CYBER DEFENSE COMPETITION: A TALE OF TWO TEAMS*

Yan Bei and Robert Kesterson
Institute of Technology
University of Washington, Tacoma
Tacoma, WA
253-692-5863
yanb@u.washington.edu

Kyle Gwinnup and Carol Taylor
Computer Science Department
Eastern Washington University
Cheney, WA 99004
509-359-6908
ctaylor@ewu.edu

ABSTRACT

Collegiate Cyber Defense Competitions have recently grown in popularity as a means of providing real-world experiences to students learning computer security at the college level. Preparation and training for these competitions focuses students on essential skills needed to defend networks against real threats and better prepares them for the problems and conditions they may encounter outside the protection of university run labs. This paper highlights the benefits of Cyber Defense Competitions and documents the experiences of two teams that trained and competed in the Northwest regional cyber defense competition. Both teams benefited from participating in the competition with students expressing positive learning experiences. Recommendations for other schools that may be interested in competing or setting up in-house cyber defense exercises will be presented.

1. INTRODUCTION

In the age of global connectivity, computer security is one of the most important topics taught within college computer science departments. As information breeches have increased in number and severity, with almost daily reports of compromised and stolen social security and credit card numbers [15] , there is recognition by CS educators that computer security skills are needed by future generations of IT professionals. This recognition of the importance of computer security education by industry, government and academia has resulted in security education being offered as part of many CS or IS degree programs. Growth of the recognized importance of computer security skills can

be quantified as a steady increase in schools becoming Centers of Academic Excellence in information assurance [9].

For all the interest in computer security education, the question remains, however, how best to teach computer security fundamentals and make it relevant to CS students. Traditional methods for teaching computer security topics are similar to methods of CS instruction: lecture with practice labs [7]. These traditional methods work well for learning general topics such as cryptography, access control policies or secure coding. Practicing concepts learned in lecture is typically done with hands-on exercises such as practicums and labs. However, because the nature of computer security involves both attack and defense mechanisms, creating exercises that provide realistic experiences can be challenging for most instructors.

Over the last few years cyber defense competitions are a recent developments that seems to foster real-world experiences for computer security students. The benefits of these competitions have been documented by others [2, 3, 11] which includes gaining insight into real-life attack and defense situations, pinpointing holes in instructional content, practicing collaboration within a team and learning how to accomplish tasks for management.

This paper documents the experiences of Eastern Washington University (EWU) and the University of Washington Tacoma in developing cyber defense student teams and competing in a recent 2011 Northwestern Cyber Defense competition, PRCCDC [10]. Training for each team will be documented. Schools currently teaching cyber security can benefit from our experiences and competition preparation.

2. CYBER DEFENSE COMPETITIONS

Competition has long been used to generate interest in learning and has become an accepted practice within most academic environments. Some of the more popular CS competitions include robotics, programming competitions and autonomous vehicle competition [6, 1, 15]. Within the area of computer security, competitions at Defcon, the popular hacker convention, have included capture the flag, wardriving (locating wireless access points) and recently social engineering where hacking people is the goal [4].

The benefits of competition within education have been well documented. Students enjoy preparation and participation in competitions and generally become more interested in topics related to the competition [5, 6, 13]. Aside from creating interest and generating enthusiasm from students, competitions allow students to integrate learning from classes and labs as they are required to solve problems outside of the classroom [11].

2.1 History of Cyber Defense Competitions

Cyber Defense Competitions date back to the US military academies first test of their students in 2001, the Cyber Defense Exercise (CDX). The purpose of this early exercise was to test students ability to both build and defend a military network from attackers trying to breech security. The Air Force, Army, Coast Guard, Navy and Merchant Marines participated in that first competition [2].

Recognition of the benefits from preparing and training military students as defenders, led a group of government and academic security educators to create a similar competition for non-military schools. The stated goal of the non-military competition was to provide more real--world experiences for students in information assurance. The first Collegiate Cyber Defense Competition (CCDC) was hosted by the Center for Infrastructure Assurance and Security at the University of Texas, San Antonio in April 2005 [3]. Following this first competition, other regions quickly became interested and started their own regional competitions. Currently, six regions participate including the Southeast, Mid-Atlantic, Midwest, Northeast, Northwest and West. Winners of these regional competitions attend the Nationals CCDC held each year at University of Texas, San Antonio.

The Northwestern CDCC, the Pacific Rim Regional Collegiate Cyber Defense Competition, was first held in 2008 at the Microsft on-site campus in Redmond, WA [10]. The competition takes place over a two-day period on a weekend and has since been held annually at Highline Community College near Seattle. About eight teams compete from both four year and two year schools. From the beginning there has been active sponsorship from large industry organizations such as Microsoft, Boeing and Cisco.

2.2 Structure of the CDCC

Each CDCC is set up so that each student team is assigned to a network that must be defended and secured. Typically there is a scenario that something happened to the IT staff of the network and the new "team" must take over and figure out the state of the network left by the departed network staff. Student teams have a grace period of a few hours to take inventory of their networks and try to secure and patch the equipment.

After the grace period, outside "attackers" can attack their networks. This threat to the network is in the form of a red team of would-be hackers trying to penetrate the network. Attacks are run against all of the teams and if successful, further attacks are leveraged against the penetrated systems.

There is also a white team of industry professionals who act as judges and monitor the network to verify services are operational plus score the teams on completion of business tasks throughout the competition. In addition to maintaining the network in an operational state in the face of attempted breeches by the red team, students must implement tasks from management. These tasks known as business injects take the form of adding users, starting or stopping services such as email or web plus producing reports. These tasks contribute to the overall score of the teams and provide some of the real-world flavor for the students as they try to maintain network functionality in the face of sometimes unreasonable demands by management.

Scoring is based on keeping required services up, preventing security breeches and completing the business injects throughout the two-day competition. The team with the most points wins and goes on to compete at the National CDCC.

3. UNIVERSITY OF WASHINGTON TACOMA

University of Washington at Tacoma has an active cyber security program and teaches courses in general and network security. The team from the University of Washington, Tacoma has competed in all four PRCCDC competitions under the direction of Dr. Yan Bei.

3.1 Current Training Strategy

Training for the CDCC consisted of focusing on five key skill areas that the team believed were critical in defending systems against cyber attacks. These skill areas consisted of:

1. Applying patches to operating systems
2. Using router tables to enforce white lists of acceptable IP addresses
3. Input sanitation for MySQL server
4. Restarting non-running network services
5. Running external penetration tests for up network services

The strategy of the Tacoma team consisted of everyone practicing and learning certain general security skills such as patching, restarting services and penetration testing but assigning more specialized skills to certain team members with those skill sets. Practices and training for these areas are detailed below.

In applying security patches, discussions about how to break patches into smaller pieces and store them on external drives was discussed and practiced. The strategy for restarting non-running services was to take snapshots of the network upon arrival and at later points when the network appeared to be stable. That way, the network could be re-installed quickly back to a known good state if compromised during the competition. The entire team learned how to perform snapshots of the system. External penetration testing was practiced in group sessions that detailed network auditing. Topics covered included many tools on the popular Backtrack system auditing CD such as Nmap, Nessus and several other tools. Students were encouraged to practice with these scanning tools to determine open ports and vulnerable services running on those ports. Team members were supposed to use the tools at home on their own systems.

Creating white lists for routing tables were designated as a specialized skill and handed to a team member skilled in CISCO routers. Input sanitation for MySQL servers was also considered more of a specialty and was assigned to a team member skilled in MySQL Server coding.

3.2 Training for Future Competitions

Overall, the team felt comfortable with their ability to patch Operating Systems. The input sanitation for an accessible web database like MySQL or LAMP is not a trivial skill and it was felt that team members will need to specifically train for this. Similarly, with creating lists for CISCO routers, special skills are needed and will be assigned to team members with those skills.

One area of improvement would be for the team to know how to implement the open source SNORT Intrusion Detection System [12] and dedicate an entire machine and team

member to running SNORT. This would enable the team to determine the type of traffic on the competition network and diagnose and fix problems during the competition.

4. EASTERN WASHINGTON UNIVERSITY (EWU)

The team from EWU has competed in three out of four PRCCD competitions. Computer security education at EWU includes courses in general and network security and secure coding. The current year 2011 is the first year the team dedicated significant time to training for the competition. Student team members assisted with training fellow team-mates and determining the content of the training sessions.

4.1 Current Training Strategy

EWU's Cyber Defense team practiced security theory and application over a ten week period leading up to the competition. All participants met every Friday for approximately two hours as a group. Several students competed the year before and provided insight for training that better reflected the competition. The training was decided to be a bottom up approach in terms of the ISO network model. The goal was to ensure all team members were comfortable with each layer before moving on to the next layer. Team members had a wide range of network and security experience. One limitation for the team was a lack of real equipment for layer two activities and an overall lack of a true multi-server network which would aid in showing a sample network and real network traffic.

Network specific administration and vulnerabilities were addressed first to ensure all students could grasp network communication for many platforms. For example, good practice to separate subnets of departments and more importantly to subnet servers from your users was covered. This was used to illustrate IP communication and how a firewall could protect your servers in a sub-netted network as oppose to everything on a single subnet. This knowledge proved helpful in the competition for our network roles.

After getting through basic networking setting up and configuring Windows Servers was practiced. Students were introduced to Active Directory, DNS, WINS, and other Windows Server specific services and tools. All computers in the practice lab are Pentium class single core processors which was a minor problem for building our virtual networks. All installations and configurations of servers were done from within virtual machines. One lab had students set up a Windows Server as the domain controller and configure several services such as AD, DHCP and DNS. Students were then instructed to create users and add a Windows XP machine to the domain and log into a domain account.

Once networking and systems were covered a small homework assignment was given to set up a small virtual network at home and play around with different configurations and settings to gain a better understanding. Students were encouraged to come in with questions. The focus was then moved to specific tools used in the administration and security industry. Proxies, traffic monitoring, administration scripting and client configurations were covered. Traffic monitoring tools were discussed. All students needed to be very comfortable with Wireshark, Snort and Squid proxy. Labs for each of these tools plus setting up and configuring snort were provided.

4.2 Training for Future Competitions

Overall, most topics could've used more discussion and practice but the concern was to first cover everything that pertained to the experience from the year before. Training next year will put even more focus on the virtual environment and ensure each team member has experience in every role instead of only one or two students responsible for a role. This will allow the team more flexibility in completing the business injects. Practicing writing the business injects will also be a future focus since completing a business class memo or document is necessary for good marks when turning documents into the white team.

5. BENEFITS OF CYBER DEFENSE COMPETITIONS

The benefits of a competition such as PRCCDC provides students with a learning environment beyond that of either the classroom or lab. Within the framework of the competition, they must deal with unexpected situations and find solutions to problems they have never encountered before. These experiences are invaluable learning opportunities for both students, who get to test their cyber security and system administration knowledge and instructors who can test the adequacy of their security curriculum.

Another benefit is the opportunity to work in teams. Within the typical CS curriculum, CS students mostly work individually on projects. Yet, in work environments, teamwork is more common especially in network management where coordinated effort is the norm.

One other positive aspect of the PRCCDC was the real-world exposure to having to please bosses who might be technically ignorant of the consequences of their requests. Thus, students had the opportunity to interact with simulated managers within the context of the competition.

6. CONCLUSION AND RECOMMENDATIONS

Overall, competing in the PRCCDC competition has been extremely beneficial to the teams from both EWU and the University of Washington Tacoma. Students have benefited from the competition by getting a taste of real-world cyber attacks and learning the skills necessary to defend against them. Both students and instructors have a better idea of where they can improve in terms of security curriculum.

A recommendation for other schools seeking to improve their security programs would be to set up a practice competition similar to the regional competitions in order to foster interest from students. At the very least, students could be divided into groups of attack and defense teams to practice skills related to maintaining a network under real-world conditions. There are numerous resources created for practicing and learning how to set up learning environments [8, 13]

7. REFERENCES

[1] ACM Intercollegiate Programming Competition, 2011, http://en.wikipedia.org/wiki/ACM_International_Collegiate_Programming_Contest, retrieved March 25, 2011.

[2] Carlin, A. et al, Developing Cyber Defenders of Tomorrow with Regional Collegiate Cyber Defense Competitions, *ISEDJ*, 8 (14), 2010.

[3] Conklin, A., Use of Collegiate Cyber Defense Competition in Information Security Education, *Information Security Curriculum Conference*, 2005.

[4] Defcon, 2011, http://www.defcon.com/, retrieved Feb 14, 2011.

[5] Lawrence, R., Teaching Data Structures Using Competitive Games, *IEEE Transactions on Education*, 47 (4), 2004.

[6] Mansaur, R., Hardware Competition in Engineering Education, *IEEE 30th ASEE/IEEE Frontiers in Education Conference*, 2000.

[7] Micco, M., Rossman, H., Building a cyberwar lab: lessons learned: teaching cybersecurity principles to undergraduates, *SIGCSE '02 Proceedings of the 33rd SIGCSE technical symposium on Computer science education*, http://www.ise.gmu.edu/~duminda/classes/spring02/p23-micco.pdf, 2002.

[8] National CCDC, Team Preparation, 2011, http://www.nationalccdc.org/files/CCDC%20Team%20Prep%20Guide.pdf, retrieved Feb 11, 2011.

[9] NSA, Centers for Academic Excellence in Information Assurance Education, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml, 2011.

[10] PRCCDC, http://ciac.ischool.washington.edu/?page_id=244, 2011.

[11] Schweitzer, D., Gibson, D., Collins, M., Active Learning in the Security Classroom, *Hawaii International Conference on System Sciences*, 2009.

[12] Snort, http://www.snort.org/, 2011.

[13] Tenable Security, Resources for Team Preparation, 2011, http://blog.tenablesecurity.com/2011/03/mid-atlantic-ccdc-lessons-learned-in-communication.htm, retrieved March 3, 2011.

[14] Virginia Tech VT Team, 2011, http://www.avt.me.vt.edu/, retrieved March 4, 2011.

[15] Widman, J., 10 Massive Security Breeches, 2011, http://www.informationweek.com/news/security/attacks/229300675, retrieved March 5, 2011.