Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

The National Collegiate Cyber Defense Competition

Gregory B. White, Ph.D., Center for Infrastructure Assurance and Security
Ronald C. Dodge JR, Information Technology and Operations Center

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 share their ideas on how such a competition should be conducted. The final report from this workshop included a number of recommendations and described a general consensus among the participants that such an event should be pursued. Several participants from the Texas school presents agreed to develop a regional competition which was held in March of 2005. After the success of this event, The University of Texas at San Antonio, who hosted this regional competition, announced at the 2005 CISSE conference that they intended to conduct a national competition in 2006. Five regional competitions were held in the spring of 2006 and the national competition was held in April. This paper describes the history that led to this national competition, describes lessons learned and the results of the regional and national competitions in 2006 and presents the proposed plan for expanding the current effort in order to establish a permanent annual competition. The paper provides an update to the paper proposing the first national competition presented at the CISSE 2005 conference.

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

I. Introduction

Competitions have long been held at the collegiate level to match teams from different schools 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 their teams. While some competitions are held for not much more than "bragging rights", many have the goal of improving the skill and knowledge of the participants in the field they are competing in.

Members of the cyber community are not immune to the desire to test their skills against those of others from different schools. Events such as "capture the flag" and "attack-defend" competitions have been held for over a decade. Several universities have conducted their own competitions to attempt to motivate and excite students in various courses on computer and network security. The nation's service academies have taken this a step further by conducting inter-school competitions for several years. The inter-service academy competition, known as the Cyber Defense Exercise (CDX), served as the initial model around which the discussions about a possible national cyber security competition were held. [1] A critical aspect of this competition, and for the proposed national competition, was that the competition would be focused on the defense of computer systems and networks and would not include a component in which the participants attempted to attack each other's networks. Two prominent reasons for this is the desire to not have any such competition be viewed as "hacker training", and to also simulate what students will face upon graduation which is the protection of an organization's network. Specialized courses can be taken at many universities which prepare students for jobs which might include penetration testing of a client's network.

In 2005 the first Southwest Regional Cyber Defense Competition was held in San Antonio, TX with five schools competing. The Center for Infrastructure Assurance and Security (CIAS) at UT-San Antonio conducted this first event. Following the lead of the service academy competition and the recommendations from the 2004 workshop, this exercise focused on the defense of a network and did not allow the participants to conduct offensive activity against other teams. The response from the schools that participated was extremely favorable and all expressed an interest to return the next year. Del Mar Community College volunteered to host the 2006 event and UT-San Antonio, which had developed the 2005 competition, decided to hold a national competition. An announcement was made at the 2005 CISSE conference in which a general call was issued for any schools that wished to participate in similar competitions and especially for any schools who might be interested in hosting such and event. Five regional competitions were organized (including the 2006 CDX) and plans went forward for the 2006 National Collegiate Cyber Defense Competition. This competition was held in April of 2006 with support from the US Department of Homeland Security (DHS).

ISBN 1-933510-98-6/$15.00

II. The Cyber Defense Exercise (CDX)

The United States Military Academy (USMA) created the first Cyber Defense Exercise (CDX) to serve as the capstone course in their information assurance program. [2] Soon all five of the service academies were participating in this annual event that uses an offensive Red Teams from the Department of Defense to attack the networks protected by the cadet teams from each of the service academies. As previously mentioned, the emphasis of the event is for the teams to maintain an operational network in the face team's network. One aspect of the CDX that differs from the national competitions is that each team is required to design, implement, and maintain their own operational network consisting of a variety of platforms. Only open source security tools are allowed in an attempt to ensure a level playing field between the teams.

The service academies continue to conduct the concept of a cyber defense exercise for several reasons. The CDX first serves as a capstone event which can be used to evaluate the students' knowledge of information assurance concepts and their ability to protect computer systems and networks. The competition also provides leadership opportunities for the team members, an aspect important to all of the academies for obvious reasons. Leadership opportunities are promoted through the requirement that cadets plan their own networks, deploy their own teams, and execute their plans during the competition. [3] Each year the competition has proven to be a popular event for both cadets and faculty.

III. The National Cyber Security Exercise Workshop

Researchers from USMA and George Washington University obtained a National Science Foundation (NSF) grant to conduct a workshop examining the feasibility of conducting a national cyber competition. Their grant allowed a group of educators, students, and government and industry representatives to meet in San Antonio, Texas, in the spring of 2004. The purpose of a cyber security competition[1] as outlined in the grant and discussed at the workshop was: [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.

This statement clearly identifies the real goal for these competitions which is to help prepare students to better protect computer systems and networks. The goals for the workshop 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

In order to conduct a national competition with a potential regional competition structure supporting it, the participants at the workshop understood the need to create a uniform structure that would be repeatable at as many institutions as possible. The group also identified concerns that might become an issue when developing or conducting a competition. Other important issues that would affect the development of a national competition structure were also addressed such as whether to limit participation to post-secondary students, how level playing fields could be created to eliminate possible advantages due to hardware and bandwidth differences at different schools, the development of a fair set of rules, implementation of a fair and impartial scoring system, and how to address possible legal concerns [1]. While the workshop did not result in an agreed upon set of guidelines for a national competition, it did see a consensus among the participants on a general framework from which further discussions could occur. The workshop adjourned with an agreement that committees would be formed to continue the work and address the various identified aspects required in establishing a national competition.

IV. Collegiate Cyber Security Competitions

While the CDX has received the most publicity and is the best known collegiate cyber security competition, it certainly does not stand alone. Giovanni Vigna at the University of California at Santa Barbara has used a competition in his course on network security to help

[1] Terminology may cause some confusion in discussions on cyber competitions. The term "exercise" is frequently used in place of "competition". For this paper the term competition will be used to identify the activity consisting of two or more individuals or teams competing in an organized event with a predefined and established set of rules.

provide the students with a better understanding of the difficulty in both attacking and defending a network. [4] In a short four hour period, two student teams have to attack the other team's network as well as defend their own. After running the competition as an event in his course alone, Giovanni opened the event to other institutions across the nation. [1]

The multi-institution competition at UC-Santa Barbara is loosely based on the famous "Capture the flag" competition held annually at DEFCON. The goal in this type of competition is for each team to maintain a set of defined services while attacking and attempting to compromise the services running on the networks for the other teams. [1] A special scoring engine is used to periodically test each team's network to see if the services are available. No points are received if the service is unavailable. If the service is functional the team receives points. A special "flag" can be planted in an opposing teams system so that their services can be claimed ("owned") which will instead give the team which planted their flag the points instead.

In order to conduct this competition with teams from across the nation (and has included international participation as well), the UC-Santa Barbara competition connects teams via a VPN to a main system which serves as a central hub. Each team is allowed to have as many hosts connected to their own subnet as desired. The only configuration requirement for each team was to have one box, referred to as the team box, connected to their subnet running Fedora Core 2. This setup is designed to simulate a real-world situation for attackers who will not know the precise configuration of their targets.

Another university that includes a competition in one of its security courses is Texas A&M University.[1] In the graduate-level *Advanced Networks and Security* course a single *gold team* is pitted against other teams who attempt to circumvent the security of the network the gold team is tasked with creating. The gold team's network includes common services and students in the opposing *black team* attempt to exploit this network without being detected. Members in the gold team consist of students with special experience in system and network administration. The gold team is also required to maintain a third set of machines inside of their network on which black team members are given user-level accounts. This provides an competition environment which simulates both insider and external attackers.

While the other schools discussed included competitions as part of organized courses, The University of Texas at Austin has conducted a series of competitions outside of the classroom environment. These competitions have actually been run by student volunteers with undergraduate students competing. The length of the individual competitions last anywhere from a week to several months. Individuals wishing to participate are provided the address of the target network and a list of objectives for the specific competition. The organizers of the competitions allow for additional activities (attacks) outside the list of objectives and individuals can actually gain bonus points through creative attacks. The targets for each competition vary from a single host to a complex ecommerce environment complete with standard security mechanisms. [1] Administration and judging for a contest is up to the undergraduate student who designed the specific competition. Without faculty involvement, the rules have deliberately been kept simple with only two overarching guidelines: competitors are not allowed to conduct denial of service attacks and no competitor is allowed to circumvent outbound restrictions of the network in order to access the Internet. [1]

The schools mentioned are not the only institutions conducting security competitions, but they provide a good representation of the types of competitions that were conducted prior to the workshop held in 2004. Some of these competitions, such as the CDX, are still being conducted today. The rules used in competitions vary with some, such as at both Texas schools and UC-Santa Barbara, allowing students to attack systems while others, such as the CDX, specifically bars this activity and focuses on the defense of computer systems and networks. One interesting note, however, is the seemingly common rule common that prohibits denial of service attacks. These attacks were described as being too disruptive and would interfere with the purpose of the competitions.

V. THE FIRST REGIONAL COLLEGIATE COMPETITION

The Collegiate Cyber Defense Competition (CCDC) took a more operational focus as opposed to either an attack-and-defend exercise or one in which the students designed, built, then administered a network as had been seen in other collegiate competitions. In the CCDC the students were given the task of assuming administrative and protective duties for an existing "commercial" network. Teams were scored based on a combination of things including their ability to detect and respond to external attacks, maintain the availability of existing services, respond to business-related requests such as the addition or removal of services, and balance security needs against business operational needs. The following guidelines were used in developing the first regional CCDC:

- 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 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 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). [5]

A primary concern for the competition was the design of the network. The decision was made to have a heterogeneous environment consisting of commercial and open source operating systems and applications typically found in industry. This provided a challenging environment for competitors without favoring teams with extensive labs and software libraries focused on a single operating system or environment. The ultimate design, which considered issues of manageability, consisted of a central router connecting each team, the red team, the scoring functions, traffic capture, and traffic generation functions as shown in the figure below.

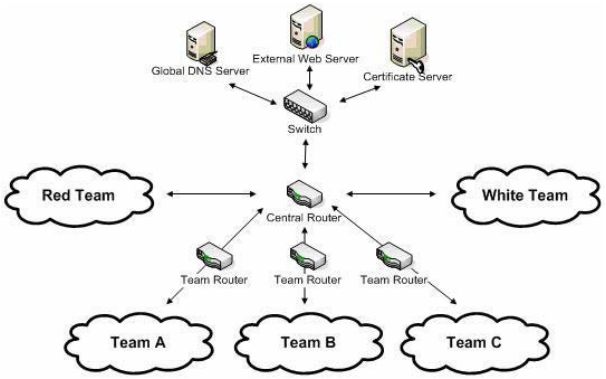

Figure 1 Exercise logical network design

Each competing team was assigned an identically configured network as shown in the second figure:

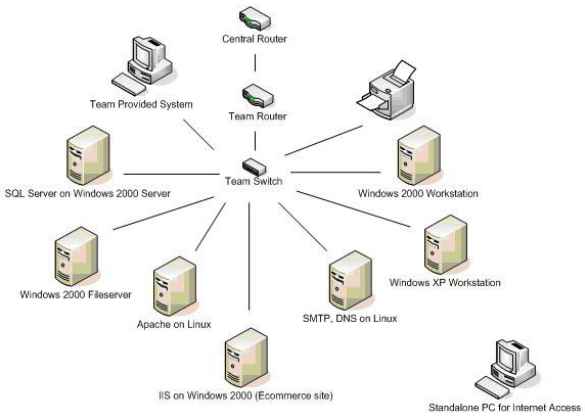

Figure 2 Team logical network

The overall scenario storyline for the competition stated that each team had just been assigned the system and network administration functions of a small company. While each team started with a network that was working in that all the basic services worked (e.g. the mail server accepted and sent mail) the network, operating systems, and applications were not necessarily installed in the most secure or efficient manner. The competitors were told that there could very well be residual "issues" from the previous administrators or past attackers. This meant that each team needed to "find and fix" these leftover issues on their networks. Teams were told that they could modify applications, patch levels, and even operating systems but they had to maintain an operational capability throughout the competition. A scoring engine was used to automatically score on a periodic basis whether the required services were functioning. To further simulate a real-world situation, each service included a service level agreement implemented through a penalty system – the longer a specific service was non-functional, the more penalty points the team received. Throughout the competition teams were also given tasks to complete such as setting up a new FTP service with public and private content and having it operational within 1 hour. The competition networks were not connected to the Internet but a method was provided, through a flash drive and a single PC connected to the Internet but not connected to the competition network, for teams to download patches and conduct research.

During the competition, a corporate red team performed scanning, reconnaissance, and attempted to penetrate each team's network. Teams were penalized for each successful attack executed by the red team with varying penalties assigned depending on the severity of the

penetration– user level access, administrative level access, or collection/modification of sensitive data. To make it harder for the teams to spot the red team activity, and to make the network traffic more realistic, the red team, scoring engine, and traffic generators all changed IP addresses at periodically during the competition. The winner was chosen at the end of the competition by tallying all points and determining who had the largest score.

VI. Lessons from the First CCDC

Overall the competition went very smoothly. The students were given two hours at the beginning of the competition to explore and modify (if desired) their network and systems. No red team activity occurred during this period. The different approaches to the competition by the teams was immediately apparent as some arrived with an explicit "game plan" they immediately followed to lock down the network. Other teams waited to make an initial examination of their network before beginning to make any modifications. While the red team was not active during this first two hours, scoring began immediately. All networks were working when the competition started and as soon as the students entered their rooms the scoring engine was started. Once red team activity commenced, penalties were applied to teams who had their systems compromised though the red team was careful to not concentrate on any one team instead spreading their efforts across all teams evenly. If a red team member was successful in compromising a system for one team, the red team would attempt the same technique on the other teams as well and another team member would verify the initial compromise..

An important aspect of the competition was a series of "injects" given to all of the teams at pre-planned points during the competition. Points were earned for either complete or partial completion of the tasks which simulated real-world business and system maintenance chores. They included events such as the addition or deletion of user accounts, installation of new hardware or software, or simply reports that managers might ask for on some aspect of network operations. All of the injects had deadlines associated with them so the teams had to be organized to complete them while maintaining their network.

While the competition went smoothly, there were some places where improvements for the next year's competition were identified. Some minor modifications to the network were suggested including adding more machines to better simulate the "real world" where there is generally not a one-to-one relationship between administrators and the systems they maintain. Teams also requested a method to allow them to view their own networks as if from an external perspective. This let them have a better idea of what the scoring engine was seeing in terms of what services were correctly functioning. During the first year's competition there were several occurrences of teams asking repeatedly whether their services were "up" or not.

VII. The 2005 Regional Competitions

The design for the national competition calls for several regional competitions that feed the national level similar to a play-off scenario. Each region conducts its own competition and the winner then advances to the next round. In 2006 there were five regional exercises that each sent a team to the national competition. The model for the regional competitions permits maximum flexibility for each participating region. The reasoning for this was twofold. First, resources in each region were provided by the respective region and therefore requiring a specific format was not feasible. Second, the competition must be designed with the local objectives in mind to satisfy local desires. The only specification was the framework for the national competition. We felt this would provide the requisite motivation to structure the regional events in a manner to provide the winning team with the best chance to succeed at the nationals.

Twenty-nine teams competed in the various regional competitions. The winning teams which went on to compete at the National Championship competition included the University of North Carolina-Charlotte, Southern Illinois University at Carbondale, Millersville University, and The University of Texas at San Antonio. In addition, a team with members from the different service academies was assembled to compete at the championship. The reason the academies fielded this combined team was because their competition had not determined the winning team in time to arrange for the winner to travel to the national competition.

VIII. The 2006 National CCDC

One of the first differences between the National CCDC and the various regional competitions is in the goals and objectives for the competition. At the regional competitions the focus of the event was generally on providing an educational experience for the students to learn from. While this is an important part of the national event as well, it is not the primary focus. The main goal of the national event is to provide a fair and impartial

competition. The students in the normal course of participating in the event will learn much about security but the event itself is not designed primarily to provide them with a learning experience. While the difference is not substantial, it did shape the way many aspects of the competition were approached.

The national competition followed a similar format to the 2005 Southwest CCDC. Some lessons learned were applied, but the format remained similar. One of the most significant differences from the 2005 CCDC was the DHS support. After representatives from the Exercise Program in the National Cyber Security Division, DHS learned of the program, they offered to provide support for the competition. As a result of their support, funds were available to provide transportation and lodging for all of the teams at the national competition. In addition to this critical DHS support, other sponsors of the event included security vendors who supplied equipment or items to give to the students as well as local sponsors who helped with items such as meals and snacks for the competitors.

IX. Results of The 2006 National CCDC

The competition was held 21-23 April in San Antonio as planned. The event experienced only one significant problem. The bandwidth promised by the hotel for the event was not provided and issues such as the downloading of patches to update and secure systems took an inordinate amount of time. To address this problem, White Team members requested a list of desired patches from the teams and downloaded them at other sites. This problem, because it was experienced evenly by all teams, did not result in an advantage to any specific school. It did allow the Red Team, however, to be more successful than they might have otherwise been. The teams were given a period of time Friday afternoon to analyze and secure their networks before the Red Team began its activities. Once the Red Team was turned loose, they had gained administrator/root-level access on machines in every team's network.

The competition was tight with every team still in contention for the trophy on Sunday morning. No team was in the lead in all three categories scored—injects, services, and penetrations (Red Team activity). Ultimately the University of North Carolina-Charlotte broke away from the others and went on to win the first national championship. Millersville University went home with the second place trophy.

X. Plans for Future CCDC Events

The interest in the CCDC has been growing with additional schools already asking whether they can conduct a regional in their part of the nation in 2007. Others, while not wanting to hold a regional competition themselves, are interested in participating in a competition close to them. The goal for 2007 is to expand the five regional competitions to between eight and ten competitions. The coverage of the regional competitions in 2006 favored the eastern portion of the United States. In 2007 the desire is to have a much more uniform coverage with regional competitions being held within a few states of any location within the nation. The format for the 2007 competition will be very similar to the 2006 competition. The regional competitions will again be allowed to use whatever format they desire for their individual competitions. Documentation and guidance will be provided by the CIAS for any of schools who want to copy the format used at the national competition. Again, the concept is to have the winner from each regional competition travel to the national competition which will again be conducted by the CIAS at UTSA.

In order for the concept of a national competition to continue beyond the loosely connected competitions now created, there needs to be a strong governing body formed. The idea of such an organization was recommended during the workshop held in 2004 but has not progressed beyond that initial recommendation. With the experience gained in the regional and national competitions there is now finally enough experience to bring individuals together to form a governing body. Once the governing body is formed, the formal rules for the national competition (and regional competitions if the body decides to address this as well) can be created.

The proposed plan to develop the CCDC governing body and rules begins with the CIAS at UTSA continuing to conduct the national competition through the 2008 national competition. After the completion of the 2006 national competition, academics and representatives from government and industry approached to determine their interest in participating in the governing body. The idea is to have the governing body established by the time the 2007 competition is held. Members of this body will be required to attend the 2007 competition to assist with it and will be asked to remain after the competition is concluded to hold their first meeting. During the year leading up to the 2008 competition, the governing body will be tasked with the development of the charter for the body itself as well as creating an agreed upon set of rules that will govern the national competition and how teams may qualify for this event. The board may also want to address the issue of what assistance or guidance will be

provided to the regional competitions. The proposed composition of the governing body is to populate it with predominantly faculty members from institutions who have been involved in cyber security competitions. The body should also have representatives from government and industry – especially individuals from organizations who have committed to be sponsors of the competition.

Following the completion of the 2008 national competition, the rules developed by the governing body will take affect and plans for the 2009 national and regional competitions should be announced at that time.

XI. Conclusion

<we will add the final conclusions after the national competition>

XII. 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

[5] White, Gregory and Williams, Dwayne, "Collegiate Cyber Defense Competitions", The ISSA Journal, pp. 42-45, October 2005.