

# Collegiate Cyber Defense Competitions

By Gregory B. White, Ph.D., and Dwayne Williams

## Introduction

For several years, competitions have been held pitting individuals or teams against each other in a security arena. The most famous of these competitions is held annually at the DEFCON conference in Las Vegas, NV. Several universities have sponsored similar “capture the flag” and “attack-defend” competitions, using them to provide an element of excitement in courses on computer and network security. More recently, a new type of competition has been introduced, one in which the participants do not engage in any offensive cyber activities but are solely engaged in defending their systems and networks. The service academies pioneered this type of competition and have conducted inter-school competitions for several years. Known as the Cyber Defense Exercise (CDX), the inter-service academy competition is based on defending networks with offensive actions prohibited. Their competition has served as the initial model around which discussions for a national cyber security competition have revolved.\*

Whether to allow offensive actions by competitors is often a point of debate. Some organizations have argued that the best way to learn how to defend against attacks is to learn the tactics and techniques used in attacking systems. Others argue that this is nothing more than training for the next generation of computer “hackers.” Individuals in this camp also suggest institutions may be liable for legal action if students later use knowledge they learned during a competition to gain unauthorized access to other systems. Another argument against permitting offensive activities by competitors is that an emphasis on defensive activities promotes a defensive mindset, which is arguably what competitors will need when they graduate.

## The National Cyber Security Exercise Workshop

A group of educators, students, and representatives from government and industry met in San Antonio, Texas in the spring of 2004 to discuss establishing a series of collegiate cyber security competitions. The stated goal or purpose of a cyber security competition discussed at the workshop illustrates the desires of the participants:<sup>1</sup>

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.

As seen, the purpose of the competition is education. The goal is to help students better defend computer systems and networks. In order to reach this goal, participants identified several objectives for the workshop including:<sup>1</sup>

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

When the decision to hold the first Texas Regional Collegiate Cyber Defense Competition (CCDC) was made, the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio volunteered to develop and conduct the competition. The CIAS formed an initial steering group consisting of representatives from the CIAS, the University of Texas at Austin, and Texas A&M University—the three Texas schools that participated in the San Antonio workshop. While designing the CCDC, the CIAS attempted to remain true to the goals of the workshop.

## Other Collegiate Cyber Security Competitions

The United States Military Academy conducted the first Cyber Defense Exercise (CDX) in 2001 in order to serve as the capstone course in their information assurance program.<sup>2</sup> All five of the service academies now participate in this annual event that pits cadet teams from each of the academies against offensive Red Teams from the Department of Defense. The emphasis is on maintaining an operational network in the face of a hostile force attempting to breach the security of each team’s network. The teams are required to design, implement, and maintain a network consisting of a variety of platforms. Security software is limited to open source tools which serves to create more of a level playing field between the teams.

Three types of teams are involved in the competition. A Blue Team is fielded by each of the service academies (as well as the Naval Postgraduate School and the Air Force Institute of Technology, which are not eligible for the winner’s trophy) to develop, operate, and defend their network. An offensive Red Team is supplied by the DoD, 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 team, the White Team, consists primarily of individuals from Carnegie Mellon University. The purpose of this team is to establish the scenarios and scoring criteria used and to serve as referees for the competition.

The service academies are supportive of the cyber defense exercise for several reasons. The competition not only serves as the capstone event in their respective programs, it also provides leadership opportunities for team members—a key goal of all of the service academies. The cadets are responsible for planning and deploying their own teams, and for the actual execution of the competition.<sup>3</sup>

While the CDX has received the most publicity and is probably the best-known collegiate security competition, it is not the only one. Giovanni Vigna

at the University of California at Santa Barbara decided to use an exercise (competition) in his course on network security to help provide students a better understanding of the difficulty in both attacking and defending a network.<sup>4</sup> Two student teams had four hours to both attack the other team's network while defending their own. The students were enthusiastic about this event, which led Vigna to include competitions and similar events in other offerings. After gaining experience with conducting the competition, Vigna ultimately opened the event to other institutions across the nation.<sup>1</sup>

The competition at UC-Santa Barbara is loosely based on the "capture the flag" competition made popular at DEFCON. The goal is for each team to maintain a set of services while attempting to compromise the services of the other teams.<sup>1</sup> A flag is associated with each service running on a team's network. Each team must protect its own flags while attempting to change the flags of competitor's services to their own. A special scoring program periodically tests to see if a service is functional on each of the competitor's networks. If the service is functional and the flag is that of the owning team, the team receives points. If the service is unavailable, the team receives no points. If the service is running, but the flag is that of another team, the other team receives points.

An interesting aspect of this competition is that it now includes institutions from around the world. The list of participants for 2004 included institutions from as far away as Vienna and Milano ([www.cs.ucsb.edu/~vigna/CTF/participants.html](http://www.cs.ucsb.edu/~vigna/CTF/participants.html)). All institutions are connected via a VPN to a main system which serves as the central hub. Each team is allowed to have as many hosts connected to their subnet as they want.

In the graduate-level *Advanced Networks and Security* course at Texas A&M University, a Gold Team develops a network with a set of common services.<sup>1</sup> Students in an opposing Black Team attempt to circumvent the security of the Gold Team's network and compromise the systems. The gold team consists of students with experience in system and network administration. An interesting aspect of the Texas A&M competition is the inclusion of a third set of machines located inside of the gold team network, which the black team members are provided user-level accounts on. This creates an environment in which insider attacks can be simulated.

The University of Texas at Austin has conducted a series of competitions which are not part of any course. In fact, the competitions, which have lasted anywhere from a week to several months, are run by student volunteers. Participants are given the address of the target network and a list of objectives for the competition. Rules allow for additional attacks outside the list of objectives and individuals can gain bonus points by developing creative attacks. The targets vary anywhere from a single host to a complex network mimicking environments, such as an e-commerce Web site complete with standard security mechanisms.<sup>1</sup> Administration and judging for the different contests is up to the student who designed it. Without faculty involvement, the rules have deliberately been kept simple, with only two guiding principles: competitors are not allowed to conduct denial of service attacks and are not allowed to circumvent outbound restrictions to access the Internet.<sup>1</sup>

These schools and the service academies are not the only institutions conducting security competitions, but they serve as a sample. The rules used in each competition vary, with some allowing offensive activities while others don't and focus on defending systems. One rule common to all is a prohibition against large-scale denial of service attacks which are viewed as too disruptive and not in keeping with the purpose of the competitions.

## Planning The Regional Collegiate Competition

During initial planning meetings, the steering group for the Texas regional competition elected to give it a more operational focus. The CCDC focused

on the task of assuming administrative and protective duties for an existing "commercial" network. Teams were scored based on their ability to detect and respond to outside threats, maintain availability of existing services, respond to business requests, and balance security needs against the needs of the organization. The steering group agreed that an even, controllable playing field needed to be established using 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 secure and maintain. This eliminates any potential advantage for larger schools or organizations with better equipment or larger budgets.
- ▲ The competition must be located on a dedicated internal network at a single location to remove variables associated with multiple locations, VPNs, and propagation delays. 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 competition.
- ▲ A neutral "red team" would provide realistic suspicious and malicious traffic and would test the security capabilities of each team.
- ▲ Where possible, an objective, automated scoring system should be used.
- ▲ Teams would consist of up to 8 graduate or undergraduate full-time students (as defined by each institution).

In November of 2004, the steering group drafted the initial ruleset, which was circulated for comments. After modifications, the rules were approved in January of 2005.

The network design was a primary concern for the steering group. The initial environment was designed to be a heterogeneous network consisting of typical commercial and open source operating systems and applications. This provided a challenging environment to competitors without favoring teams from institutions with extensive labs and software libraries focused on specific systems. In order to be manageable, the competition network consisted of a central router connecting a limited number of systems for each competing team, the red team, the scoring functions, traffic capture, and traffic generation functions as shown in Figure 1.

Each team was assigned an identically configured network as shown in Figure 2.

The overall scenario described a situation in which each team had been hired to take over the system and network administration functions for a small company. While each team started with a network that was "functional" in that all the basic operations worked, the network, operating systems, and applications were intentionally not installed in the most secure or efficient manner and could have residual "issues." This provided each team an opportunity to find and fix problems on their own networks. Teams were allowed to modify applications, patch levels, and even operating systems, but they had to maintain the operational capability. Each service was scored automatically at periodic intervals with a functioning service earning the team points. A non-functional service did not result in a deduction of points, unless the service remained non-functional for an extended period. Each service carried a service level agreement implementing a penalty system—the longer a service was non-functional, the more it affected the team's score through the application of an increasing number of penalty points. Throughout the competition, teams were also given business tasks to complete, such as setting up a new FTP service with public and private content and having it operational within a specified period of time. The competition networks were not connected to the

Internet, but each team was given one PC connected to the Internet and a 1GB flash drive to facilitate file transfer.

During the competition, the red team was responsible for performing scans, conducting network and system reconnaissance, and attempting to penetrate each team's network. Teams were penalized for each successful attack by the red team with the level of penetration—user level access, administrative level access, or modification of sensitive data—determining the number of penalty points assigned. Any penalty assigned to a team as a result of a breach of some sort was verified by a white team member. To help mask activity, the red team, scoring engine, and traffic generators all changed their IP addresses periodically. At the end of the competition, the team with the most points was declared the winner.

## The Collegiate Cyber Defense Competition™

Five Texas schools participated in the competition held at the University of Texas at San Antonio April 15-17, 2005. After 24 hours of competition, Texas A&M University took the top honors. Del Mar College, a community college from Corpus Christi, was second. The competition went very smoothly, with only one hardware and one software problem. Neither significantly impacted the competition or affected the final outcome.

During the first two hours of the competition, no red team activity occurred in order to provide teams time to examine their networks, address problems, and enhance security. The teams exhibited very different approaches, as some arrived with an explicit "game plan" they immediately implemented to lock down the network while others waited to make an initial examination of their network before making modifications. While no red team activity occurred during the first two hours, scoring commenced immediately. All networks were fully functional when the competition started, and as soon as the students entered their rooms, the scoring engine began. Once red team activity commenced, penalties were also applied to teams who had their systems compromised. It was important for the red team to not concentrate on any one team and care was exerted to spread efforts across all teams. If a red team member was successful in compromising a system from one team, the member would then attempt the same technique on other teams and a white team member would verify the compromise.

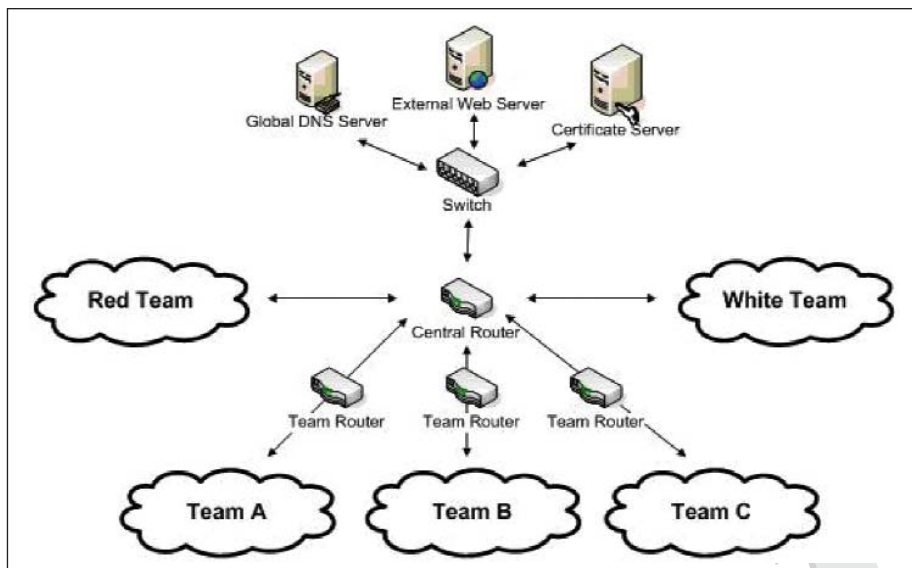


Figure 1: The Competition Network

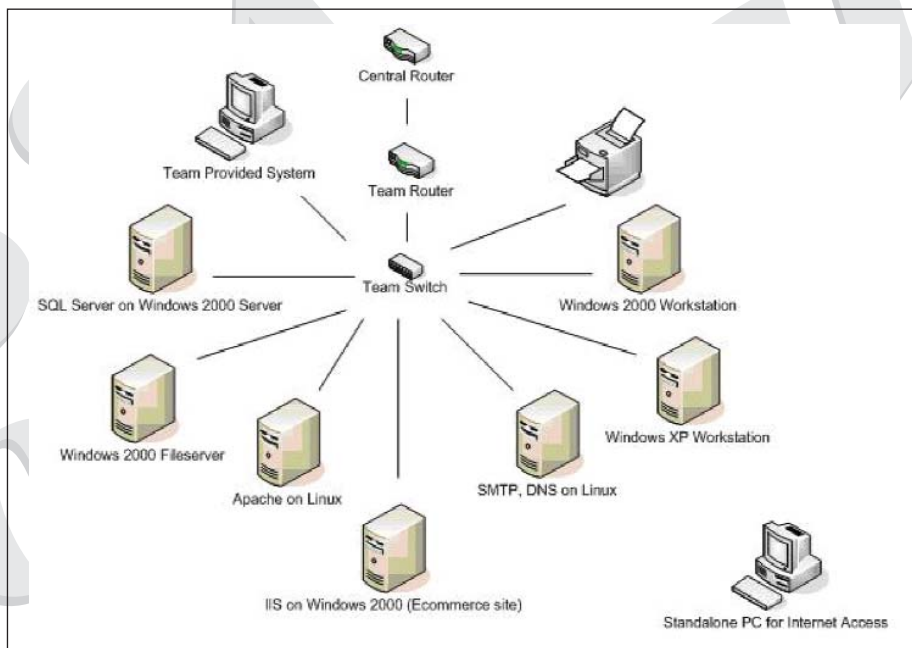


Figure 2: A Team Network Configuration

An important aspect of the competition was a series of "injects" given to the teams at pre-planned points during the competition. The injects were designed to simulate operational activities that administrators face daily. They included events such as the addition or deletion of user accounts, installation of new hardware or software, or requests for reports that managers might ask for on network operations. Injects had deadlines associated with them and were scored by white team judges assigned to each team.


While the competition went smoothly, there were some places where improvements could be made. Minor modifications to the network were suggested, including adding more machines to

better simulate the "real world." Minor incidents also occurred that emphasized the need to more clearly state competition rules, specifically rules and documentation governing forbidden activities and any associated penalties.

## Conclusion

The competition was a tremendous success, with very few problems occurring. The event proved the value of this model for competitions, as the blend of security and operations meant the students had to make decisions similar to the type organizations 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 e-commerce site down loses any business that might have occurred while the system is down. At the same time, leaving a site operational but with a security flaw might result in a compromise which can have a devastating impact on the organization. Students had to weigh the relative merits of a security enhancement versus the known loss the team would take from an unavailable service.

The event was such a success that planning has already begun for next year's competition. More significantly is the intention to take the lessons learned from this and other competitions and develop a national collegiate competition. Plans for such an event are already underway, and sponsorship for this event is being sought. 

---

*Gregory B. White, Ph.D., and Dwayne Williams are with the Center for Infrastructure Assurance and Security.*

<sup>\*</sup> Throughout the documents to denote an activity consisting of two or more individuals or teams referenced, the term "exercise" is frequently used in place of competition. In this article, the term competition will be used competing in an organized event with an established set of rules. In the context of a cyber security competition, the terms exercise and competition are often used synonymously.

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Dodge, Ronald C., Ragsdale, Daniel, and Reynolds, Charles, "Organization and Training of a Cyber Security Team."

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

<sup>5</sup> White, Gregory and Williams, Dwayne, "The Collegiate Cyber Defense Competition," *Proceedings of the 9th Colloquium for Information Systems Security Education*, 6-9 June, 2005, Atlanta, Georgia.