Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

# The Collegiate Cyber Defense Competition$^{tm}$

Gregory B. White, Ph.D., Dwayne Williams, Center for Infrastructure Assurance and Security

***Abstract – In 2004, a workshop was held in San Antonio, TX to discuss the possibility of establishing a national collegiate cyber security competition. Academicians and students from across the nation were invited to discuss the possibility and to share their ideas on how such a competition should be conducted. A report was generated later that year detailing the recommendations from that workshop. Several of the participants from Texas schools agreed at the competition to develop a regional competition and to conduct it the next academic year. This paper discusses the resulting Collegiate Cyber Defense Competition$^{tm}$.***

**Index terms – Exercises, cyber competitions, collegiate, cyber defense**

## I. Introduction

Competition is not new to either the collegiate or cyber realms. Colleges have a rich tradition of conducting competitions in a variety of activities ranging from athletic sporting events, to dance, chess, bridge building, and even robotics. Rich rivalries have been created between institutions and tremendous amounts of money are donated annually by alumni supporting the teams of their choice.

This desire to compete has not been ignored in the cyber world. “Capture the flag” and “attack-defend” competitions have been held at various venues for the last decade. Several universities use internal competitions in classes to provide an element of excitement to courses on computer and network security. The service academies have progressed even further in this area as they have conducted inter-school competitions for several years. Known as the Cyber Defense Exercise (CDX), the inter-service academy competition served as the initial model around which discussions of a possible national cyber security competition revolved. [1] A key premise of this competition was the emphasis placed on defending networks, not attacking them.

Whether to allow offensive actions by competitors is often a point of debate in organizing competitions. Many argue that the best way to learn how to defend against attacks is to actually learn how to attack systems. Others argue that this, in essence, is akin to “hacker training” and suggest that institutions may open themselves up for legal action if students later use knowledge they gained during the competition to break into industry or government systems. Another argument against allowing offensive activities by competitors is that the emphasis on defensive activities encourages and promotes a defensive mindset which is arguably what the competitors will require upon graduation.

## II. The Cyber Defense Exercise (CDX)

The first Cyber Defense Exercise (CDX) was created in 2001 to serve as the capstone course in the information assurance program at the United States Military Academy. [2] All five of the service academies now participate in this event that pits offensive Red Teams from the Department of Defense against cadet teams from each of the service academies. The emphasis of the event is on being able to maintain an operational network in the face of a hostile force attempting to breach the security of the network. Each team is required to design, implement, and maintain an operational network consisting of a variety of platforms. In an attempt to have a level playing field between the teams, security software is limited to open source freely available tools.

There are three major categories of teams involved in the competition. Each of the service academies (along with the Naval Postgraduate School and the Air Force Institute of Technology which are not eligible for the trophy awarded to the winner) fields a Blue Team which develops, operates, and defends their own networks. The DoD supplies the offensive Red Team consisting of personnel from the National Security Agency, the Air Force’s 92nd Aggressor Squadron, and the Army’s 1st Information Operations Command. The final category of team that participates is a White Team consisting primarily of individuals from Carnegie Mellon University. The purpose of the White Team is to initially establish the scenarios and scoring criteria used in the competition and then serve as referee for the competition.

The service academies support the concept of a cyber defense exercise for several reasons. As well as serving as a capstone event used to evaluate the students’

*Gregory White serves as the Interim Director for the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio. Dwayne Williams is an Assistant Director at the CIAS.*

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE

knowledge of information assurance concepts and their ability to protect computer systems and networks, the competition also provides leadership opportunities for the team members. The cadets are responsible for planning, deploying their own teams, and executing the competition. [3] The competition has proven to be very popular with both the cadets and instructors alike. The competitors have walked away gaining not only a better understanding of what it takes to secure a network while keeping it operational but also have enhanced their leadership training and learned the value of teamwork in an environment normally not considered a competitive arena.

## III. The National Cyber Security Exercise Workshop

In the Spring of 2004, a group of educators, students, and government and industry representatives met in San Antonio, Texas, to discuss the possibility of establishing regular collegiate cyber security competitions. The goal or purpose of a cyber security competition[1] as discussed at the workshop illustrates the desires of all those who participated. The overarching purpose was defined as: [1]

> To provide a venue for practical education in the implementation of all strategies, tools, techniques, and best practices employed to protect the confidentiality, integrity, authenticity, and availability of designated information and information services.

In this statement can be seen the real goal which is to help prepare students to better defend computer systems and networks. With this common purpose in mind, the participants set about to define the goals for the workshop which included: [1]

1. Providing a template from which any educational institution can develop and conduct a cyber security competition.
2. Providing enough structure to allow for competition among schools, regardless of size or resources
3. Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance

One of the major desires of the workshop was to create a uniform structure that would be applicable and repeatable at as many institutions as possible. The group also identified concerns that might become an issue when developing or conducting a competition. These concerns included whether to limit participation to post-secondary students, creating a level playing field to eliminate possible advantages due to hardware and bandwidth differences, having a clear set of rules, implementing a fair and impartial scoring system, and addressing possible legal concerns [1]. While the workshop did not result in an agreed upon set of guidelines for a national competition, the participants did agree upon the general framework from which further discussion could be launched. The workshop was adjourned with the agreement that committees would be formed to address the various aspects of establishing a national competition.

When initial planning on the first Southwestern Regional Collegiate Cyber Defense Competition (CCDC) began, the CIAS formed an initial steering and planning group consisting of representatives from the CIAS, the University of Texas at Austin, and Texas A&M University. While designing the CCDC, the steering and planning group attempted to address or incorporate the goals and concerns outlined during the San Antonio workshop.

## IV. Other Collegiate Cyber Security Competitions

While the competition between the service academies has received the most publicity and is probably the best known cyber security competition, it is certainly not the only one held at the collegiate level. Giovanni Vigna at the University of California at Santa Barbara decided to use an exercise (competition) with two teams in his course on network security to help provide the students with a better understanding of the difficulty in both attacking and defending a network. [4] Within a four hour period, the two student teams had to both attack the other team's network as well as defend their own network. The students responded favorably to this event and Vigna decided to include this competition and similar events in future offerings of the course. After several experiences with conducting the competition as an event in his course alone, the event was opened to other institutions across the nation to participate in as well. [1]

The multi-institution version of the competition at UC-Santa Barbara is loosely based on the "Capture the flag" competition held at DEFCON annually. The goal in this competition is for each team to maintain a set of services while attacking and attempting to compromise the services of the other teams. [1] Each service running on a team's network is assigned an associated flag. The goal for each team is to safeguard their flag while attempting

[1] Throughout the documents referenced the term "exercise" is frequently used in place of competition. In this paper the term competition will be used to denote the activity consisting of two or more individuals or teams competing in an organized event with an established set of rules. In the context of a cyber security competition, the terms exercise and competition can, and have been, used synonymously.

to change the flags of competitor's services to their own. Scoring for the competition is based on the services and the flags. Periodically throughout the competition a special scoring program tests to see if a service is functional on each of the competitor's networks. If the service is unavailable, the team receives no points. If the service is functional and the flag is that of the owning team, the team receives some points. If the service is running but the flag is that of another team, the other team receives points.

An important aspect of the UC-Santa Barbara competition is the remote nature of the networks. The list of participants for the 2004 competition included institutions from as far away as Vienna, Austria and Milano, Italy. (see www.cs.ucsb.edu/~vigna/CTF/participants.html) Each competing institution could have any number of teams on separate subnets. All were connected via a VPN to a main system which served as the central hub connecting all institutions. Each team was allowed to have as many hosts connected to their subnet as they wanted. The only requirement for each team was to have one box, referred to as the team box, connected to their subnet and running Fedora Core 2. One benefit of this setup is that it simulates a real-world environment in which attackers will not know the precise configuration of the networks they attack – they will have to discover this.

Another university that conducts a competition between teams of students taking a specific course is Texas A&M University.[1] In the graduate-level *Advanced Networks and Security* course a single *gold team* sets up a network with common services and students in the opposing *black team* attempt to circumvent the security of this network and compromise a system without being detected. The gold team consists of students with special experience in system and network administration. Some members of the gold team are actually selected prior to the beginning of the course. Other members are added after the semester begins. An interesting aspect of the Texas A&M competition is a third set of machines located inside of the gold team network which the black team members have user-level accounts on. This provides an environment from which attacks simulating both insiders and outsiders can be launched.

A third school, the University of Texas at Austin, has conducted a series of competitions outside of the classroom environment. Run by student volunteers, and with undergraduate volunteer students competing, the competitions have lasted anywhere from a week to several months. Participants are provided the address of the target network and a list of objectives. The rules allow for additional activity (attacks) outside the list of objectives and individuals can actually gain bonus points in this manner. The targets, and the individual competitions, vary anywhere from a single target host to a complex ecommerce environment complete with standard security mechanisms such as firewalls and intrusion detection systems. [1] Administration and judging for a contest is up to the undergraduate senior who designed the specific round of competition. Without faculty monitoring and involvement, the rules have deliberately been kept simple with only two guiding rules: competitors are not allowed to conduct denial of service attacks and are not allowed to circumvent outbound restrictions of the network to access the Internet. [1]

These three schools and the service academies are not the only institutions conducting security competitions, but they are representative. The rules used in each competition vary with some, such as at both Texas schools as well as UC-Santa Barbara, allowing the students to attack systems while the competition at the service academies specifically bars this activity and focuses on defending systems. One rule common to all, however, was a prohibition against denial of service attacks. These attacks were viewed as too disruptive to the purpose of the competitions.

## V. Planning The Regional Collegiate Competition

During initial planning meetings, the steering group organized to develop the Texas competition elected to give it a more operational focus than had been seen in other competitions. Some competitions such as traditional "capture the flag" competitions are both offensive and defensive in nature while others examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester. The CCDC is focused on the more operational task of assuming administrative and protective duties for an existing "commercial" network. Teams are scored based on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs. To assist in development of the competition, the steering group agreed that an even, controllable playing field needed to be developed with the following guidelines:

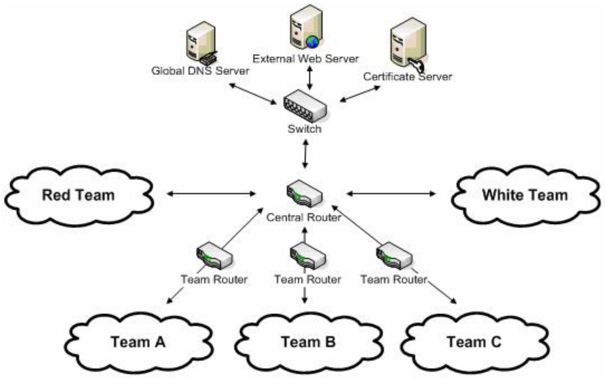
- Each team must operate with an identical set of hardware and software consisting of a small, pre-configured, operational network they would then need to secure and maintain. This eliminates any potential advantage for larger schools or organizations that may have better equipment or a larger budget.
- The entire competition must be located on a dedicated internal network at a single location to

remove the variables associated with multiple locations, VPNs, and propagation delay. This allows control over bandwidth, network traffic, and scoring and eliminates the technology issues associated with a distributed, VPN-based network.

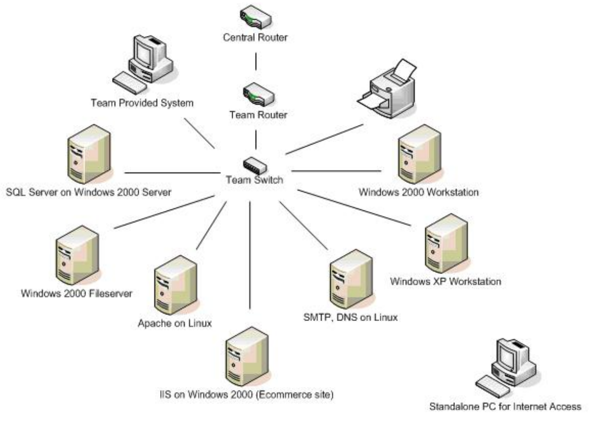
- Each team must be given the same set of business objectives and tasks at the same time during the course of the competition.
- A neutral “red team” must be used to provide realistic suspicious and malicious traffic as well as to test the security capabilities of each team evenly.
- Where possible, an objective, automated scoring system should be used.
- Teams consist of up to 8 graduate or undergraduate students but only full-time students (as defined by each institution) would be allowed to compete.

In November of 2004, the steering group started drafting the initial ruleset to cover student eligibility, competition operations, scoring, allowed actions, allowed materials, etc. The draft ruleset was approved by the steering group in January of 2005 but was still available for modification as needed prior to the competition.

A primary concern for the steering group was the competition network design. The group determined that the best initial environment would be a heterogeneous one consisting of typical commercial and open source operating systems and applications. This provides a challenging environment to competitors without favoring teams coming from institutions with extensive labs and software libraries. Due to equipment limitations and manageability considerations, the group elected to have a competition network consisting of a central router connecting each team, the red team, the scoring functions, traffic capture, and traffic generation functions as shown in Figure 1 below.



Each team is assigned an identically configured network as shown in Figure 2 below:



The overall scenario for the competition is that each team has just been hired to take over the system and network administration functions of a small company. While each team will start with a network that is “functional” in that all the basic operations work (i.e. the mail server will accept and send mail) the network, operating systems, and applications are intentionally not installed in the most secure or efficient manner and there could very well be residual “issues” from the previous administrators or past attackers. This provides each team an opportunity to “find and fix” the issues individually on their own networks. Teams are allowed to modify applications, patch levels, and even operating systems but they must maintain an operational capability. Each supported service is automatically scored on periodic intervals where a functioning service will earn the team points and a non-functional service will not. Additionally, each service carries a service level agreement implementing a point penalty system – the longer a specific service is non-functional, the more it will affect the team’s score. Throughout the competition teams are also given business objectives or tasks to complete; setting up a new FTP service with public and private content and having it operational within 1 hour for example. As the competition networks will not be connected to the outside world, the steering group determined that the CCDC must provide a way for teams to download patches and conduct research. To provide this capability, each team is given one PC connected to the Internet and a 1GB flash drive to facilitate file transfer.

During the competition, the red team performs scanning, reconnaissance, and penetration activities on each team’s network. Teams are penalized for each successful attack executed by the red team – user level access, administrative level access, collection or modification of sensitive data are all weighted and points deducted from the affected team following a verified, successful attack. To help mask activity and make the competition more challenging, the red team, the scoring engine, and the traffic generators all change IP addresses at periodic intervals throughout the competition. At the end of the competition, the team with the most points is declared the winner.

## VI. The Collegiate Cyber Defense Competition™

Five schools participated in the competition which was held the weekend of 15-17 April, 2005 on the campus of The University of Texas at San Antonio. Texas A&M University took the top honors with Del Mar College, a community college from Corpus Christi, TX, coming in second. The competition went smoothly with only one hardware and one software problem. Neither significantly impacted the competition and neither affected the final outcome.

During the first two hours of the competition, no red team activity occurred. The students were given this time to examine their networks, address existing issues, and enhance their security. The different approaches by the universities to the competition was immediately apparent as some arrived with an explicit “game plan” and began to immediately follow it to lock down the network. Other teams were more loose and waited to make an initial examination of their network before beginning to make modifications. While no red team activity occurred during this first two hours, scoring did. All networks were fully functional when the competition started and as soon as the students entered their rooms the scoring engine developed for this competition began recording points. Points were awarded to each team for every required service that was operational when the engine checked for it. Additional penalties were assessed when the length of time a service was continuously down exceeded certain thresholds (similar to service level agreements commonly found in industry). Once red team activity commenced, penalties were also applied to teams who had their systems compromised with root/administrator-level compromises resulting in greater penalties than for user-level compromises. The red team was careful to not concentrate on any one team but instead spread their efforts across the various teams. If a red team member was successful in compromising a system on one team, the member would then attempt the same technique on the other teams as well.

An important aspect of the competition, one for which as many points could be earned as for continuous operation of the required services, was a series of “injects” that were given to the teams at pre-planned points during the competition. The injects were designed to simulate operational activities that administrators face on a daily basis. They included events such as the addition or deletion of user accounts, installation of new hardware or software, or simple things such as reports that managers required on some aspect of network operations. Injects had specific deadlines associated with them and were scored by the judges for each team when the deadline was reached.

While the competition went smoothly, there were some places where improvements could be made for next year’s competition. Some minor modifications to the network were suggested including the addition of more machines to better simulate the “real world” where there is generally not one administrator for every machine the organization owns. Additionally, another system or capability will be added to allow each team to view their own networks from an external perspective. There were several occurrences of teams asking the white team repeatedly whether their services were “up” or not. The additional “outside” machine would allow the teams to see exactly what was visible external to their networks. Finally, minor incidents occurred that emphasized the need to more clearly identify what was considered offensive actions (and therefore forbidden during the competition) and what is considered “outside help” (also forbidden by the rules) and what the specific penalties for such actions will be. Even with what can only be considered minor incidents, no competitive advantage was gained by any team and the competition continued. The lesson learned was by the organizers and more extensive rules documentation governing forbidden activities and the penalties for conducting them will be included in future events.

## VII. Conclusion

The competition was a tremendous success with very few issues occurring during the competition. We believe that the event proved the value of this model for competitions. A blend of security and operations meant that the students had to make decisions similar to the type that a business might make when deciding whether to implement some aspect of security. If a service was brought down in order to make adjustments to security software or hardware, it meant the team would lose points. In a similar manner, a business that brings their ecommerce site down loses any business that might have occurred while the system is down. Students, like businesses, had to weigh the relative merits of the security enhancement versus the known loss the organization would take while the service was unavailable. The response to the injects was predictable. Students whose only network experience was in academic settings were occasionally heard to complain about the likelihood of specific events happening in the “real-world”. Team sponsors, who were mostly instructors from the respective universities, smiled when these comments were heard and explained to their students that the events depicted in the injects actually were very realistic. In this sense, the students were given a glimpse of their lives to come.

The event was such a success that planning has already begun for next year's competition. Of more significance is the desire to take the lessons learned from this event and combine them with lessons learned from other similar events (such as the service academies CDX competition) to develop a national collegiate competition. Discussions on this possibility have already begun and plans moving forward will shortly be announced.

## VIII. References

[1] Hoffman, Lance and Ragsdale, Daniel, "Exploring a National Cyber Security Exercise for Colleges and Universities", Report No. CSPRI-2004-08, The George Washington University, Report no. ITOC-TR-04001, United States Military Academy.

[2] Schepens, Wayne J. and James, John R., "Architecture of a Cyber Defense Competition", Electrical Engineering and Computer Science Department, United States Military Academy, West Point, New York.

[3] Dodge, Ronald C., Ragsdale, Daniel, and Reynolds, Charles, "Organization and Training of a Cyber Security Team",

[4] Vigna, Giovanni, "Teaching Hands-on Network Security: Testbeds and Live Exercises", Journal of Information Warfare vol. 3, no. 2 8-25 2003