Experiences with practice-focused undergraduate security education.

Robert L. Fanelli and Terrence J. O'Connor
United States Military Academy
West Point, New York

Abstract

The combination of competitive security exercises and hands-on learning represents a powerful approach for teaching information system security. Although creating and maintaining such a course can be difficult, the benefits to learning are worthwhile. Our undergraduate *Information Assurance* course is practice-focused and makes substantial use of competitive exercises, such as the National Security Agency Cyber Defense Exercise, to promote learning. We recount experiences and lessons learned from creating and conducting this course.

1 Introduction

The United States Military Academy's *Information Assurance* course offers intensive, practice-focused education in information system security. We emphasize hands-on learning and security competitions to make this course a challenging and rewarding experience for our students. We continually update and improve the course to address changing technology, tools and threats.

Our *Information Assurance* course is organized into two phases. The first is a classroom phase, combining lectures, practical exercises and laboratory work. The second phase centers on planning, implementation and execution of a capstone exercise, the annual National Security Agency (NSA) Cyber Defense Exercise (CDX) [6].

This paper presents an overview of our current *Information Assurance* teaching methodology, recent experiences with the course and a discussion of lessons learned. Section 2 discusses the classroom phase of the course, including our capture-the-flag scrimmage. Section 3 presents the exercise phase, including a discussion of new CDX features and the student response. Section 4 provides a discussion of lessons learned. Section 5 is concluding remarks.

2 Classroom Phase

The classroom phase of *Information Assurance* covers foundation concepts for information system security and provides practical experience with a wide range of security techniques and tools. We emphasize active learning, combining traditional lecture with hands-on practical exercises and laboratory work. We have also incorporated competitive security exercises as part of the classroom curriculum.

2.1 Classroom Instruction

Our classroom instruction includes a mix of lecture and hands-on learning. The class schedule generally follows a pattern of a lecture lesson to introduce a concept followed by a practical exercise lesson that provides deeper, hands-on exploration of the topic. As with all classes at West Point, our course is conducted in a small group format with sections of no more than 18 students.

We use Skoudis' Counter Hack Reloaded [5] as a textbook. This book gives clear coverage of a wide range of practical security topics in a way that engages our students. We also cover concepts of network security monitoring and defensible networks presented by Bejtlich [2].

The course includes bi-weekly laboratory periods. These labs offer the opportunity for more independent work. The students have tasks to accomplish and guidelines for doing so. However, they are required to perform research on their own to accomplish the tasks. "Search the Web" and "Read the Manual" are common replies to questions posed in the lab. The labs have the students working in pairs to build secure servers. The teams each build a FreeBSD server and a Windows Active Directory domain controller, then install and securely configure services such as DNS, Web and a database. This approach develops the students' capacity to solve technical problems for themselves as well as to prepare them for tasks they will perform in the CDX.

West Point has a well-provisioned Information Warfare laboratory for students to do the hands-on security work. This laboratory offers each student dedicated access to multiple host systems on air-gapped networks. We make extensive use of virtualization both to emulate larger physical

infrastructures and for the ability to easily 'undo' errors and experiments gone awry. Students are more likely to experiment with new techniques when they know that they can easily back out by reverting to a virtual machine (VM) snapshot.

2.2 Capture-the-flag Scrimmage

This year we included a new 'Capture the Flag' (CTF) Scrimmage exercise as one of the lab periods. This exercise allowed teams of students to go head-to-head, applying both defensive and offensive security skills. The CTF Scrimmage tied together the security concepts presented throughout the course while also giving the students a glimpse of the conditions in which they would operate during the CDX.

The exercise objective was for each team to defend a body of information they possessed while capturing as much of the other teams' information as possible. The students operated in four teams with three or four on a team. The teams had identically-configured sets of Linux and Windows servers to defend. The servers had vulnerabilities and configuration problems designed to illustrate course concepts such as enforcing least-privilege, the need to minimize services and best practices for password authentication. Every team also had four workstations configured with the Backtrack 4 "Linux-based penetration testing arsenal" [1] available for their use in attack or defense.

The teams had great freedom in how they could go about defending their servers. However, a requirement to keep certain network services available prevented simple defensive solutions like 'pulling the plug' or executing a denial of service attack on the network infrastructure.

The exercise 'flags' represented items of valuable information an attacker would want to pilfer. The flags were text-based, consisting of a unique identifier and a verification phrase. Ten flags were placed on each of the servers, some in obvious locations and some not so obvious. We created flags in three classes. First were the 'Easter eggs', readable simply by looking in the right place, such as by banner grabbing. Second were 'user-mode' flags, requiring user-level access to the server to be read. Third were the 'root-mode' flags that could be read only with root or administrator-level access. This approach ensured all the students could at least gather some 'low-hanging fruit' while making it hard for anyone to get all the flags in the time available.

Guidance provided to the students for the CTF Scrimmage was deliberately vague:

> You will have the two hour lab period to secure your systems and gather as many flags as you can find. Submit the list of flags identifiers and corresponding phrases you have found, along with the results of your reconnaissance, at the conclusion of the lab. You may submit this information in hard copy or in electronic form on the exercise network.
>
> **Scrimmage Rules of Engagement:**
>
> 1) Don't secure your servers into uselessness. Your monitored services must remain available on the network. On the Windows 2008 Server these services are http, ftp and smtp (Internet Information Server). On the Ubuntu server they are http (Apache), MySQL and ssh. If the status monitor shows your system or services as 'red', you have done something wrong.
> 2) Do not change the IP addresses of the systems.
> 3) Do not shutdown or cripple any target server systems.
> 4) Do not delete, move or otherwise modify any flags.
> 5) If you get root on a box, do not carry out a 'scorched earth' policy. If flags are modified or deleted then they may be declared invalid for scoring. If a target system is destroyed or crippled, the set of flags on that system may be declared invalid for scoring. Thus, it is in your interest to avoid destroying the sensitive information after you have gathered it.
> 6) Don't revert VMs to a snapshot without permission. [This is a CDX rule, and a good one.]
> 7) Don't execute network flooding attacks, denial of service on the network infrastructure or other similarly unsophisticated attacks that will only serve to ruin the exercise. Violators will have their switch ports disabled with extreme prejudice.
> 8) Think differently. Compete hard. Have a good time.
> 9) Whining is forbidden.

The students had to work out for themselves how to organize their teams, how to defend their servers and how to find and capture flags. This required the teams to do research, planning and coordination before the lab period. As a graded pre-lab assignment, the teams prepared written action plans in the form of checklists, outlines, flow charts or other formats they found appropriate. The action plans detailed how the students intended to secure and defend their servers and go about capturing flags from the others.

The teams were free to begin securing their servers and to attack simultaneously at the start of the two-hour CTF Scrimmage lab period. The teams with the best thought-out action plans closed the most

obvious holes in their servers quickly. Some others struggled or jumped right to difficult tasks while missing simple, relatively obvious measures such as changing the default administrator password on a server.

On the attack, teams that did more complete reconnaissance and coordinated their efforts performed better on capturing flags. For example, many of the 'Easter egg' flags were easily discovered using the reconnaissance techniques covered earlier in the course. Conversely, some teams went right into using Metasploit [3] to 'get root' on the first target they found, ignoring the 'low-hanging fruit'. Further, the teams knew they had been given nearly identical servers. Some teams used this knowledge to good effect, applying what their defenders had learned about vulnerabilities on their own servers to help the attackers' efforts against the other teams.

The final flag counts were mostly for 'bragging rights' rather than for course grades. We instructed the teams to "submit the flags they possessed" at the conclusion of the lab period. The most successful teams came to the realization that 'possession' meant they could improve their results by submitting the flags on their own servers along with the flags they had captured. This was a good example of the creative problem solving we encourage.

The teams prepared written after action reviews (AAR) as another graded deliverable. These detailed good and bad points about the teams' action plans and their efforts during the exercise. The AARs also addressed suggestions for how to improve the exercise itself. We later conducted an in-class AAR that reviewed the teams' performances, detailed the initial vulnerabilities, configurations issues and the flag locations, and discussed how the teams could have improved their results.

The students enjoyed the CTF Scrimmage and learned a great deal. They saw the need for preparation and coordinated effort as well as the value of looking beyond the obvious and applying creative problem solving. The CTF Scrimmage also reinforced many of the information system security lessons presented earlier in the course. Finally, the competitive aspect of the CTF Scrimmage seemed to build enthusiasm in several students who had been somewhat indifferent to the earlier course work. The challenge of the competition captured their imaginations and led them to achieve deeper learning during the exercise phase of the course.

The classroom phase provided the students with a solid foundation of security knowledge and skills. We found that the alternating lecture and practical exercise format was effective for presenting security topics and reached students of various learning types well. This phase also set the conditions necessary for the students to get the most out of their participation in the CDX.

3 Exercise Phase

The latter third of the *Information Assurance* course revolves around the students' participation in the annual NSA CDX. The CDX gives the students the opportunity to apply their knowledge to design, implement and defend a network against live adversaries.

3.1 CDX Description

The CDX is an annual event challenging teams from the service academies and military graduate institutions in the design, implementation and defense of computer networks. The 2010 CDX included undergraduate teams from the United States Military Academy, United States Naval Academy, United States Air Force Academy, United States Coast Guard Academy and United States Merchant Marine Academy. It also included graduate student teams from the Air Force Institute of Technology, Naval Postgraduate School and the Royal Military College of Canada. Although all teams participate equally in the competition, only the undergraduate teams compete for the NSA Information Assurance Director's trophy.

As the name implies, the CDX is primarily defensive in nature. The exercise scenario casts each school's 'Blue Cell' as a military headquarters operating a network as part of a joint military task force. The NSA provides a 'White Cell' that acts as the scenario's joint task force headquarters, controls the exercise and determines the winner.

The teams design and implement networks conforming to an exercise network specification. This includes a set of required services, such as e-mail, web or voice over IP telephony, which must remain available during the exercise. The teams must also operate a population of end-user systems, including two Linux workstations and an Active Directory domain with three Windows workstations. The exercise imposes a notional budget on the network implementations, limiting the type and quantity of systems, software and security safeguards a team may use. This forces the teams to make realistic tradeoffs between competing requirements, deciding how to spend their limited budgets to get the greatest

benefit given the mission and the threat.

The adversaries for the CDX are a NSA-provided 'Red Team' that attempts to penetrate and exploit the Blue Cell networks. The exercise is unclassified, so the Red Team uses only exploits for publicly disclosed vulnerabilities. Limited 'social engineering' attacks, such as spoofed e-mail messages, are allowed. However, on-site exploitation attempts and other 'out-of-band' attacks are outside the scope of the exercise. Sustained denial of service attacks based on bandwidth starvation or sending large volumes of traffic are also prohibited. Since the teams compete from their own labs, connected by a virtual private network, it would be trivial to saturate the network, bringing the exercise to a halt while teaching the students little.

The team scores for the CDX depend on their ability to preserve the confidentiality, integrity and availability of their systems. Teams loose points should one of their required services become unavailable, whether from Red Team activity or a mistake by the owning Blue Cell. Teams also loose points if the Red Team successfully penetrates their networks, with more severe compromises resulting in larger penalties. The penalties for compromises are assessed per-system and on a daily basis, meaning that a compromise of a single system that persists over multiple days generates a new penalty each day.

Teams also have opportunities to earn points. For example, teams can gain points for thorough, timely and accurate processing of incident reports and periodic system status reports. The CDX also presents the students with 'scenario injects' designed to further test their knowledge and skills. These 'inject' tasks typically include forensic analysis of a recovered system, responding to scripted security incidents and reacting to orders to add new systems to the network on short notice. Teams earn bonus points for successfully completing these tasks.

3.2 New Features in the 2010 CDX

The NSA organizers and faculty members of the participating schools collaborate to update the exercise content to support changing educational objectives as well as new technology and threats. The 2010 CDX was designed to confront teams with a more realistic threat of client-side attacks. User workstations were included in previous years; however, the teams were not really challenged with effective client-side threats. Previously, students were the only users of the workstations and could secure them almost to the point of uselessness. Further, the students could sit at the workstations, watching closely for anomalous activity and killing processes with extreme prejudice.

In 2010 the NSA provided a Grey Team of non-malicious but unsophisticated users located at each Blue Cell site. These users operated the workstations, generating realistic traffic, using email, opening attachments, visiting dubious web sites and performing similar actions that facilitate client-side attacks. The Grey Team operated under a common set of 'rules of engagement' to ensure each team faced a consistent client-side threat.

The five user workstations were intended to represent a much large population of systems. Thus the exercise rules prohibited Blue Cell team members from directly accessing the user workstations outside of a declared maintenance period. This prevented unrealistic security measures such as 'process whack-a-mole.' Administrators may be able to play this game effectively on five workstations but could not do so on 500. However, a team could declare an incident and access a workstation to investigate or contain a compromise. Doing so would result in a small point penalty to reflect the loss of productivity and inconvenience to the users. Teams thus had to make some realistic cost/benefit decisions when considering incident response.

Teams also had the opportunity to publish 'acceptable use policies' (AUP) for their networks and their Grey Team users. This provided the students with the opportunity to consider the issues with writing an effective AUP and how to combine administrative and technical security measures. It also provided some interesting learning opportunities as the students enforced their AUP on the Grey Team.

To further increase the challenge of client-side threats, software patching for the workstations was frozen as of September 2009. This allowed the vulnerabilities disclosed from September through the April 2010 exercise start to represent 'virtual 0-day' threats. The teams could not apply software patches, but could use other mitigation strategies. An exercise inject replicated the availability of a 'new' software patch and opportunity for the teams to install the patch during the exercise to mitigate a vulnerability actively exploited by the Red team.

3.3 Preparation for the CDX

At the mid-point of the term, we shift focus of the *Information Assurance* course to preparation for the CDX. We use the SANS Institute model for incident handling [4] as a framework to guide the students' effort before and during the exercise. This incident handling model includes the following sequence of

steps: 1) Preparation 2) Identification 3) Containment 4) Eradication 5) Recovery 6) Lessons Learned.

Preparation. We assign the students specific jobs for the CDX based on their preferences, proficiencies and overall work load. The students work in sub-teams of two or three on a specific service or function, such as providing web services, network infrastructure or network security monitoring.

Students design their network to meet the requirements and budgetary constraints in the CDX network specification document. The team meets as a whole to develop the design, with each sub-team briefing their requirements, proposed courses of action and the corresponding costs. The students then determine required versus 'nice to have' items, making the necessary tradeoffs to create a final design and budget. NSA reviews the designs for compliance with the network specification and approves them for implementation.

The students have approximately three weeks to implement their approved network design. They build their systems from scratch, starting with 'bare metal' and installation media. The team typically builds a common FreeBSD baseline operating system VM image. Each sub-team then customizes its copy of the image, installing required services and configuring for security.

Approximately two weeks before the start of the competition, the NSA delivered two pre-compromised workstation VM images to be included in the Blue Cell network. These were a Windows XP machine and an Ubuntu Linux machine, containing malicious executables, callbacks, weakened security postures, pre-shared SSH keys, and a kernel-mode rootkit. The students had to dig deep to clean up these systems since the CDX rules restricted the use of anti-virus software and pre-packaged hardening scripts to automate the task.

Our students this year approached cleaning and validating machines for use on the network this year with a systematic method that proved rather successful. The forensics team led the effort, mounting the hard drives offline and calculating hashes of each file and comparing those hashes to known benign and known malicious files. After identifying the known malicious files and the unknown content, the students reduced their scope to perform a thorough forensic analysis of the files created by the NSA. With a reduced scope, the students were able to identify locations for callbacks, packed files for unrolling rootkits, and scripts to further weaken the local machine security posture.

Also, as mentioned above, the workstations were vulnerable to the 'virtual 0-days' created by freezing the patch date eight months before the exercise. The team extensively researched security bulletins pertaining to these vulnerabilities. In many cases they were able to apply procedures in these bulletins to mitigate the vulnerabilities without a software patch. They were also able to identify these known, but unmitigated, vulnerabilities on the workstations to the network security monitoring team for additional surveillance.

3.4 The CDX Live Phase

The CDX live phase ran four days with students in the labs from 7:00 AM to 10:00 PM daily. The students were required to vacate the labs outside of these hours. The Red Team, however, retained opportunity to operate against the Blue Cells 24 hours a day. This gave the Red Team the ability to replicate a real attacker's ability to strike at a time of his choosing, not just when administrators are sitting at consoles. Actions in the live phase also tended to follow the steps of the incident response process.

Identification. Differentiating an *event* (something merely measurable on the network) from a security *incident* (an adverse event or the imminent threat of such an event occurring) provided an excellent learning opportunity for the students. The exercise's mix of legitimate and malicious traffic formed a rich context for examining events and incidents.

The addition of Voice-Over-IP in the exercise this year provided a valuable lesson in distinguishing between an actual malicious incident and a benign event caused by poor network design. Within minutes of the exercise starting, improper Session Initiation Protocol (SIP) configurations at multiple schools caused a storm of SIP registration packets that appeared as a flood attack by an adversary. Teaching the students to holistically examine an event by looking at logs, talking to on-site handlers, and soliciting advice from network engineers served the students well in their incident response during the exercise.

Containment. The students moved quickly to contain each incident as it was identified. The CDX scoring model forced the students to make some realistic cost/benefit decisions on the fly. For example, is it worth the point penalty to pull a machine offline and remove malware or can network safeguards mitigate the risk of a compromise penalty until a scheduled maintenance period?

Concerned the adversary would attempt to

deliver client-side exploits to the vulnerable version of Adobe Reader required on the workstations, the students created a proxy to examine incoming PDF documents. The proxy re-rendered the files to cripple any exploits. This allowed the students to temporarily contain the risk posed by a malicious file without having to take the machine offline.

Eradication. The students performed actions to eradicate threats and vulnerabilities after the initial incident containment and daily during the scheduled maintenance periods. During eradication the students removed any content left by attackers or, possibly, by Grey Team users that exposed the network to attack. The on-site handling incident team used this time to examine log-files, turn-off unnecessary services and securely delete any suspect or malicious files.

We used this eradication phase to remind students that attackers often try to reuse successful methods. Consequently, the students archived the malicious content later analysis, gaining insight in methods to identify and mitigate subsequent attacks. For example, the students identified that Grey Team users had run software that enabled the SSH service on the Linux work stations. While the network perimeter blocked SSH traffic from entering the network – any subsequent attempts to use SSH received a thorough investigation.

Recovery. The fast pace of the exercise and the constant attack pressure by the Red Team forced the students to perform recovery activities throughout the CDX. We used this as an opportunity to reinforce the lesson that many threats are persistent, requiring vigilance to prevent additional incidents. During recovery the students continually monitored traffic, service availability, and user activity on the network for anything they failed to remove during the eradication phase. They also examined other systems to ensure similar vulnerabilities did not exist elsewhere in their network.

Realizing that the user workstations posed the most significant risk in the exercise, we used small a budget increase granted by NSA to all teams during the exercise to further mitigate this risk. The network security monitoring team 'bought' additional capability for the intrusion detection system to capture traffic within the segregated virtual LAN (VLAN) connecting the workstations. This proved useful, as the monitoring team was able to identify malicious network traffic that was confined within this VLAN and not previously visible to the IDS.

4 Lessons Learned

The value of competition. Competition inspires our students to a higher level of interest in mastering the course material. Incorporating competitive events such as the CDX and CTF Scrimmage in our *Information Assurance* course leads the students to commit considerable effort to learning and applying the course material.

The thought of facing live opponents and competing with their peers tends to capture the imagination of our students far more effectively than could traditional classroom work alone. The competitions also offer valuable opportunities for working under pressure in a complex team environment that may not otherwise be available.

Security makes the 'other stuff' more interesting. Studying security can lead students to a deeper understanding of computer science and information technology concepts. In many cases a thorough understanding of how a protocol, program or operating system works is needed to effectively attack or defend it. In studying security our students also gain a better grasp of networking, file systems, operating systems and similar concepts they learned earlier in their studies.

They don't know what they don't know. Undergraduate students require significant guidance to complete and learn from a complex security competition. A large majority of students have little to no professional experience in IT security or system administration. They need sufficient guidance to stay on track and achieve their goals in the time available.

We have used course assignments to lead our students towards their goals. Clearly, assignments are a way to progressively build student skills and knowledge. A series of assignments can also discretely establish the milestones that students must achieve, while leaving them the latitude to learn by doing.

A useful technique is to assign deliverables necessary for a coordinated team effort, such as lists of network port and protocol requirements for each server, as graded assignments. With experience the need to produce many of these deliverables becomes obvious. However, a relatively inexperienced group of students will benefit from this additional guidance. In many cases, at the conclusion of the CDX, our students look back and acknowledge the benefit of course assignments that had previously seemed overly difficult or irrelevant to them.

Students also need guidance in knowing when they have met an objective in system implementation. We have found that they often get something 'just working' and stop, not realizing that more needs to be done. Additional guidance with validation checklists and the development of effective test plans helps students to determine for themselves when they have truly achieved their objectives.

It takes longer than they think it will. We find undergraduate students generally do not yet have the experience to accurately estimate the time required to accomplish complex IT tasks. Our students, for example, consistently underestimate how much time it will take them to implement their Blue Cell network, leading to a weekend-long 'death march' of final CDX preparation. Students should make specific, written estimates of the number of hours they expect a task to take. Faculty can then provide realistic feedback on the estimates, giving the students at least a fighting chance to avoid the need for a 'death march.' On the other hand, there may be a learning benefit from being on such a 'death march' at least once.

Students often miss the obvious, but learn from doing so. On the CTF Scrimmage, several students skipped relatively easy reconnaissance techniques and exploits and went directly to more advanced and time consuming techniques, such as Metasploit. This may be due to the students learning the more advanced techniques in the lessons just before the CTF Scrimmage, making those methods seem more relevant. Some also stated that they assumed simple methods like banner grabbing would not payoff, so they skipped them. The students learned some useful lessons about not missing the obvious possibilities just because they are obvious.

The value of preparation. The CTF Scrimmage showed the students how preparation tends to trump raw skill when it comes time to execute. The students who did best on the CTF Scrimmage were not necessarily the students with the strongest 'hacker skills' but rather those who came up with well thought-out action plans. They were able to move quickly to lock-down their servers and to quickly capture flags from teams trying more improvisational approaches.

Replicating the client-side is hard but important. Client-side threats have eclipsed threats to servers in recent years. Security curricula and exercises must include the client-side to remain relevant. However, replicating client-side threats in an exercise is non-trivial. Many such attacks require user cooperation and may include a social engineering component to get that cooperation. Thus it is necessary to have a live user to act as the foil. The approach of using a Grey Team of unsophisticated users provides a good method to challenge exercise participants with realistic client-side threats.

Security courses are among the most time and resource intensive. Many undergraduate courses, even in computer science, will remain relevant and effective for several years with minimal updating. However, practical security education is dependent on changing technologies and threats and can grow stale quickly. A security practical exercise that is more than a few years old will often be irrelevant to current technologies or threats.

Competitive exercises require extensive preparation but can also provide powerful learning opportunities. The CTF Scrimmage lab required considerable time and effort for preparation. Virtualization is important for creating, maintaining and distributing the computing environments required for hands-on learning in an efficient manner.

5 Conclusion

As with many topics in computer science and information technology, security is best learned through a hands-on, practice-focused approach.
Hearing about threats, vulnerabilities, exploits and safeguards is not nearly as useful as experiencing them first-hand.

Competitions can significantly enhance the effectiveness of an information system security curriculum. A well-structured competitive exercise can provide the context for achieving deeper educational objectives involving synthesis or evaluation. Competitions can also build enthusiasm and interest in students who are less engaged by traditional classroom settings.

West Point's *Information Assurance* course is practice-focused and capitalizes on competitions, notably the NSA Cyber Defense Exercise, to provide a challenging and rewarding educational experience. Although creating such a course and keeping it current is difficult, the benefits are worth the effort.

References

[1] BackTrack Linux. 25 May 2010. <http://www.backtrack-linux.org/>

[2] Bejtlich, Richard. The Tao of Network Security Monitoring: beyond intrusion detection. New York: Addison-Wesley, 2005.

[3] Metasploit Project. 2010. Rapid7, LLC. 25 May 2010 <http://www.metasploit.com/>

[4] Northcutt, Stephen. Computer Security Incident Handling: Step-by-Step. Bethesda: SANS Institute, 2003.

[5] Skoudis, Ed and Tom Liston. Counter Hack Reloaded: a step-by-step guide to computer attacks and effective defenses. New York: Prentice Hall, 2006.

[6] United States. National Security Agency. "Fact Sheet: NSA/CSS Cyber Defense Exercise – After Exercise." Press Releases - 2010 - NSA/CSS, 30 April 2010. 29 June 2010. <http://www.nsa.gov/public_info/_files/press_releases/cdx_fact_sheet.pdf>