Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives

William J. Adams
United States Military Academy
Tim Lacey
Air Force Institute of Technology
Efstratios Gavas
United States Merchant Marine Academy
Sylvain P. Leblanc
Royal Military College of Canada

Abstract

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.

1 Introduction

This paper illustrates how the National Security Agency/Central Security Service (NSA/CSS) annual *Cyber Defense Exercise (CDX)* affects curricula and teaching used at federal service academies. We present the academies' views on the effectiveness of hands-on, live-attack exercises. We also argue that these types of exercises should be part of any computer security curriculum to strengthen and enhance classroom learning.

We provide observational data in support of live-attack exercises as an effective technique for teaching well-founded security and administration skills. Our experiences show a substantial connection between understanding and hands-on activities. Additionally, we will discuss how these activities are scalable from simple tasks geared toward an individual, to complex tasks which can challenge a large team of students. These activities can also be scaled in terms of instructor workload from self-guided tasks on a single laptop to tasks requiring setup by multiple instructors with complex infrastructure.

Each academy defines success differently, with learning goals covering topics including: network design, system administration, cost benefit analysis, forensics, and leadership. The competition provides a structure to objectively evaluate the effectiveness of these learning goals as a function of the operational performance and security of a live network. By design, the CDX is also a collaborative environment which makes it easy to share lessons learned and develop best practices across academies.

During CDX 2009, the number of significant, distinct compromises decreased compared to previous years. This suggests the defensive tactics being used have become more effective. In particular, the largest category during CDX 2008 (callbacks from pre-positioned malware) was much smaller during this years competition, indicating some academy teams are developing effective tactics against this attack vector.

2 Overview

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.

CDX 2009 was the ninth year this annual information security event occurred where teams of students from various military institutions (Blue Teams) designed, built, and defended computer networks against simulated intrusions by the NSA/CSS Red Team. The NSA also sent a White Team representative to each participating school to act as a liaison between the school and the exercise headquarters.

The following teams participated in this year's CDX:

- United States Military Academy (USMA)
- United States Naval Academy (USNA)
- United States Air Force Academy (USAFA)
- United States Coast Guard Academy (USCGA)
- United States Merchant Marine Academy (USMMA)
- Air Force Institute of Technology (AFIT)
- Naval Postgraduate School (NPS)
- Royal Military College of Canada (RMC)

Each team was given control of enterprise systems similar to what they may find in a poorly managed network. Their first task was to identify vulnerabilities in these potentially exploited machines and mitigate the problems. The various tasks needed to secure the network were assigned notional costs to reflect real-world labor, licensing, and hardware expenses. The teams then had to redesign, or reconfigure, the network and services

to be more secure and reliable while staying within a notional budget.

Students were graded on their ability to maintain the enterprise systems including: email, instant messaging, database and web servers, workstations, and a domain controller. They also had to submit timely and accurate incident reports as they detected Red Team activity and respond to service requests, called *injects*.

CDX challenges teams of students from each academy to design, build, and successfully defend a real-world computer network against simulated intrusions by a team of NSA and Department of Defense (DoD) personnel over a four-day period.

CDX gives students a sense of the risks that exist in a hostile network environment. It teaches network defense strategies that can mitigate those risks while considering financial and labor resource trade-offs.

A team of NSA and DoD personnel act as evaluators during the exercise, and the NSA/CSS IA Director awards a trophy to the team that most effectively maintains network services while deterring and recovering from network intrusions. The NSA Red Team challenges teams using only publicly available, well-documented exploits on a closed network that is separate from the Internet.

New elements this year included a *help desk* structure in which students must research and respond to daily computer questions emphasizing school learning objectives. Undergraduate schools were authorized to consult graduate schools for assistance and mentoring with these *help desk* requests as well as any other issues that came up during CDX.

Similar to last year's event, students completed exercise *injects* which included a packet capture analysis and system forensics analysis. Additionally, CDX 2009 included a requirement for each school to demonstrate its competence with the principals behind IPv6 and Domain Name Systems (DNS), by establishing an IPv6 tunnel and performing a DNS zone transfer.

This year also marked the first year that a foreign school, RMC, participated in the CDX. Their participation has paved the way for other strategic foreign partners to participate, and has built a stronger international community of collaboration and sharing.

3 Academies' Experiences

3.1 United States Military Academy

USMA's participation in the CDX starts in a research center dedicated to IA. The *Information Technology and Operations Center (ITOC)* performs internationally recognized security research. Members of the ITOC help embed security lessons in all of the computer science and information technology courses at the USMA. They are also responsible for the student chapter of the *Association for Computing Machinery (ACM)* and course-directing portions of the IA course sequence.

The student ACM chapter has monthly events including a *Capture the Flag* exercise every semester, trips to the NSA, and attendance at conferences such as *Shmoocon* and *Defcon*. Other events have included guest speakers such as Johnny Long, Ed Skoudis, and Peiter "*Mudge*" Zatko.

In addition to extracurricular activities, the IA course sequence is open to computer science, information technology, and electrical engineering students. The sequence covers topics such as networking, operating systems, and distributed applications. The courses in this sequence are all prerequisites to a senior-level computer science capstone elective entitled *Information Assurance*, directed by Colonel William J. Adams, Ph.D. This class forms the basis for USMA's participation in the CDX and is a fitting capstone to the IA sequence.

This capstone course covers a broad range of topics in computer and network security. Each lesson has a hands-on component where students use virtual machines, open source tools, and an air-gapped network to accomplish IA learning objectives. Students become very familiar with many tools in class, such as *Backtrack*, *Metasploit*, and *Helix* to name a few.

During the preparation phase, cadets assessed and cleaned the "untrusted" user workstations using a home-made *Tripwire*-like script that compared the NSA provided workstations with clean installations of the same operating system. They successfully identified most of the malware that had been hidden on the workstations, but discovered that they had to be careful removing the offending programs, as the machines would stop working if programs or DLLs were deleted or upgraded without testing.

The second biggest task the cadets faced was the complete rebuild of the Blue node's website and database. Utilizing material taught in USMA's *Distributed Network Applications* course, every html/php page was recoded in a secure manner. The database was rebuilt from the ground up, with all of its data verified and validated. Several instances of embedded malware were discovered in this way. These discoveries were credited with USMA's resistance to the SQL injection attacks that were launched against the Academy's network.

Communication is vital to USMA's success in the CDX. This was a special focus this year and was demonstrated by the speed with which students were able to detect, diagnose, and block attacks from the Red Team. The team also standardized as much as possible on a FreeBSD platform, easing configuration and troubleshooting.

The leadership, faculty, and students at USMA firmly believe that the CDX is an excellent capstone to the IA sequence. The CDX provides the students the chance to design, build, and defend a computer network against professional-level, full-speed attacks. Many students have commented that they learned more in the four weeks of CDX preparation and execution than they did in the rest of their four years as a computer science student.

3.2 Air Force Institute of Technology

AFIT has two courses focused strictly on the CDX, *Cyber Defense I* and *Cyber Defense II*, taught by Mr. Tim Lacey. The courses are each worth four credit hours, consisting of forty hours of class time and twenty hours of scheduled lab time. In practice, our teams spend about twenty hours of class time and upwards of fifty to sixty hours of lab time preparing for the CDX. Most classes at AFIT are taught by lecture and reinforced through labs. However, the CDX classes are designed to get the students into the lab and onto the machines as quickly as possible. Some class time is necessary to provoke network design and security methodology discussions and to track progress as we set up and secure the network. However, once the decisions have been made as to the design of the network, the students spend most of their time in the lab.

Prior to 2007, AFIT teams averaged twelve members. Since then, AFIT has fielded two teams averaging fifteen members per team each year. The teams are made up of Air Force officers ranging in rank from Second Lieutenant to Major, Air Force Non-commissioned Officers, and DoD civilians. All participants are AFIT students seeking either a Master's degree or a Ph.D. Students' technical abilities range from novice computer users to seasoned network administrators.

Information Assurance is one of the key tenets of security taught at AFIT as part of its *Cyber Curriculum*. The CDX courses at AFIT are conducted under the supervision of the *Center for Cyberspace Research (CCR)* and include network defense, network attack, software security, forensics, and various courses on computer theory. The CDX courses are among the most popular at AFIT due to their heavy hands-on makeup.

Our use of *Internet Protocol Security (IPsec)* to protect individual machines proved to be very successful. We chose an architecture that featured a proxy server to filter workstation access to the Internet and a firewall to keep unauthorized users from attacking private machines while keeping malware on the workstations from calling back to pre-configured servers. The use of classic network defense techniques such as the removal of unnecessary services and minimal user privileges also proved to be a very good tactic.

During the exercise, we discovered our Instant Messaging (IM) servers were vulnerable to an attack that allowed users to change other users' passwords. A patch for this vulnerability was published the week before the CDX, but our teams failed to discover it and the IM servers were compromised. Fortunately, the user accounts that had passwords changed by the attackers were not administrative accounts and thus the damage caused by this exploit was limited to just the changing of passwords. We also had a couple lines of incorrectly written code on our web server that allowed an attacker to add records to our database. Once again, the user privileges limited the amount of damage the attacker could inflict.

The attackers' strategy was to first exploit any malware that had not been disabled on the workstations. At AFIT, we were able to utilize scripts developed in-house that searched for unsigned executable files. Files signed by Microsoft were known to be authentic and free from malware. Any unsigned files were then assummed to be malicious and deleted. This technique proved very effective as no malware on our workstations initiated callback sessions to the attackers. The skill level involved in creating these scripts was high and we were not aware of any other school that utilized this technique. Traditional utilities to identify malware was simply not sufficient to discover all the files planted by the attackers, and these are the very tools most used. Simply put, running a tool is not sufficient to find all the malware planted on the workstations by attackers. In-depth knowledge of how executable files are constructed and signed is also needed.

The only specific attacks launched against the AFIT teams was those against the IM servers and the web servers. The IM and web server attacks were successful, though in both cases the damage inflicted was limited by appropriately configured user accounts. The only other attacker activities we recorded were the intense scanning of our networks. These scans were continuously probing our machines for open ports and unsecured applications that could then be exploited.

AFIT is a firm believer in the importance of hands-on reinforcement of learning through exercises like the CDX. Most of our students have never had the opportunity to set up a network, much less the chance to secure one. It's very important for our future leaders to have first-hand knowledge of the difficulties encountered in securing a network while maintaining its functionality. The competition itself provides motivation for the students to give it their all. They want to win, so they invest long hours ensuring their services are working securely. They take great pride in their work. When they perform well, they are very gratified. Likewise, when they stumble or are tripped up, they are disappointed. Fortunately, we have had more success than failure.

3.3 United States Merchant Marine Academy

USMMA is the undergraduate federal service academy established to train merchant marine officers. The USMMA is the smallest of the five service academies with approximately 1000 students. This year's CDX team consisted of five members – two freshmen and three seniors.

The USMMA does not have a computer science or electrical engineering department. The IA program at the USMMA is an extra-curricular activity taught by Mr. Efstratios Gavas and handled as a club organization. The CDX team members participate for fun or as part of an independent study outside their main course of study. The students generally have little, or no, formal training in information technology (IT), computer science, or IA prior to their participation in CDX.

In earlier years, we tried to cover more topics in the classroom to establish a foundation of knowledge but we found it difficult to translate into operational knowledge. We found setting up services was constructive and stimulated questions. For example, in the first exercise the students were walked through the point-and-click *Ubuntu* webserver installation, which provoked student questions that were addressed in short focussed discussions. This style of teaching naturally revisited concepts with regularity and the learning objectives were achieved through reinforcement.

Peer teaching between students was encouraged, and resulted in a team with general knowledge about all the systems. Given the small size of the team, specialization was not possible. Contrary to what is generally considered best practice, specialization would not have helped our team as we had, at times, only one or two people monitoring and administering all of the systems. Once a group had achieved their goal, the final task was to share key points about a system with the other groups. This final task helped solidify understanding of each topic, and advanced the start of the other groups' learning.

The team showed improvements in handling the Windows domain and workstations over previous year, this area continued to provide challenges to our team. The NSA placed several pieces of malware on the provided host-nation workstations. The team was able to find a number of viruses using a traditional virus scanners, but missed the malware which was modified to hide its virus signature. These missed viruses would make various callbacks and generally try to enable VNC, or shell, access back to the workstation.

In most cases, using their network monitors tools, the team was able to see the unusual traffic and track the traffic back to the particular workstation. After first blocking the network connection, they worked to identify the specific application using tools from the *SysInternal Suite*, particularly *TCPView*, and *Process Explorer*, as well as *NetStat* and other standard administrative tools. Although the team was able to stop the connection and eliminate the specific executable, they were not able to track down the malware which activated the executable. Consequentially, the malicious connection would reestablish after some time, and the elimination process would repeat.

The team did choose to rebuild the webserver using part of their notional budget. In doing so, they sanitize the input fields using the following added code:

```
foreach ($_COOKIE as &$cookie) {
 $cookie = trim( htmlentities(
   strip_tags(@mysqli_real_escape_string(
     $mySQL, $cookie)),
   ENT_QUOTES));
}
foreach ($_GET as &$get) {
 $get = trim(htmlentities(
   strip_tags(@mysqli_real_escape_string(
     $mySQL, $get)),
   ENT_QUOTES));
}
foreach ($_POST as &$post) {
 if (is_array($post)) {
  foreach ($post as &$_post) {
   $_post = trim(htmlentities(strip_tags(
     @mysqli_real_escape_string(
        $mySQL, $_post)),
     ENT_QUOTES));
  }
 }
 else {
  $post = trim(htmlentities(strip_tags(
    @mysqli_real_escape_string(
       $mySQL, $post)),
    ENT_QUOTES));
 }
}
```

This code uses only standard PHP functions and provided the needed protection from the attempted SQL inject and XSS attacks. Although the website was heavily targeted these changes, along with careful configuration of the webserver and database on FreeBSD was enough to prevent any compromises of the website.

Another area which had mixed results was the use of graphical tools such as *m0n0wall* (firewall, NAT, routing, DNS) and *eBox* (email, chat, web, database) to simplify administration and understanding of various services. By using the graphical tools, the students were able to focus on concepts before worrying about most of the implementation details, but still in an interactive and hands-on way. The graphical interfaces were more approachable and less intimidating. However, ultimately

these systems where phased out in favor of a more flexible FreeBSD solution. This additional effort further aided the understanding of the final setup.

3.4 Royal Military College of Canada

This year was the first year there was foreign participation in the CDX. Located in Kingston, Ontario, RMC fielded a CDX team of eight graduate students. While RMC offers accredited degrees at the bachelor, master, and doctoral level, winter term exams precluded participation from undergraduate students. Two members of the faculty, a technician and a research assistant, also helped prepare the RMC CDX team. Preparation for the CDX became a major activity of RMC's *Computer Security Laboratory (CSL)*, a research group from the *Department of Electrical and Computer Engineering* focusing on computer network operations within the *Canadian Forces* and the *Department of National Defence*. The principal investigator of the RMC CSL is Dr. Scott Knight. Two other faculty members are investigators in the CSL and they are joined by other associated faculty members and numerous graduate and undergraduate students.

All of the RMC team members were enrolled in graduate programs in either computer engineering or software engineering. The majority of them participated in the CDX as part of a graduate level course in *Computer Systems and Network Security* taught by Dr. Scott Knight. The course devoted three hours to lectures and two hours to laboratory components each week, although students spent many more hours completing laboratory exercises. Laboratory topics included Linux installation, network configuration, packet capture, internetwork routing and ARP, password cracking, physical access attacks, network sniffing and spoofing, firewalls, and packet crafting.

Many of the practical aspects of this graduate course were geared toward preparing the students for their eventual CDX experience. Each student became familiar with network engineering and design, and they were also required to conduct more in-depth research for a graduate-level paper on a topic relating to the CDX. This specialization by individual team members allowed the RMC team a wide range of expertise, without requiring team members to become experts in all topics.

The CDX experience was invaluable for the RMC team members. None of the students had experience in a *Network Operations Center (NOC)* prior to the CDX, and they relished the opportunity to apply the theoretical concepts they had been exploring over the course of their studies. Many of the students commented on how seeing their network under attack brought home the importance of sound, simple designs that could be easily monitored, and of a network architecture that was flexible enough to allow them to respond to the fluid situation cause by the Red Team activity.

Many valuable lessons were learnt during the CDX. The exercise helped reinforce the importance of communications. It may be easy to work in isolation when designing a network, but such an approach is not suitable to react to the ever-changing situation caused by Red Team actions.

4 Attacks

Red Team attained twenty-one significant, distinct compromises of Blue Team hosts in the course of CDX 2009. This figure does not count reported compromises that were disallowed by White Team as being trivial or redundant. It also does not include repeated compromises on the same host when using substantially similar methods.

These twenty-one compromises fall into several categories, as follows:

- *Credential hijacking (1)*: Stole administrative credentials after domain administrator logged into a server that had already been compromised.
- *Credential replay (2)*: Replay hashed administrative credentials or cookies, gaining control of web servers.
- *Cross-site scripting (1)*: Modifying an already compromised Web server to introduce a cross-site scripting vulnerability that remained in place for the remainder of the exercise. Later, leverage this vulnerability to recover web cookies.
- *Malware callbacks (7)*: Pre-positioned malware, designed to open contact from inside the Blue Team network, gave rise to several distinct compromises. These callbacks came from the Windows workstations supplied to the teams.
- *OpenFire remote access (4)*: A new remote access vulnerability in the *OpenFire* instant messaging server was made public, just days before the beginning of CDX. Four teams found using this server had failed to apply the available patch. The Red Team was able to develop a exploit during the exercise and gained user-level access to all four servers.
- *SQL injection (2)*: Used two distinct SQL injection vulnerabilities in order to make arbitrary queries into a backend database. Exploited this capability to obtain hashed passwords for administrative accounts.
- *SSH reverse tunnel (1)*: Set up an SSH reverse tunnel from a compromised workstation to that site's email server, gaining unauthorized access.
- *Windows DNS stack overflow (1)*: The Windows domain controller provided was vulnerable if not properly patched. Used Metasploit to exploit this vulnerability, gaining system-level access to the domain controller.
- *Weak passwords (2)*: Guessed passwords that yielded user-level access.

Red Team had a range of success against the various academies participating in this publication. While

USMA had no significant compromises. AFIT was only compromised once using the *OpenFire* exploit. Meanwhile, USMMA and RMC both had issues with repeated *Malware callbacks*. Additionally, using a *SQL injection*, the Red Team was able to retrieve the users table for the RMC website, and gain control of the machine.

The range of success in exploiting the teams can be attributed to the operational experience of the students. Programs which provide a structured approach to teaching involving hands-on learning, and allow the students to develop over time, seems to be the most effective. In the case of RMC, the lack of experience participating in the CDX also played a part in their exploit troubles.

5 Conclusions

Participation in information security exercises can provide focus to an IA curriculum and is an enduring motivator for students to learn effective security skills. By incorporating budgets, help desk requests, and other operational issues into the exercise, the learning experience strengthens practical aspects of risk mitigation.

Labs and hands-on activities can better direct student learning than traditional classroom teaching alone, as well as positively reinforce traditional teaching time. We have seen a correlation between emphasis on lab activities and better achievement of learning goals and retention of knowledge. An effective security curriculum should be designed to get students into lab activities early and develop security concepts through hands-on tasks. Although these tasks can be time and resource intensive, they can be scaled to fit the instructor's workload and class size.

Many key skills are developed during the CDX based on the teamwork aspects of the competition. Through the planning and organization of the network and the high-pressure environment of the competition, students not only develop the technical skills needed to design and implement security solutions, but the leadership skills needed to manage systems in a hostile network. Trying to develop these skills without the operational pressures of a live network would be difficult to simulate. In surveying the students after the exercise, the overwhelming response was that the students felt they knew significantly more just after the competition then even just days before. An objective assessment of their skills also showed an improvement in many areas, including operational skills, false alarm rates, network design, and leadership.

CDX illustrated a number of effective measures used to prevent, or detect, compromises. Workstation analysis using comparisons against known-good files proved much more effective than traditional virus scanners. However, the analysis did require more time to perform. Also, thoroughly sanitizing web inputs was critical for safe website operations, but requiring an understanding of form processing. Additionally, it was important to make sure the systems used have been properly patched and updated. Although this is a somewhat obvious statement, it should be noted that in real-world operations, patch management is a complex issue that requires responsiveness and care. Further, password management and conservative use of administrative access require careful thought to properly secure a system.

Lastly, for participants to truly extract the full potential from an information security exercise, the exercise infrastructure must be conducive to collaboration. Premeetings and after-action reports to establish learning goals are critical for proper dissemination of information. The exercise organizers must encourage sharing of lessons learned among all the participants and carefully consider all the various learning goals while constructing the exercise.

Exercises, such as the CDX, provide much needed hands-on experience, and an approach to training which includes communication, management, and team building along with the needed technical skills. It is not sufficient to just teach technical skills and expect the students to understand how to properly secure a network. It is only when all of the communication channels, administrative processes, and configurations are understood and working together that a system can be manageably secured.

Acknowledgment

The authors would like to thank all of the participating service academies for providing a challenging competition environment and a collective learning experience. Additional thanks goes to Jon F. Zeigler and the whole NSA team for their hard work developing and supporting the CDX.

The authors also respectfully acknowledge the sacrifices and service of all our men and women in the armed forces.

References

[1] Cyber Defense Exercise (CDX) 2009, *Realistic Network Defense in a Hostile World*, NSA CDX Fact Sheet. 21-24 April 2009.

[2] Information Technology & Operations Center, *Cyber Defense Exercise*, United States Military Academy. *http://www.itoc.usma.edu/cyberexercises/cdx/*

[3] Academic Center for Cyberspace Research, *Cyber Defense Exercise*, United States Air Force Academy. *http://www.usafa.edu/df/dfcs/accr/cdx2.cfm*

[4] B. Mullins, T. Lacey, R. Mills, J. Trechter, S. Bass, *The Impact of the NSA Cyber Defense Exercise on the Curriculum at the Air Force Institute of Technology*, 40th Annual Hawaii International Conference on System Sciences (HICSS), pp.271b, 2007