The Impact of Regional Cyber Defense Competitions on Student Motivation, Engagement, and Curriculum at Champlain College

Jim Hoag*, Zachariah Tanko**, *Champlain College*

Abstract

Student participation in cyber defense competitions provides an environment different from a normal classroom/lab situation and thereby providing an opportunity for alternative learning and motivation. These competitions are characterized by intense three-day situational exposure to real-life network management, administration and security issues. This experience appears to increase motivation and engagement in student's learning. Students who participate in these competitions gain a perspective of the limits of their current knowledge, the benefits of a more extensive understanding of technical concepts, and the significance of integrating content from a number of areas. Faculty participants, acting as coaches, get insights into curriculum modifications through observation, peer institution discussions, and student feedback. Challenges include student participation, funding, and preparation.

This paper describes how the curriculum at Champlain College has evolved based on our experience with the Northeast Collegiate Cyber Defense Competition (NECCDC) and the effect on student motivation and engagement.

Index terms: Cyber Security, Cyber Defense, security curriculum, information assurance education

---

* *Associate Professor and Chair of the Information Assurance and Technology Department at Champlain College in Burlington, Vt. jhoag@champlain.edu*

** *Assistant Professor of Computer Networking and Information Security, Champlain College, Burlington, Vt. tanko@champlain.edu*

I. INTRODUCTION

Information Assurance, Cyber-Security, and Information Security are areas experiencing rapid growth in industry, government, and education. These fields integrate concepts and skills from a variety of areas including Computer Science, Cryptography, Information Technology, Databases, Networks, and Digital Forensics. Methods need to be developed to allow students to develop a combination of skills and knowledge to be able to meet the future needs in these areas. Curriculum in this area is fairly new and undergraduate programs only recently began to include content in security.

Hands-on learning and motivation are important factors when learning, particularly when learning about technology. Hands-on activities help students associate concepts with skills. Learning is enhanced when students are engaged and motivated. Many networking and security courses include a hands-on component which involves practical applications of concepts [1,2,3,4]. However, students aren't always aware of the "bigger picture" and motivation often becomes finishing the assigned lab task. In addition, the new knowledge might be compartmentalized by the student and only be associated with that setting. If lab activities are based on cookbook-type step-by-step instructions, there may be no learning, simply action. Lab activities are generally focused on a particular topic and are not designed to give a holistic network environment experience. In particular, students do not get to experience a real-world network and security environment. It is also difficult to integrate some networking and security methods in a lab environment due to the inherent risks.

There are some challenges in determining what should be included in Security Education. A single

ISBN 1-933510-96-X/$15.00

course can provide a survey of Information Security. However, the content is extensive and spans a number of technical domains. Educating practitioners able to meet the current and future needs of industry can be attempted using two approaches: adding security content to existing courses or developing courses with specific security content. Federal guidelines and certifications content need to be balanced with theory, conceptual learning and practical skill-sets.

II. HOW THE COMPETITION WORKS

The collegiate cyber defense competition is primarily an undergraduate student event. Teams are limited to eight people. At most two of these may be graduate students.

Each collegiate team is a 'BLUE' team provided with a complete and working enterprise network. The scenario is that the existing IT staff was let go for failure to perform their function adequately and the BLUE team is coming in to take over the management of the network. Each enterprise network configuration is identical for all BLUE teams and consists of a number of computers and network appliances. The computers run various operating systems and offer a standard network services.

At the start of the competition, the teams need to secure their network and maintain network services, while a RED team of experts from academia and industry begin to attack the BLUE teams. Only the RED TEAM can attack during the competition. If a vulnerability is discovered in one BLUE team site, it is reported to a WHITE team. The WHITE teams are the competition judges and scorers.

There is also the BLACK team that is responsible for automatically checking whether service level requirements of the BLUE teams are being met and to generate normal (non-attack) traffic to all BLUE team sites. The BLACK team is also charged with maintenance of the competition network, up to the BLUE team network borders. The BLUE teams are responsible for their own enterprise networks.

During the competition, the WHITE team 'injects' requirements into the workflow of the BLUE teams. All BLUE teams receive the same 'injects' at the same time, to keep the playing field level. 'Injects' can be of any type, from requiring a report to management, to removing one or more team members (simulating illness, for instance) to changing the requirements of the enterprise.

To win the competition, a BLUE team must be able to balance service level responsibilities with external attacks and internal demand. [5]

III. EXPERIENCE

In 2006, Champlain College was approached to see if they would be interested in participating in a regional Collegiate Cyber Defense Competition (CCDC). There had been no previous Northeastern Regional Competitions and hence no experience with this type of activity.

Champlain College had a Computer Networking major that had grown out of an associate's degree program in the late 1990's. An Information Security component was introduced in 2005. In contrast to a traditional Computer Science or Computer Information Technology program, this major focuses on network theory and concepts coupled with practical skills. Each networking course includes security issues for that content area. In addition, the curriculum includes four security courses: Computer and Network Security (SEC 250), Software and Web Security (SEC 335), Securing the Enterprise Network (SEC 350), The Business of Information Security (SEC 420), as well as an introductory Digital Forensics course (FOR 240). The curriculum meets the National Security Agency standards and Champlain College was designated as a center for Academic Excellence in Information Assurance in 2007. There are approximately sixty-five Computer Networking and Information Security majors in any academic year

A. First Year (2007-2008)

Upper-division information security courses were being offered for the first time to a small group of students. It was felt that the students did not yet have

ISBN 1-933510-96-X/$15.00

a sufficient background to participate in a cyber defense competition. In addition, financing the trip, transportation, and timing of the competition were hurdles. Eventually, seven students volunteered and travel was arranged.

A practice session was scheduled, but with little constructive activity. Strategies were suggested and discussed. The coach encouraged hands-on practice sessions, but students were confident they could account for themselves well given their current skills.

1. First Year Competition

During the first competition the students' systems administration backgrounds gave them the necessary background to get essential network services up and running. However, their lack of perimeter security background and weaknesses in areas such as SQL injects took their toll over the weekend and they placed in the middle of the teams in scoring.

From a faculty perspective, the results were exceptional. The students returned to campus with enthusiastic suggestions for networking and security content they wanted/needed to know. As the security courses had just been offered for the first time and were under revision based on classroom experiences, the additional content could be added to these courses.

Students also reported spending long hours at the competition writing incident reports and security policies which was to be part of the Business of Information Security course. They also discussed teamwork successes and challenges.

2. First Year Curriculum Revision

Curriculum should not be designed around a competition event nor should the outcome of an academic program be to win a competition. However, the competition provided guidance on areas in systems administration and information security where the current curriculum was lacking.

Based on the student's reports and information from conferences such as Colloquium for Information Systems Security Education (CISSE), the curriculum was revised to match gaps in content and learning. In addition, the faculty applied for an Information Assurance equipment grant from Cisco Corporation.

Several changes were made to the Security courses. The perimeter security course had been based on an open-source software solution. The course on Software and Web Security had focused mainly on Operating System Security. The Computer Networking and Information Security major is not based on a Computer Science curriculum. As such, there was minimal programming involved in the major. Therefore covering web applications and database vulnerabilities is difficult. However, as it was clear that these are key elements of security, that course was redesigned to introduce these concepts.

B. Second Year (2008-2009)

The initial curriculum changes were implemented. Web scripting and SQL were included in the Software and Web Security course along with web application vulnerabilities. The department purchased a number of used firewalls for students to use in the perimeter security course.

Based on the experience of the first year, the Cyber Defense team was formed earlier and practiced twice prior to competition. In the practice sessions, the team worked on bringing up services, keeping services up while under attack, and remediating problems and tasks given as management injects. About half the team had participated the year before, providing motivation through experience and validating the benefits of understanding network systems concepts and security. It was clear that the students also enjoyed these activities in both the hands-on nature and the interactive environment. This is a good framework for learning not just about security concepts, but also information systems, services, communication, working in groups, and technical writing,

Students served in roles based on technology experience and background. The coaches tried to provide the functions of both management and attackers.

1. Second Year Competition

ISBN 1-933510-96-X/$15.00

The competition provided another opportunity for learning. The students knew they needed to organize better and have more experience in systems security. A competition room was provided for coaches and alternates to participate and they were able to experience the environment. It was clear from the competition activity that students need to understand all services, their relation to the overall system, and the associated security risks. There were also some obvious security content areas to improve on. In particular, SQL injection and rootkits were areas where students had insufficient background.

The debriefing by the RED team was also an incredible learning experience for the students. They could see there was much more to learn in the field. They also got to see the members of the RED team and appreciated the skills of the people they were defending their network against.

2. Second Year Curriculum Impact

The plan for the next year was to organize sooner, practice more, and learn more about particular threats such as rootkits, SQL injection, etc. Curricular changes were made to three courses: Network Design, Software and Web Security, and Securing the Enterprise Network. In addition, it was decided to try to create a course mimicking the environment of the competition to some degree. The goal was to engage students in both security and this integrated network services configuration.

Network Design (NET 330) was modified to include lab activities in which students build a running network, thereby learning about network services from the ground up.

Software and Web Security (SEC 335) was designed to cover operating system security, application security, and web application security. Scripting and the associated security risks were introduced. In addition, a module on SQL and SQL injects was developed. Each area included lab-based activities to help integrate the new information into existing knowledge. There was also a shift to emphasize the mindset of hackers and a security-based approach to thinking.

It was also decided to offer a one–credit hour class in Cyber Defense/Security, recreating some of the environment of the competition, but in a classroom setting.

We received a Cisco grant for Information Assurance which included a number of network and security appliances. The Enterprise Security course (SEC 350) was modified to include lab activities on open-source solutions, legacy equipment, and the new security appliances.

3. Prospective Students

During admissions events, participation in the competition is pitched to the prospective students. It was noted that the Cyber-Defense competition was an event that interested them very much. This seems to be something that engages students at several levels: it is technology based, hands-on, and topical. And while the idea of hacking is a nice fantasy, the idea of securing your network and protecting data may be appealing as a career choice.

4. Infrastructure Modifications

The system configurations during the competition in the second year had been based on virtual systems. This environment seemed ideal for a situation in which a variety of networking and security configurations were necessary. It was decided to switch to a virtualized configuration in the lab environment the networking and security classes were taught in.

5. Collaboration

During the competitions, it was clear that the faculty for the various teams were trying to determine how to implement security into curriculums and the role these competitions played. In our discussions, there were a variety of approaches and challenges. Some schools offered a traditional Computer Science major and were trying to add security components to it. Others had more targeted programs but were still faced with issues such as how to leverage more security content into courses. Challenges included administrative issues, lab space and environment, and faculty training. Conferences and journal articles are

ISBN 1-933510-96-X/$15.00

a traditional method for disseminating information, but as the cyber defense competitions were fairly new, there was little published material.

C. Third Year (2009-2010)

A one-credit Cyber Security class was offered for the first time in the Fall of 2009. The prerequisites were a Microsoft Windows Server and Linux System Administration courses, so most participants were juniors and seniors. The class filled to capacity (15 students). The format of the five weeks class mimicked to some degree, the competition. LANS were comprised of three servers running the common set of services (Web, Email, E-commerce, Database, DNS, DHCP). In the first week, teams were formed and they were to secure the networks. In the second week, management injects and "RED TEAM" attacks were added. The instructors acted as management and attackers. To provide alternative motivation, the students were allowed to attack other teams in the last half-hour. This provided a variety of reactions. Some students concentrated on attacking the other networks, while others focused on defending their networks against these new threats. Still others continued to try to implement injects that had not yet been completed.

In the subsequent three class sessions, the procedure was the same. However, students complained about injects, as they had to learn something on the fly and secure it. Although this is the environment in competition, it seemed a class might need to be more structured. So the instructors "warned" what some injects were going to be (i.e. learn how to secure Solaris). It turned out the students were not proactive with these warnings and would just wait until the next class, when Solaris had been added to their LAN and try to figure it out.

In the course evaluations, specific questions were asked about injects, security, attacking phase, taking the class more than once, and suggestions along with the standard questions. Responses indicated that while students felt the injects were necessary, it was difficult to accommodate them in a one-credit hour class. They also felt that the myriad of attacks (from the red-team and in the last half-hour, everyone) were fun, but they would like to know more about what worked and how people configured attacks. They asked for more structure. Some student comments:

"Due to this class I want to learn more about vulnerability scanners, password brute forcing, IDS, and the metasploit framework."

"This class has made me appreciate the field of network security more than I ever did before."

1. Third Year Competition

Nine of the ten students who participated in the Cyber Defense competition had been in the Cyber Security class. This provided a background in the environment and served as preliminary practice for the competition.

Five practice sessions were held on Sunday afternoons. The Students dedication and motivation were impressive. A major component of their experience was assessing their own knowledge levels and each others and digging deeper into areas where they were lacking. An important perspective on a career in technology is that one cannot know all things.

In the 2010 competition, the group from Champlain College placed in the middle of nine teams. While this might seem to indicate mediocre performance there were important gains in learning, motivation, and engagement. The students came away with several goals. In conjunction with faculty we developed goals of becoming more proficient at managing injects and increasing understanding of security concerns. It was clear that these needed to be learned at the component level, but also at a systems level. We discussed how and where these concepts could be improved in the curriculum. Changes were suggested for several courses but the primary focus was on the one-credit hour course. Discussion also began about a Cyber Security major.

2. Third Year Curriculum Impact

Based on the experience this year, we proposed the following changes to offer two one-credit hour courses in Cyber-Security/Defense in 2010-2011.

ISBN 1-933510-96-X/$15.00

The first would focus on bringing a set of normal network services up and keeping them running while under attack. The second would introduce management injects (system changes) into the mix. This would hopefully give students an opportunity to learn how to secure a system while offered standard services. Those who took the second class would gain experience in system evolution while continuing to offer services in a secure setting.

The pressure of the Cyber Defense competition would be removed, and structure added to promote learning. In the courses, each week a set of exploits/attacks would be given. Students could find out what that attack looked like, how to defend against it, and how to launch the attack. This is similar to what is done in the existing security courses, but presented from a systems perspective. The assignment for the next week would be to finish and bring up whatever services that were not operational, securing them, and investigating the topics for the next week.

The services/exploits might be structured as:

	Software, Services	Exploit, Method
Week 1	OS, Web	Brute Force, Open Ports
Week 2	Email, SSH	Brute force, Cross-site, Phishing
Week 3	Database, E-commerce	SQL injects
Week 4	DNS, ARP	DNS and ARP cache poisoning
Week 5	Connectivity Devices, Wireless	Spoofing and Source Routing

In addition, a Cyber Security specialization was developed to address the need for security personnel at large organizations dealing with multi-national, inter-agency issues. One of the new courses is Systems Security and will be a three-credit hour extension of these one-credit hour courses.

The students on the team also sponsored a local cyber defense event for the first and second year students to help motivate and engage them in the major and security field. The students who participated in the regional competition served as the host group, providing the roles of BLACK, RED, and WHITE teams. The hope is to provide a similar experience for local high schools and community colleges providing an opportunity for those students to get interested and engaged in information security and Cyber Defense

D. Fourth Year (2010-2011)

The proposal for two sequential one-credit hour courses was modified to be two parallel one credit-hour courses. In the previous version of the class, the instructors provided the functions of the management team and attackers. The event in which the students who attended the competition provided those services to our first and second year students spawned the idea to let students who had take the one credit hour course previously and participated in the competition to act as the RED team. This gives them an additional perspective on security and provides a different motivation. In response to the students request for more structure, different vulnerabilities and the associated defenses would be explored each week. Initially, the RED team would exercise exploits against a particular unsecured vulnerability while the BLUE teams observed the consequences. Then the BLUE team would implement the appropriate security measure and the RED team would try again.

Seven students signed on for the RED team and twelve for the BLUE teams. This class was held on Friday afternoons, the last five weeks of the term. It was impressive that this many students would participate at that time of the week.

The responsibility of the RED team was to learn vulnerabilities and exploits around a particular service each week. They were to submit plans for the session that week in advance of the class. It was felt that since the students were juniors and seniors and had participated in the previous year's events, they would investigate and coordinate attacks. Some reports indicated they wanted more content provided by the instructor. A few local offensive security

ISBN 1-933510-96-X/$15.00

people joined in on the RED team which was a plus to both groups.

Feedback from students on the RED team indicated that they did not have the most effective learning experience. The process needed by the BLUE teams to secure their networks after the attacks on the unsecured service took time, during which the RED team could do nothing. Once secured, there was little the RED team could do against the BLUE team. Also, it was noted that when the activity was reduced to one service vulnerability and no management injects, the intensity diminished.

The BLUE team participants had a better experience. Some of the reflective comments may help provide that student perspective:

"Overall I feel like this is an exciting and engaging course. It is terribly challenging because of the amount of information received over a 5 week period. I think that as this course develops, it will be a very fun class for students, and give a clear demonstration to students in terms of computer security principles."

"Prior to this class I had very little experience with offensive security. We had done some things in software and web security but never a holistic attacking approach."

These parallel classes did provide a preliminary practice environment for the competition the following March. All team members had been involved in one of the groups.

E. Motivation, Engagement

One of the premises of this paper is participation in the cyber defense events and the practice activities contribute to motivation, engagement, and learning. Most of the data presented has been based on the observations of the instructors/coaches. Some student data may help add another perspective. Following is a segment of an email after the most recent competition from a graduating senior who participated for the first time:

"It was truly the most educational and FUN event I've ever experienced! I've never learned so much in such a short period of time" - a senior

Students were asked to contribute their views regarding the impact of these events on learning, motivation and engagement. The questions were sent to the eight students on this year's team and two alumni. Three students responded and excerpts are given below.

Do you feel that participation in the Cyber Defense activates has affected your motivation toward learning about security.

"Yes. Experiencing the competition was a major eye-opener for me. I hadn't really realized how much more there was to security than I had initially thought" – sophomore

"*Yes, I realized how much I did not know."* - alumni

Our observation is that the comprehensive net/sec environment of the Cyber Defense competition and practices is a different learning environment than the traditional classroom, topic-specific lab environment and that it generates learning and motivation for learning in different ways from the other environments.

"Agree 100%. It helps solidify foundation teaching. Combinations various facets of the curriculum into a concise, streamlined hands on activity."- alumni

"This created a completely different environment….. it is a much different way of learning that is much more interesting" - sophomore

"Definitely" - sophomore

IV CONCLUSION

The Computer Network and Information Security major, students, and faculty at Champlain College has benefited immensely from the Cyber Defense competitions. Curriculum has been modified to account for gaps we may not have known about without that experience. Most changes are based on feedback from students that participated and faculty observations. The changes enable the students to not only learn concepts but also apply them in a real-time operational environment. Students see an effect on

ISBN 1-933510-96-X/$15.00

curriculum, infrastructure, and environment based on their experience and some of their suggestions. They feel like they are part of the process. Students learn most effectively when they feel they are part of the process and are the ones setting their learning agenda [8]. This has increased student engagement and motivation. They also become aware of the reasons why all changes cannot be made quickly and that technology curricula evolve at a pace that does not match industry.

Our findings are similar to Conklin [8] and Mullins et al. [6] in the impact on student engagement, motivation, faculty, and the academic program. The former dealt with graduate students and a graduate program while the latter involved military institutions.

The reinforcement of instruction with application helps students understand network system security. Most of the courses that we teach in our major are structured to have lecture and lab components. While students enjoy the lab components, it is difficult to develop real-world environments for all classes. Several more courses now have been moved into a lab environment and hands-on components added.

The one-credit hour Cyber Security course provided an opportunity for the students to get more exposure to hands-on activities that are real-life based. The class provided an opportunity to incorporate lab concepts from many other courses in a systems setting.

We see an increase in motivation and engagement from students entering into the program. Many hope they can be part of this experience and would like to become knowledgeable in Security concepts. During our open houses, prospective students and parents are told about the competition and how it has helped both the students and the program. Many of the prospective students like the idea and look forward to enrolling in Champlain College and hopefully make the team.

V. REFERENCES

[1] Du, W., Jayaraman, K., Gaubatz, N, (2010). Enhancing Security Education with Hands-On Laboratory Exercises. 5th Annual Symposium on Information Assurance (ASIA '10). Syracuse, NY.

[2] Bogolea, B. and Wijekumar, K., (2004). Information Security Curriculum Creation: A Case Study**.** Proceeding of the 1st annual conference on information technology curriculum on Information **s**ecurity curriculum development, ACM

[3] Azadegan, S., O'Leary M., Wijesinha, A., Zimand, M. (2006). Undergraduate Computer Security Education: A Report on our Experiences & Learning. Proceedings of Seventh Workshop on Education in Computer Security (WECS 7), 4-6 January 2006, Monterey, California

[4] Locasto, M., Sinclair, S. (2009). An Experience Report on Undergraduate Cyber-Security Education and Outreach. The Second Annual Conference on Education in Information Security (ACEIS 2009). February 2009. Ames, IA, US

[5] Rochester Institute of Technology, 2008 <http://neccdc09.nssa.rit.edu/node/10>

[6] Mullins, B.E., Lacey, T.H., Mills, R.F. (2007). 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 2007.

[7] Bransford, J., Brown, A., & Cocking, A. (Eds.). (1999). *How people learn: Brain, mind, experience, and school* (Report of the National Research Council). Washington, DC: National Academy Press

[8] Conklin, A (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. HICSS '06 Proceedings of the 39th Annual Hawaii International Conference on System Sciences.