Architecture of a Cyber Defense Competition*

Wayne J. Schepens and John R. James[I]
Electrical Engineering and Computer Science Department
United States Military Academy
West Point, NY 10996, U.S.A.
John-James@usma.edu
Wayne-Schepens@usma.edu

Abstract – *This paper describes the effort involve in executing a Cyber Defense Exercise while focusing on the White Cell and Red Forces activities during the 2003 Inter-Academy Cyber Defense Exercise (CDX). These exercise components were led by the National Security Agency and were comprised of security professionals from Carnegie Mellon University's CERT, the United States Air Force, and the United States Army. This hands-on exercise provided the capstone educational experience for information assurance students at the U. S. service academies. The White Cell developed the scenarios and anomalies, established the scoring criteria, refereed the exercise, and determined the winner based on the effectiveness of each academy to minimize the impact to their networks from the Red Forces network intelligence gathering, intrusion, attack and evaluation. To understand better all that is involved this paper takes advantage of the authors three years of experience in directing the activities associated with the planning and execution of the 2003 exercise.*

1 Introduction

Designed to fill the CAPSTONE requirement for the United States Military Academy's Information Assurance course in 2001, the Cyber Defense Exercise (CDX) pits teams of cadets from each of the five US service academies against security experts within the Department of Defense. Each team is challenged to design, implement, and manage an operational network of computers. Management of various platforms (Windows, LINUX, Solaris, FreeBSD, etc.) is required and services such as web, email, public key infrastructure, and database sharing must be provided. Students are encouraged to establish architecture, policy, and procedures that invoke a defense-in-depth and defense-in-breadth posture to keep the aggressors at bay. To keep the playing field level, security measures are limited to open source freely available tools. Strategies and techniques employed by the students that were tested on the CDX battlefield have provided industry, academia, and government with valuable lessons. These lessons are related to work in network mapping, port scanning, vulnerability scanning, password integrity checking, network monitoring tools, intrusion detection systems, host-based and network-based firewalls, and layer-two bridges.

As the competition begins, the National Security Agency (NSA) - led Red Force identifies vulnerabilities and launches repeated attacks on each network over a four-day period. Students have the ability to enter into direct cyber combat in an effort to keep services on-line and running. Teams are then evaluated on maintaining services as well as efforts to recover from and prevent future security breaches. The winner is presented the NSA Information Assurance Director's Trophy. West Point held the title in the first two years of the competition; however, the US Air Force Academy took

Figure 1. NSA Information Assurance Director's Trophy

* **U.S. Government work not protected by U.S. copyright**

[I] This work was partially supported by an endowment establishing the Adam Chair in Information Technology. The views expressed herein are those of the authors and do not purport to reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

home the trophy in 2003, Figure 1.

The CDX has resulted in an intense rivalry between the academies and has become a staple of each academy's information assurance curriculum. The DoD's investment in this project has already reaped extraordinary benefits and the sky is the limit. The CDX should serve as a model for inter-agency programs as there are several players involved each year whose vision and dedication make this effort a success. In just three years the number of personnel involved in carrying-out and participating in the exercise has grown from approximately 40 to over 300.

The CDX consists of three main components: the *Blue Forces* consisting of the five US service academies, the Naval Postgraduate School and the Air Force Institute of Technology[1]; the *Red Forces* consisting of the National Security Agency, the Air Force 92nd Information Warfare Aggressor Squadron, and the Army 1st Information Operations Command; and the *White Cell* consisting primarily of personnel from Carnegie Mellon University and led by Mr. Wayne Schepens. This paper focuses on the responsibilities and activities of the Red Forces and the White Cell in establishing an effective cyber defense competition.

2 White Cell Lays the Groundwork

The White Cell developed the scenarios and anomalies, established the scoring criteria, refereed the exercise, and determined the winner based on the effectiveness of each academy to minimize the impact to their network of the Red Forces malicious activities.

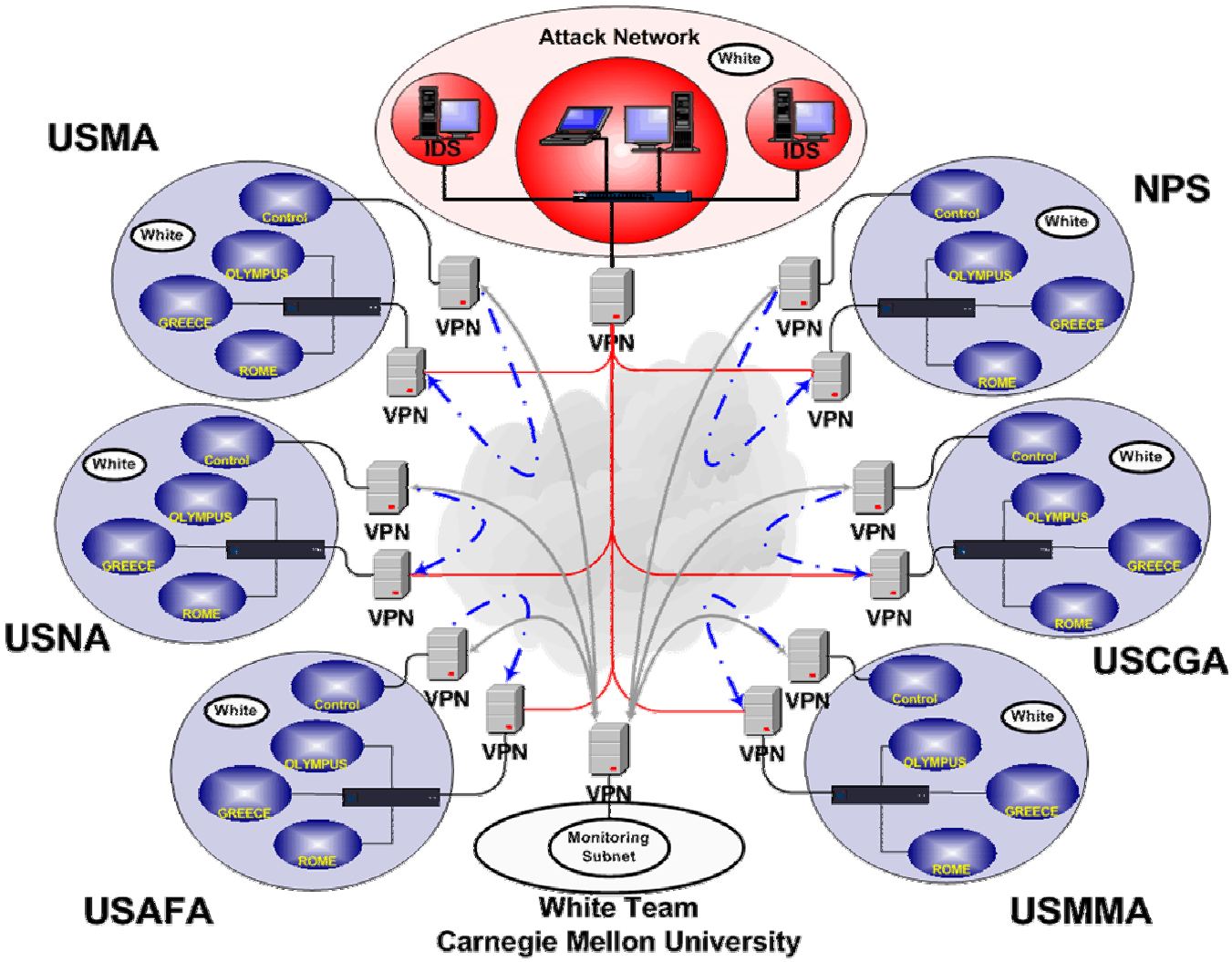

Figure 2. Top-Level Architecture of the Global Liberation Grid (GLG) for the CDX

2.1 Scenario

Completing the scenario early is essential to enable each participant time to provide input. Six months is adequate, but no matter how much time is provided the

[1] AFIT and NPS competed in a separate competition that was run in parallel with the service academy competition.

White Cell must be persistent because if the input does not come by way of comments during the planning stages it will come by way of complaints during the execution stages.

The military academies use exercises to capture realistic situations and put future military officers in positions in which they are expected to encounter upon graduation. The 2003 CDX scenario was as follows:

A multi-nation coalition force has initiated a liberation operation against the hostile country of Red. The coalition combatant force is to be supported by a network architecture known as the Global Liberation Grid (GLG). The coalition is depending on the United States X Academy to establish a command to support this network. The GLG will consist of seven commands located in various places throughout the world, each requiring their own Cyber Defense Network (CDN) in order to create, maintain, and share critical mission information. The physical infrastructure to provide connectivity between these commands will be the responsibility of the National Security Agency. It will be each commands responsibility to design, develop, and implement the hardware/software necessary to host a CDN capable of meeting a specific set of requirements.

Threats against the information maintained in this network can be expected from Red cyber-attack forces as well as from untrusted entities within each command. We must assume that the Red forces may have some knowledge of the GLG architecture, and that they may also have access via external hosts. Red forces can be expected to attempt to access the allied CDN and adversely impact allied operations by obtaining and/or manipulating information deemed critical to the allied mission. The Red forces are not expected to perform network availability attacks, as their operational doctrine favors surreptitious information exploitation over the more overt denial of service attack profile.[2]

This scenario laid the burden on each academy to define an adequate architecture and software implementation to support the mission. It also made clear that the objective of the Red Forces was one of security evaluation and data acquisition through compromise rather than a brute force attack. This scenario was played out at each academy based on providing the following requirements:

Requirements:

- *Headquarters has chosen email as its primary electronic means for communication. Implement email and establish means for forward deployed personnel (White Cell) to access email. These personnel will be required to use DoD PKI certificates for access and transport of sensitive information. They must be able to remotely utilize either web or application based email, therefore you must provide for both. Each local user must have an email account and capability to login and access machine utilities. HQs will establish 20-30 user accounts in order to distribute mission update information as required.*
- *It is critical for coalition partners to know the organization make-up of each command and be able to find contact information. Therefore you must provide a web based organizational chart and telephone and email directory.*
- *Situation Reports (SitRep) describing operational capabilities must be securely delivered electronically to xxxxx@.cdx.*
- *A supply database for each command must be locally managed based on updates provided by Headquarters. The database shall be updated on a daily basis and should be made statically available to each command. Supply officer at HQs must have edit capability. Updates to supply data will be sent daily via attachments to email.*
- *Establish a Local Registration Authority (LRA) to enable external users to download any local users public key certificate. HQs will need a way to push public certificates to each command's LRA providing means to initiate secure communications. This push must be executed using means other than email.*
- *Unless otherwise noted, all information deemed to be shared among outside commands should only be offered statically, outside commands must not be able to manipulate information.*
- *The mission will rely on the availability and integrity of all required information. Provide survivability to all aspects of information and functionality.*
- *Provide command leaders with audio and video conferencing on-line.*
- *The command standard for desktop is windows 2000.*
- *HQs will maintain the main DNS server. Each command must maintain a local DNS.*
- *Provide complete concept of operations, account information, network diagrams, and provided service to HQs.*
- *Be prepared for the unexpected. Establish means to evaluate the functionality and security of your local CDN. Establish means to monitor CDN activity and be prepared to respond with redundant functionality and report known compromises.*[2]

Students were warned to be prepared for the unexpected as anomalies were injected with absolutely no warning and the Red Forces owned a rogue box on each

[2] Inter-Service Academy Cyber-Defense Exercise Directive, dated 9 January 2003.

academy's CDN capable of launching stealthy attacks. The mission's success relied upon the availability and integrity of all required information and survivability of the networks functionality. In order to maintain an effect network over a one-week active period, students would have to design and build with information assurance as a cornerstone…something we all should be doing don't you think?

2.2 Schedule of Engagement

After months of hard work in analyzing the requirements, conceptualizing and defining a design, and implementing a functional product the time came to face the enemy. Although all involved were primed as always to start, glitches here and they make all involved wish for more time to prepare. Some students spend 20 hours per day in the lab during the weekends preceding the exercise. This level of effort is obviously put forth for more than just a grade.

Early in the academic year each academy agreed to a common week of attack in which students would stand watch in their respective labs throughout the day while the White Cell utilized their systems manually and by way of automated tools both locally and remotely and the Red Forces performed their art. In order to ensure a clean start, the White Cell started verifying functionality and services a few days prior to the exercise for any school interested. They helped trouble shoot and get everyone on same page to ensure the best fight for all. This proved to be extremely valuable because in the past two exercises the Red Forces were requested to hold back on the first day of activity while everyone made ready. It seemed no matter how much time was given, the final tweaking came down to the last minute for all involved. A valuable lesson in ensuring adequate testing prior to going live is learned by faculty and students alike.

During the evenings of the exercise, students spend their time recovering, thinking of new and eloquent solutions and back-up plans, and documenting the results of the day's exploits and modifications to their system's configurations. The effectiveness of their efforts will be reflected in the scoring.

2.3 Anomalies

Each day without warning, anomalies are injected into the scenario. These operational irregularities test the student teams' and/or their systems ability to react on the fly. They can be as complex as requiring each team to stand up an anonymous FTP server based on a commanders order to share information rapidly and readily to the other commands or as simplex as requiring a student to give up a system password as if someone was not diligent in providing password protection. They may include requiring all hands to man their battle stations such that no one is left to monitor logs and provide real time systems administration or they may be introduced as a piece of malicious software injected on a specific platform or service waiting for a specific time or event to execute. An anomaly may require a student user to load the latest intriguing piece of software made available via the Internet, which may introduce a new vulnerability, or it may require the student to fall back to an earlier version of software that is vulnerable to a well-known exploit. Whatever the anomaly, all participants are exposed equally and their actions, procedures and policies to address them are evaluated.

2.4 Organization

The *top-level architecture* of the CDX is shown in Figure 2. As indicated in the figure, each of the schools local area networks had two Virtual Private Network (VPN) nodes, one for providing services to each of the other participating schools, the White Cell and the Red Forces and another for the competing teams to evaluate their own systems from the vantage point of an outsider.

The use of the VPNs during the CDX provides an environment to conduct the exercise and to evaluate and "test drive" software before placing it into a production environment. It is intended to protect the integrity of the exercise as well as ensure any offensive measure taken by the Red Forces does not make it to the outside world. Any offensive action taken by the participating students is strictly prohibited and grounds for disqualification as only the Red Forces have the appropriate legal authority to attack.

White Cell members are located at each participating school to serve as a local referee and are directed by leadership located at a Headquarters stationed in Maryland. The White Cell uses a combination of automated tools and manual evaluation to determine service availability and the degree of compromise. They utilize a scoring criterion that invokes penalty points for loss of services and/or compromises and provides redemption points for effective reporting. Penalty points assessed for service degradation are dependent upon time of outage while penalty points assessed for compromise depend upon root or user level access. It is critical to have coverage remotely and on-site as well as to work closely with the Red Force leaders to ensure de-confliction between cause and effect.

2.5 Post-Exercise Deliberations

Upon the conclusion of the exercise the White Cell works closely with the Red Forces to certify the rank and order of each team and as a result the winner of the CDX. In addition, they document the results and accounts of the activities throughout the exercise to provide and after action report for each school. They also conduct a telephone conference with all interested participants, which serve as an effective venue for learning. This gives the students and faculty and opportunity find out all that the Red Forces knew and how successful or unsuccessful they were in exploiting their network. Sitting in on this meeting provides outstanding evidence to how effective an educational tool this exercise really has become. Undergraduate students demonstrate their understanding of computer science at the graduate studies level. Strategies and techniques employed by these students go on to serve as examples that the NSA and CERT utilize to teach to industry professionals.

3 Red Forces Organization and Activities.

The Red Forces provided the insider and outsider threat during the cyber defense exercise. They also were involved in providing valuable input to the White Cell during the planning and preparation phases. They are only limited in their tasks to avoid distributed Denial of Service (DoS) attacks to agreed upon times in the exercise since doing this early in the game could greatly the limit the learning experience for all involved.

3.1 Organization

While the White cell had elements at each of the Cyber Defense Network (CDN) nodes and Headquarters, the Red Forces were all gathered together operating at a location outside of Baltimore, Maryland. The Red Forces were linked to the CDX VPN and could see all of the traffic over the VPN linking the service academies together. They were on the network but were limited in privileges to services available to all coalition partners. They also ran a rogue machine at each academy for which they have administrative privileges. The intent of the rogue boxes was to throw off the participants in efforts to preclude them from filtering based on IP ranges. If they locked out IP ranges that required services they would be heavily penalized.

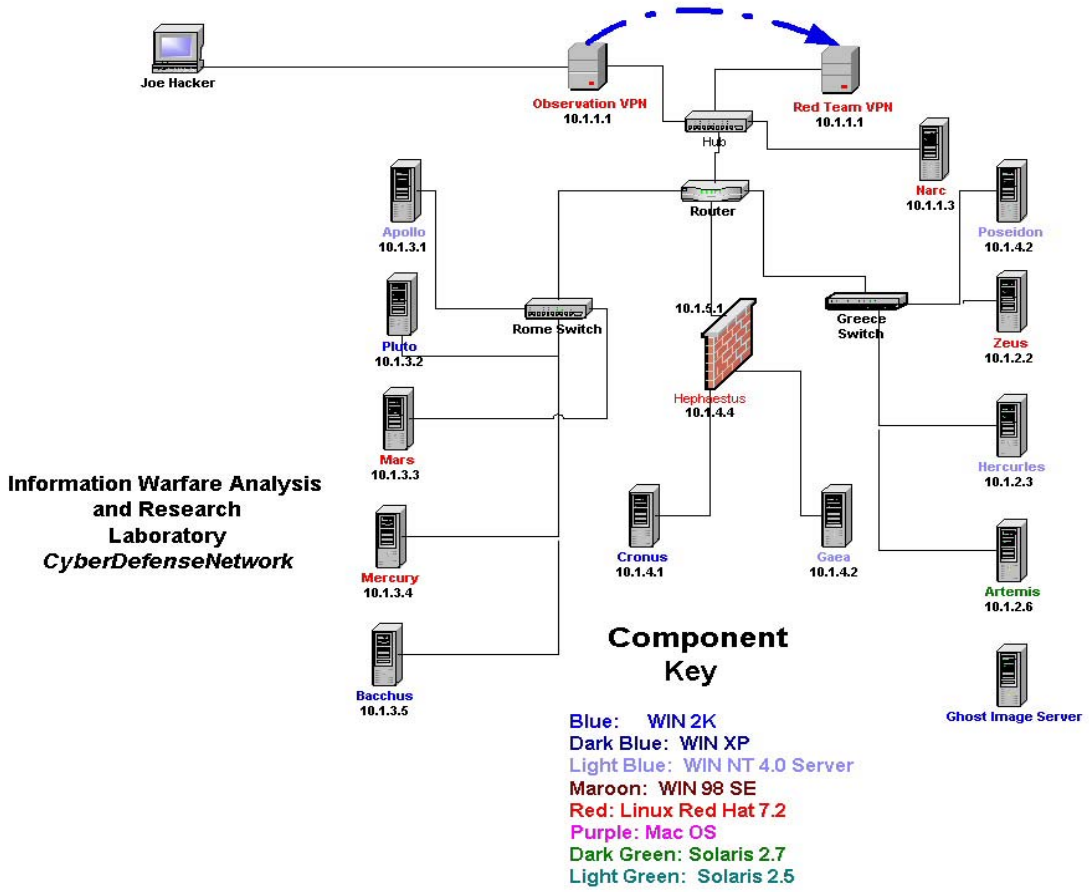

Figure 3. Cyber Defense Network circa 2002

3.2 Activities

Figure 3 shows the range of operating systems and network components used in CDX 2002. For CDX 2003, while all teams had the same hardware, each team could pick the operating system used to provide a required service. The Red Forces went through a sequence of activities to perform network intelligence gathering, execute intrusion attempts, conduct network attacks, and evaluate the effectiveness of their attacks.

A tcpdump file (about 500Mbytes) is available for the traffic over the net during the 2002 CDX. This data is almost totally malicious in nature since during the 2002 exercise the schools were required to provide a service but not to actively use the service. During 2003 there was considerably more non-malicious traffic over the net since all schools were required to use the net to submit periodic reports and send messages, traffic generators were utilized by the Red Forces to hide their attacks, and the White Cell actively exhausted the services required to be provided. However, technical problems prevented creation of a tcpdump file of the 2003 traffic. For the 2004 CDX we expect to again increase the friendly network traffic and a tcpdump file is expected to be available for the 2004 exercise. Contact either author to obtain the 2002 data.

4 Conclusions

In this paper, we have presented a summary of some of what is involved in executing a Cyber Defense Exercise. Lessons learned are plentiful and continue to help us make this a better experience for the participants each and every year. Students have repeatedly told us that the CDX is the best educational activity they have experienced at the USMA. Red Forces individuals have also repeatedly informed us that they have both enjoyed participating in the CDX as well as benefited professionally from participating in the CDX. The CDX has been made possible by extensive support from the National Security Agency (NSA) Public Key Infrastructure (PKI) Management Office.

The benefits of the CDX are realized both at the highest levels of the DoD as well as the lowest levels at the academies. For example, the excitement of the CDX coupled with West Point's 2001 and 2002 victories, sparked interest among the entire corp of cadets. As a result, the first ever student information assurance group was formed at West Point. The club, affiliated with the Association for Computing Machinery (ACM) Special Interest Group for Security Audit and Control (SIGSAC) has now grown to over 450 student members (over 10% of the entire corps of cadets) representing each of the 13 academic majors. The first student chapter of its kind, SIGSAC includes a wide range of interdisciplinary activities and has members from every academic department. In fact in there second year of existence they earned honors from IEEE as student chapter of the year.

The CDX has proven to be an effective vehicle in increasing information assurance awareness, facilitating ethical education and debate, providing leadership development opportunities and generating excitement in students for information assurance.

References

[1] J. Schafer, D. J. Ragsdale , J. R. Surdu, and C. A. Carver,"The IWAR range: a laboratory for undergraduate information assurance education," presented at Consortium for Computing in Small Colleges, Middlebury, Vermont, 2001.

[2] D. W. Welch, D. J. Ragsdale, and W. Schepens, "Training for Information Assurance," *IEEE Computer*, pp. 2-9, 2002.

[3] W.J. Schepens, D.W. Welch, and D.J. Ragsdale, "A Lesson in Cyber Defence," *Defence Systems International: Critical Information Systems*, June 2002.