Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

# Instruction, Exercise, Competition and Certification: The Cyber Defense Training Continuum

Duke Ayers, VP, Program Manager, CyberNEXS Global Services, MBA, CISSP, HISP

***Abstract – Training students in cyber defense requires an educational model that includes instruction, exercise, competition and certification. To be qualified, the student will need to not only understand the techniques and technology of cyber defense, but also be tested in a live environment, under stressful conditions, in their ability to maintain critical services, while thwarting real-world attacks. As the educator preparing this individual, what curriculum, tools and technologies are required to train and challenge your students from basic instruction through certification?***

## I. Introduction

There are many issues that prevent most high schools from training and exercising their students in computer science. This is especially true in the cyber defense skills that are essential to personal safe computing, as well as preparing students to meet critical positions in our work force. What needs to be answered is what training curriculum, tools and technology are required to effectively train students beyond simple retention of learned facts. Those facts must become real knowledge through practical exercise that reinforces their understanding through trial-and-error.

Additionally, it has been our experience that the students find competition exciting and stimulates their desire to learn more as a result. As a final gate in the educational process, we believe that certification is also necessary to document the student's ability to effectively apply what they have learned in a real-world situation. Figure 1 depicts that training continuum of instruction, exercise, competition and certification, which, once certified at one level, begins the continuum anew until achieving the next level of competency.


Figure 1. Continuum of Cyber Defense Training.

## II. Classroom Instruction

Classroom instruction starts the continuum primarily through lectures and reading assignments. This is when the student adds new information to their personal knowledge base with which they will continue the educational growing process. During classroom instruction, questions are raised to better understand concepts and details. The instructor might use the cyber training environment to demonstrate principles presented in class. This instruction may also be in the form of policies, procedures, technical details and anecdotes, but all are fuel for the actual experimentation that follows next.

## III. Live Exercise

Armed with this instruction, the student needs to reinforce their understanding of this information through trial-and-error exercises; this is when the information becomes personal and is permanently registered with context in their knowledge base. They need to put their hands on the keyboard, and through the computer interface, see the consequences of the actions they take. They should be expected to identify and remove vulnerabilities, while maintaining critical services and reporting, even when under attack. (see Reference [1] for more information on Cyber Defense Training.) We have found that as young as 8th grade middle school children can comprehend cyber security principles and can effectively apply them during competition as observed during the San Diego Mayor's Cyber Cup (Reference [2] applies).

To be meaningful, their actions must receive immediate feedback in the form of real performance numbers that will measure the success of their actions. Additionally, immediate feedback has the added benefit for the instructor, who, recognizing where the students are less capable, is then able to focus training in those weak areas.

When you have a controlled training environment in which you can take any action as part of your trial-and-error process, you empower the student to use standard techniques, as well as their own creativity, to solve problems. The outcome is a richer learning experience.

An important element of live exercise is that it must be provided routinely. This will permit the iterative process of learning through instruction and understanding,

ISBN 1-933510-99-4 

followed by reinforcement through exercise. This knowledge cycle readies them to once again be open to more information through subsequent instruction. In working with the high school students, we have observed this phenomenon. Few of the 25,000 U.S. high schools have any formal computer science programs. When we have provided the students with some basic training prior to the exercise, it is amazing how much they are able to apply during the exercise and retain thereafter. We also observed that from the competition experience, the students are instilled with a refreshed sense of wanting to learn more. "The kids were still pumped up on Monday after the competition. In fact, they used their 'newfound' knowledge and crashed the server they had set up to practice on!" (Greg Volger, educator)

At the end of the exercise, to fully reinforce this knowledge, the students should be presented with graphical representations of "what they said was happening, what actions they took, and in fact, what was the reality of the situation." The feedback should show how well they maintained critical services, while both removing vulnerabilities and thwarting hacker attacks. There should be log information that also shows their communications to the white team (control cell and acting trouble desk). Figure 2 depicts the key cyber defense skills that all system administrators and security professionals should possess.


Figure 2. Key Cyber Defense Skills.

This is the tall pole in the education tent, as there are few educational institutions that are adequately prepared to provide this live, real-time feedback environment, one that quantifies performance in the key skill areas on a minute-by-minute basis.

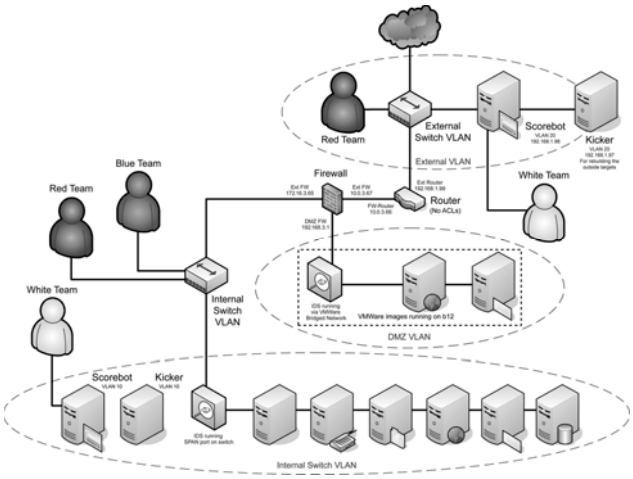


Figure 3. Live, Realistic Cyber Defense Environment.

It requires a dedicated training system depicted by Figure 3 above. It is comprised of real Information Technology (IT) systems, including Windows® (Microsoft Corporation) and Linux® (Linus Torvalds) operating systems, switches and routers, intrusion detection devices (IDS) and firewalls. These systems must be highly reconfigurable, easy to use and quickly reconstituted in the event of a crashed system. There must also be that scoring system that quantifies key cyber defense skills on a minute-by-minute basis.

## IV. The Value of Competition

Competition is the way we measure the individual, or team, against another; or, we can simply measure our own performance versus the environment. Whatever the goal of the game, the experience is exciting, challenging and an excellent way to learn. Typical teenagers can figure out and start winning most video games through simple trial-and-error.

Competitions, like exercises, should become a matter of routine, so that the lessons learned, whether self-realized, or through observation of an opponent, can be used during subsequent engagements and the power of learning is continually reinforced.

Another benefit of both exercises and competitions is that students learn to work as a team. In the competitions we run, one of the signs of success is that the best teams communicate a lot of information. As one member notices a particular condition, or a successful action taken, they relay that to the others so that they may also see if this advice may help them improve their systems. To act as a team, they must also demonstrate basic organizational skills, such as leadership, sharing, evaluation of information, and organizing themselves to most effectively deal with the game problems. Figure 4 depicts one team's method for ensuring that they follow a

prescribed set of actions to ensure they have employed best practices.

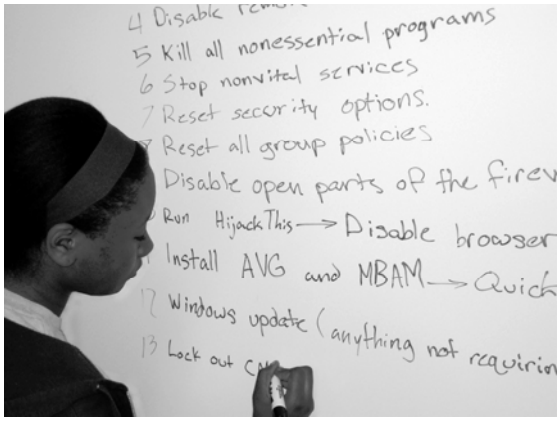

Figure 4. Learning Organizational Skills.

Students not only learn how to do things, but they also learn while under pressure. Normally, we would provide a period of time to allow acclimation to the exercise environment and to begin fixing vulnerabilities that we have pre-configured into the targets (Windows and UNIX® systems). At the prescribed time, we begin to launch a series of scripted exploits. (Note: The same exploits are always launched at the same exercise time for all contestants to ensure fairness.)

Another benefit of competition is the level of enthusiasm generated. During the event, the students furiously apply whatever knowledge they possess, as they want to do well for themselves and their teammates. When the moment arrives to announce the winner, there is a huge response, especially at the high school level. During the first National high school Cyber Defense competition in Orlando, February 2009, the winning team was hugging and high-fiving each other; it was quite an experience! During the second year of qualification rounds, we ran a test exercise to make sure the new technology was ready to deliver Internet-based competitions. In Figure 5 you can see a picture that was sent to us right after this team successfully completed the exercise. Behind them is the projection of their status, which shows that they fixed 100 percent of the vulnerabilities. In fact, this team did amazingly well, completing the exercise in less than two hours; the remaining three teams never did complete the exercise in six. I'll bet you can't tell that they were energized!


Figure 5. Students Celebrate.

Whether winner or loser, the game stimulates the students to want to further pursue learning so that they may better perform the next time they get a chance to compete. When presented as an on-screen video game, the learning medium captures their attention.

## V. Modernizing Competitions

Conducting competitions have historically been large, costly logistics nightmares of assembling large number of systems, configuring them for the function they will perform, and shipping equipment to the central location where all the contestants will travel to for the competition. This can be a very costly venture, and is typically relegated to once a year. This model is not efficient, neither in terms of labor required nor dollars to fund all activities. It also means that this competition environment is not routinely available for the iterative process of the cyber defense training continuum. We believe there is a better model.

Virtualization and remote connectivity are changing the way we operate. Using hypervisor technology and virtual machines, a single server can now run multiple operating system machines. The benefit is that the images can be configured with the requisite services, pre-configured vulnerabilities and level of complexity required for the game. They can be reused from one game to another, or quickly reconstituted in the same game if a student damages their copy. Virtualization reduces the number of physical machines required and therefore the cost and logistics to run a game.

Remote connectivity, through a client-server model and a virtual global cyber defense service as shown in Figure 6, also reduces cost, and therefore allows more routine conduct of competitions.

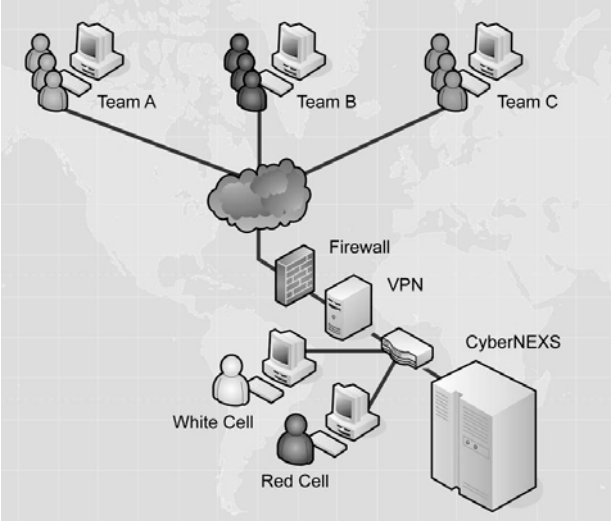

Figure 6. Virtual Global Cyber Defense Service.

We developed two forms of remote games that can scale and provide the degree of complexity required for most competitions:

**1. Distributed Game** is typically used when there is a large number of people/teams competing, such as in practice or qualification rounds. By pushing most of the computer processing out to the contestants' computers, we are able to run hundreds of simultaneous connections into the central scoring system (ScoreBot). To execute this game model, the contestants download a misconfigured VMware® image from a central server, add a few small pieces of communication software to their computer, and they are ready to participate in a remote game. At the start of the competition, the students download a password that is used to unlock the contents of the image. Once unlocked, the image connects into the ScoreBot, registers their system, and starts receiving a HTML page displaying their status. We have successfully run this model of game as part of our STEM outreach. During AFA Cyber Patriot II competition series, the first qualification round included 150 schools participating simultaneously over the Internet, across the nation. We were pleasantly surprised by the results of the last qualification round (medalist round). Thirty-four schools, from 20 different states, competed by removing vulnerabilities from two Windows and one UNIX target during a six-hour period. Of the 34 schools, every one was actively working at least one VM target; 70 percent were working all three. Ninety-two percent of the VM images had positive scores and the average score of all the teams was 56 percent. The top eight teams, from seven different states, maintained an overall average of 75 percent across all three targets. Figure 7 depicts the demographics of the competition.

Figure 7. CP II Medalist Round.

**2. Centralized Game** is typically used after the qualification rounds have narrowed the field and there are only a few best-of-the-best contestants. The centralized game will exercise and score all of the key cyber defense skills: ability to maintain critical services, harden systems, thwart attackers and communicate to report status and seek assistance. This model provides contestants with their own complete cyber defense live environment, including Windows and UNIX operating systems, switches and router, firewalls and intrusion detection devices. All computer processing is contained within the central service, thereby preventing any hacker exploits from exiting to the Internet and causing problems. To compete requires a few freeware programs and minimal Internet connectivity as noted in Section VIII above.

At the start of the competition, the contestants will log in to this centralized competition environment, assume control of their "Blue" (exercise) systems, and begin to harden them as quickly as possible. Sometime later, the "Red" team (hackers) will begin to attack their systems. During all of this activity, contestants are expected to submit trouble tickets to request support (i.e., load patch, etc.) and to report status.

## VI. CERTIFICATION

Certification is the next logical step. Once the student has demonstrated a satisfactory base of knowledge through written and practical exams, and has gained sufficient real-world experience through competition, they are ready to demonstrate their individual level of competency. Certification standards for cyber defense have not yet been codified, and would need to be tailored to each level of education. Suffice it to say that this final exam would test the same skills that we have been reinforcing during the continuum. Whether a professional certification listed on a resume, or simply a final exam, the certification documents the final step in demonstrating a certain level of proficiency.

As with the competitions, there are two modes that can be used to test the individual. There is the less complex level of remediating vulnerabilities and maintaining critical services using the distributed game; the more complex game, exercising all of the skills while under attack, can test the more seasoned candidate. The benefit of the former certification mode is that it can be done without human interaction by the certification service. The candidate simply downloads the VMware image, takes the exam during a prescribed period of time, after which the automatic scoring system provides a numeric value. The individual is therefore certified if they achieve the passing score.

To increase the level of complexity, the centralized game can be used. That would more of the cyber defense skills. The downside to this mode is that it requires at least one individual to act as both white and red teams. This requires significantly more interaction and resources, and therefore cost, but the results provide a complete insight into the individual's ability to perform each of the cyber defense skills.

## VII. Cyber Defense Environment

To provide for this continuum requires a dedicated cyber defense-training environment (Figure 3 above refers) that has the following characteristics:

- Self-contained, live IT environment in which students can freely use trial-and-error without fear of making a mistake. It must also be properly secured with a trusted gateway that allows students access, without permitting exploits or otherwise unintended traffic from exiting into the Internet. This environment must be available anywhere, anytime, so that it can service the broadest user group, and reduce cost through its virtual accessibility.
- An automated scoring system should track the security health of the network by measuring the student's ability to perform key cyber defense skills as noted in Figure [2] above. Of great importance, is that the scoring system must be automated to provide real-time feedback; if not, the moment of learning is lost. The scoring system should maintain a database of system status while providing a standard network management view for students. It should also provide a special view for instructors to keep the game-play on track and enable them to focus training based on real-time results. The scoring system will drive various graphical displays that assist both the instructor, as well as the student, in understanding how well they are progressing on a minute-by-minute basis that Figure 8 depicts. At the end of the exercise, these displays present all of the results in a meaningful way and thereby create the "Aha!" moment for the students.

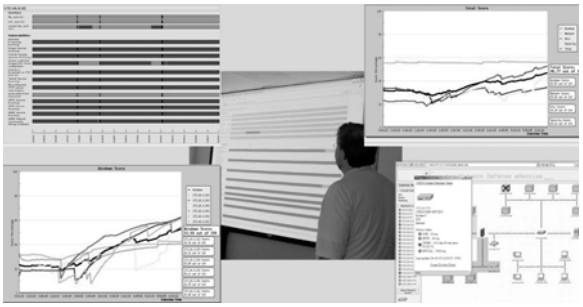

Figure 8. Example Cyber Defense Feedback Displays.

- **Exploit Injector Tool**. A semi-automated exploit injection tool should allow the user to select which vulnerabilities they wish to use for a given session. With each inject, there is a time and IP address against which the exploit will be launched. This point-and-click mechanism has several benefits: (1) simplifies the job of Red Team, thereby reducing resource requirements; and, (2) ensures fairness for all competitors in a single game, or across multiple games. The exploit scripts are continuously updated as new threats emerge.
- **Target Provisioning System**. The VMware images are comprised of different operating systems and service functions, such as: Web, email, database, and file servers, as well as workstations and network-based intrusion detection systems. To accommodate the many exercises, competitions and certification activities, a library of VMware images will be compiled. Management and provisioning of these many images can become a real headache without a semi-automated system that indexes the images, and can be programmed to provision a cyber defense environment with specific images at a prescribed time.
- **Session Scheduler**. As this cyber defense training environment is centralized, it can be used by several organizations, and therefore a cost savings is realized. Using the same hardware, the scheduler will provide login credentials to the intended user at the intended time. At the conclusion of that session, the scheduler must also reset the environment so that it is ready to be provisioned for the next user.

All of these tools are essential to the success of this cyber defense environment. If the system is not easy to use, then it will require specialists to run. This will not only drive up the cost, but keep the system from scaling to meet the needs of the U.S. educational system. These tools must

empower the local educator to deliver and score their own curriculum, which in turn, will make it affordable to the 25,000 high schools across the nation.

## VIII. Student Requirements

Here are the minimum requirements for the students' competition systems:

**Hardware Requirements**

- 1 Ghz Intel compatible processor (AMD processors have had issues with VMware and are not recommended)
- 2 GB RAM
- 15 GB of free disk space
- Keyboard and mouse
- Network connection
- 1024x768 or higher display
- (Optional) It is recommended to use a projector or large display to share the screen output with the rest of the team, but not required.

**Software Requirements**

- Operating System (Windows 2000 or newer, recent VMware supported Linux, or Macintosh 10.4.11 or later)
- Web Browser
- ZIP client capable of handling encrypted ZIP files
- VMware Player (for Windows or Linux) or VMware Fusion (for Macintosh)

**Connectivity Requirements**

- 256K upload/download speeds per connection

As you can see, the requirements are easily met by most computers that you would buy in computer discount stores today, as well as internet connections that are commonplace in many US homes.

## IX. Author Experience

To put this paper in perspective, I think it is worth providing our experience with the cyber defense-training continuum. Science Applications International Corporation (SAIC) has developed a cyber defense system over the last seven years, which we have used in over 50 cyber defense training and competition engagements. We have conducted remote exercises for several state collegiate and high school competitions. We are also heavily involved in using this capability to provide in-kind support to science, technology, engineering and mathematics (STEM) initiatives throughout the United States, which are intended to excite, attract and retain students in technical degree programs.

SAIC is a founding partner in the Air Force Association (AFA) National high school Cyber Defense Competitions called Cyber Patriot, which completed the second year of competitions discussed earlier. Also, in 2008, the University of California San Diego (UCSD) and SAIC teamed to bring San Diego high school students to the SAIC campus to receive training and experience a cyber defense competition. Figure 9 shows one of the 2008 competition teams.

Figure 9. Students during 2008 San Diego Competition.

Based on that success, we have once again teamed with UCSD to establish an annual event called the San Diego Mayor's Cyber Cup, which includes multiple rounds of competition.

## X. Summary

For cyber defense training to be effective, it requires a system that is realistic, delivers real-time feedback and can be made routinely available. Without this comprehensive system, schools may not be able to provide for the continuum of cyber defense training. We need to take students beyond the simple learning of facts; we need them to routinely practice their instruction in a hands-on environment and demonstrate their ability to perform the key cyber defense skills. With the right cyber defense trainer and series of lectures and exercises, capped by competitions and certification, we will excite and prepare students as they successfully progress through the continuum of cyber defense training.

## XI. REFERENCES

[1] Strengthening the Weakest Link: Organizational Cyber-Defense Team Training, by Duke Ayers, presented at CISSE 2009
[2] Air Force Association (AFA) National High School Cyber Defense Competition (called Cyber Patriot) September 2009 – February 2010
[3] San Diego Mayor's Cyber Cup February – March 2010
[4] Developing a National High School Cyber Defense Competition, by Dr. Gregory B. White, Dwayne Williams, and Keith Harrison, Center for Infrastructure Assurance and Security (CIAS) at the University of Texas San Antonio (UTSA), presented at CISSE 2010

---