capstone exercise. The students and faculty of the Service Academies were not the only ones who benefited from this teaming. The NSA teamed with members of the Air Force, Army, Navy, Marine Corps and Army Reserve information operations organizations in planning the White and Red Cell. Again, this provided an excellent opportunity for cross-flow of ideas, tools and techniques.

Though this exercise is clearly focused on information assurance principles, it has proven to provide a strong leadership experience for all students involved [6]. Throughout the course of the entire exercise, students are provided little guidance by faculty members. Students must choose their leaders and then follow thru on assembling and training their teams. Students must schedule their staff, balancing the need for expertise and expected red cell activity with the realities that many students have classes, exams and other school obligations. During the exercise, students are required not only to defend their network, but continually report operational status and log attack attempts. These concurrent events rival some of the most stressful situations that experienced network professionals must face, and therefore provide an outstanding opportunity for students to practice their leadership skills.

Perhaps the most useful and yet unexpected benefit of the CDX was its student allure. While there are no shortages of bright, motivated, science-oriented students at the US Service Academies, the Computer Science and Information Systems Departments at these schools must keep the students interest in order to compete favorably with other majors. We found that at a number of the schools, students were motivated to learn more Computer Science or Information Systems principles as a direct result of the excitement generated from the CDX. Once in the major, students then pay great attention to all information assurance education in hopes of learning enough to win future competitions.

## V. Survey Results

Though the planners of the CDX certainly have notional success stories through their involvement over the past few years, we chose to survey students and faculty to provide a better depiction of their CDX perceptions. Immediately following the CDX seventy-four students and thirteen faculty answered anonymous surveys. These surveys were not intended to provide a rigorous statistical analysis but do lend credence to the argument that the CDX is beneficial to the participating students.

We asked students to categorize the percent of information assurance learned. On average, students claimed that 45% of their overall information assurance learning came from participation in the CDX. It is important to understand that two of the six schools do not have official majors in computer science, and therefore the perception that little information assurance knowledge comes from classroom education is explained. Even in those schools with very strong curriculums, students claim 40% of their subject learning from participation in CDX. Nearly tied for second place, reading on their own and classroom learning was rated at about 20% each, and students rated practicing on their own at about 15% of overall subject learning. Faculty perception of student learning percentages was similar also placing the CDX at almost 40% of learning with a variation from student perception listing the curriculum at almost 30% of overall learning. These results imply that both students and faculty answering this survey believe that the CDX is integral to student information assurance learning.

Additionally, students were asked to list three items that were taught as part of their curriculum but were enhanced with CDX. A majority of students noted: network layers and protocols, encryption methods, secure architecture design, use of firewalls, traffic monitoring and analysis and the need for security-in-depth. When asked to list three items that had either not been previously taught or learned, students answered with a number of items key to implementation of good security. These included: specific firewall rulesets, rootkits, analysis of logging, patching and updates use of Linux and Microsoft Exchange, use and analysis of honeypots, the need for clean backups and software forensics. Students from the Air Force Institute of Technology almost unanimously listed IPSEC as they used this form of encryption in their network design.

Faculty were asked to describe the impact that CDX has on student training as well as how the CDX compliments curriculum information assurance programs. Though possibly somewhat biased toward CDX success, all thirteen faculty members answering the surveys noted that the CDX provides one of the most focused forums for hands-on experience provided throughout the school-year. More than half of the faculty noted that the CDX is an integral part of their curriculum planning including timing of concept teaching. Other faculty noted that with only a single networking class in the curriculum, the exercise is invaluable in adding an opportunity for guided self-learning of Information Assurance principles.

When asked how CDX has been used as a recruiting tool for computer science or information technology majors, faculty from four of the six schools noted that some students choose these majors strictly based on their projected participation in the exercise. All faculty noted that the CDX definitely motivates students to pay attention and learn while in class as well as encouraging students to either read on their own or take on information assurance related electives or senior projects.

## VI. Summary

The annual CDX provides an opportunity to reinforce student learning of strong information assurance principles. This exercise maximizes its effectiveness through strong prior-planning by faculty, exercise controllers and exercise Red Cell members. Though the backdrop of the competition provides additional student motivation, planners base all inputs on well defined learning objectives. Experience over the past six years shows us that with proper planning an exercise of this nature can meet numerous objectives for hands-on learning while providing enough differences among the teams to define a clear competition winner.

## VII. References

[1] W.J. Schepens and J.R. James, "Architecture of a Cyber Defense Competition", in IEEE International Conference on Systems, Man and Cybernetics, vol. 5, 2003, pp. 4300-4305.

[2] R.C. Dodge, Jr., D.J. Ragsdale, "Organized Cyber Defense Competitions", in Proceedings of IEEE International Conference on Advanced Learning Technologies, 2004, pp.768-770

[3] L.J. Hoffman, T. Rosenberg, Dodge, R., and Ragsdale D., "Exploring a National Cybersecurity Exercise for Universities", IEEE Security & Privacy Magazine, 2005, vol. 3, issue 5, pp.27-33.

[4] D..A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*. Prentice-Hall, Inc., Englewood Cliffs, N.J. 1984.

[5] J. Harris, "Maintaining Ethical Standards for a Computer Security Curriculum" in InfoSecCD Conference '04, Kennesaw, GA, pp. 46-48.

[6] R.C. Dodge, Jr., D.J. Ragsdale, and C. Reynolds, "Organization and Training of a Cybersecurity Team", in IEEE Conference on Systems, Man and Cybernetics 2003, vol. 5, pp. 4311-4316.