2006-2009: CYBER DEFENSE COMPETITION

Douglas Jacobson, Iowa State University
Dr. Doug Jacobson Associate Professor Department of Electrical and Computer Engineering
Iowa State University Ames, IA 50011

Nate Evans, Iowa State University
Nate Evans Computer Engineering Student Department of Electrical and Computer Engineering
Iowa State University Ames, IA 50011

Cyber Defense Competition

Abstract

The world today is becoming more and more reliant on the use of information technology. Hence the world is becoming potentially more vulnerable to the loss of that technology. The lack of designed-in security and wide dissemination of hacker tools makes the prospect of asymmetrical threats very likely. To increase awareness and understanding of these and other security issues the Information Assurance Student Group and Iowa State University's Information Assurance Center created Cyber- Defense Competition (CDC). The Information Assurance Student Group organizes the competition and develops the scenario. The competition is held at a cyber security research facility at the university and the faculty members oversee the competition and provide the judging. The competition has been designed as a defense and survivability exercise where the participants need to minimize the risk of a security breech while ensuring necessary operational services are maintained. The competition is open to all students to promote a multidisciplinary approach since the information infrastructure is a multidisciplinary space. Teams participating in the exercise develop and implement security plans that safeguard their users and secure their networks. The students have several weeks to design and implement their defenses based on a scenario. The student teams (blue team) must then defend their network for 18 hours against a team of security professionals (red team). The students maintain a usable network and provide services to a group of users (green team). The green team provides a way to get others involved in the competition even if they are not computer experts. The first competition was held in the spring of 2005 and in the fall of 2005 the second competition was held. The spring of 2006 a regional competition will be held and student teams from other universities will be invited to participate. The competition consists of 12 teams of 3-4 students each. This paper discusses the planning and operation of the competition and the network environment used to ensure the attackers and students were isolated from the real internet. Feedback from the attackers and the students are presented along with lessons learned.

Introduction

Iowa State University has a robust program in computer security and offers a masters degree in information assurance. The university offered its first security course in 1995 and created a course on information warfare in 1996[1]. In addition to formal course work and faculty research projects we saw a need to develop opportunities to allow students to become involved in computer security. This led to the development of the Information Assurance Student Group which provides students an opportunity to meet and discuss security issues. The group also provides hands-on experiences for students where they learn how to secure wireless networks, install firewalls, and work with other tools. The students were looking for opportunities to try different security methods and to get experience with real attacks.

In February 2004 the National Science Foundation sponsored the Cyber Security Exercise Workshop[2] in San Antonio Texas. This workshop helped provide some guidelines for running Cyber Defense Competitions. The student group was enthusiastic about holding a competition at Iowa State University. They agreed to help plan the event and organize the student involvement.

There are several types of cyber competitions that have sprouted up over the last several years[3]. They range from capture the flag competitions where students try and hack into systems to gather information (the flag) to competitions where students configure a set of systems and then defend them. We wanted a competition that was both challenging and as close to realistic as possible. To that end we decided on a competition where the students were given a scenario and some equipment. They then needed to develop a plan to deploy the equipment and to install and configure the software. We also decided that the students needed to support users of their networks. We partnered with the local chapter of InfraGard[4] to help provide the hackers and some of the users. Many of the hackers are security professionals that are involved in white hat hacking.

This paper will describe the goals and objectives of the competition along with the teams and the scenario. A brief description of the student setups and the testbed network will also be provided. A narrative on the first two competitions including what worked and what did not work and a description of the future plans will also be provided.

Objectives

The purpose the Cyber-Defense Competition is to provide students with a simulation of real-life experiences with information assurance. Students play the role of the Blue Team, or information assurance professionals, under fire from the Red Team, simulating the hackers on a network. The White Team oversees the competition, judging (and scoring) each Blue Team based upon reports received from the Red and Green Teams. The Green Team effectively demonstrates the role of the general network users. The Blue Team with the fewest demerits at the end of the competition will be named the winner. Each member of the winning team is given a gift certificate to the book store for 100 dollars and their names on a plaque. The second place team members are each given a twenty dollar gift certificate.

One of the primary goals of the competition is to give students an opportunity to design a security plan to protect an organization based on a scenario. They must install, configure, and manage a wide range of security devices in order to carry out their security plan. This includes configuring systems straight "out of the box" and also reconfiguring legacy systems that may already exist in an organization. The students are given very few constraints on what they can do in designing their network. They must provide the services described in the scenario and keep their systems running during the competition. During the first competition we had 6 teams of 6 students each. During that first competition we noticed the teams were too large and that a larger number of smaller teams would work better. In the fall 2005 competition we had 11 teams of 4 students each. The students choose their own teams through a web based sign up sheet. The web site also provides the rules and scenario.

The information assurance student group (IASG)[5] organizes much of the competition. They are responsible for designing the rules, the scenario, and the scoring system. The IASG appoints a competition director who is responsible for many of the aspects of the competition. The director helps run the competition and answers questions about the rules during the setup time. The student teams are given three weeks prior to the competition to setup their security systems. The

setup will be discussed later. The IASG holds several educational sessions during the semester leading up to the competition in order to give interested students an opportunity to learn about typical defense systems. The information assurance faculty members help facilitate the competition and provide the resources needed to run the competition, like food, recruiting of the Red Team members, and leading the green and white teams. The resources used for the competition will be discussed later.

The scenario

Every student team is given the same scenario about a month before the competition, which describes the requirements and services they need to provide. The students use the scenario to help frame their security architecture. They are free to use any public domain technology to provide the services. The addition of the Green team helps keep the students focused on both providing security and providing a useable network. The scenario used for the fall 2005 competition is provided below. The scenario was modified from the spring 2005 competition based on feedback from spring and to keep past participants from having an advantage.

> CDC University is a small college in Metropolitan, Iowa. Until recently the campus has relied on the old fashioned methods of information exchange as there was never a push to implement technology beyond what the students brought with them. However the board of directors has recently decided that a computer network on the campus is inevitable and would provide many benefits to the curriculum at CDCU. The University has formed an Information Technology department, purchased equipment, and hired a team of network administrators to implement this network for them. This team is now responsible for the initial set up of the network.
>
> Given the small startup budget the university gave the Information Technology department, a less than generous amount of equipment has been purchased. However, this is a small network for a small campus so the board sees no need for additional equipment. No specific software requirements have been outlined by the board, however it is expected that whatever software is used does not add to the cost of the program or violate any copyright laws. This said the board will be happy with any implementation as long as it meets the following requirements:
>
> 1 A Web Server for www.cdcu.edu
> *The board has hired an outside web development team create the site, and will provide the network administration team with the content once the server is operational. The only requirements for this are that the web server be PHP compatible, as dynamic content on the pages will be developed in PHP. Resolution of www.cdcu.edu will need to handled by the network administration team. This means you will need to set up some sort of DNS.*
> 2 An Email Server for @cdcu.edu
> *This service will provide accounts for the students and staff with spam filtering and virus protection. A list of users will be provided (between 25 and 50 are expected for now). Additionally, configuration of cdcu.edu is needed, so that mail is directed to the appropriate address (DNS resolution). Users should be able to check email from both inside and outside the campus network using both POP and IMAP. The Administration*

Team is also expected to set up some sort of Web based e-mail system allowing users to access their accounts via a web browser.

3 A File Server

There is currently a ftp and smb server running by Professor Evans. This server needs to stay running as various faculty members need it for research and classroom instruction. This server can be patched for security purposes but it cannot be updated to a newer or different operating system due to faculty protests.

4 Remotely Accessible Programming Environment

The newly formed programming department requests remote access to a lab server so that students can work on C/C++ programming assignments. Users should be able to log in to this service via command line with the same credentials as above and compile simple C/C++ programs using GCC.

5 Firewall

To test security the board asks for the ability to shut off the firewall for small periods of times. This will allow a complete test of the internal security and help encourage board confidence in you and your setup. Please build in a switch to shutdown the all firewalls within 15 minutes for testing purposes.

6 Wireless

To increase the appeal of our school to students of the technical nature we ask that you set up a wireless access point that students can employ to access your network. You can use whatever you wish to secure this but we would prefer it to be a standard that is accessible to numerous students.

CDC Teams, rules, and scoring

A brief description of the four teams is listed below and a complete description is provided in appendix A.

The Blue Team consists of Iowa State University students playing the role of the information assurance professionals. The Blue Team must design a security architecture based on the scenario and defend against various security threats from the attackers. The Blue Team must also provide access to the network and services on the network to the users (Green Team).

The Red Team is comprised of professionals from the information assurance community playing the role of hackers. The Red Team is led by a team leader who is responsible for coordinating the Red Team activities. The Red Team provides most of its own computers and software. Any additional computing resources are provided. The Red Team has about 15 members. The Red Team must create and implement various attack strategies against the Blue or Green teams. The Red Team is also provided with several student scribes that help keep track of the attacks and aid in scoring.

The White Team is comprised of respected individuals from the information assurance community, such as professionals and cutting-edge developers. The team is led by the faculty coordinator and is the judging authority for the CDC.

The Green Team consists of members with various computer familiarity and skill levels. They play the role of typical network users. The Green Team provides two different functions during the competition. First they are there to score the Blue Team on which services are working (email, web, file sharing, etc.) The second function is to provide an opportunity for people who are visiting the competition to get involved. Some of the Green Team members sign up ahead of time, but many are just people who drop by to see what is going on. The Green Team duties include regular Internet usage and the execution of pre-defined anomalies. Anomalies are random events typical to real world situations. These events are injected into the system at various times throughout the competition. Anomalies are designed to test, or simply just complicate, the Blue Team duties during the competition.

Figure 1 shows an overview of the competition showing each team and how they are connected to the network. As shown in the figure each Blue Team provides a computer to be used by the Green Team which is attached directly to the blue team's network. In addition there are several computers for the Green Team to use to access the Blue Team networks from the outside. The White Team has computers setup to help monitor the traffic, receive email, and to introduce background traffic.

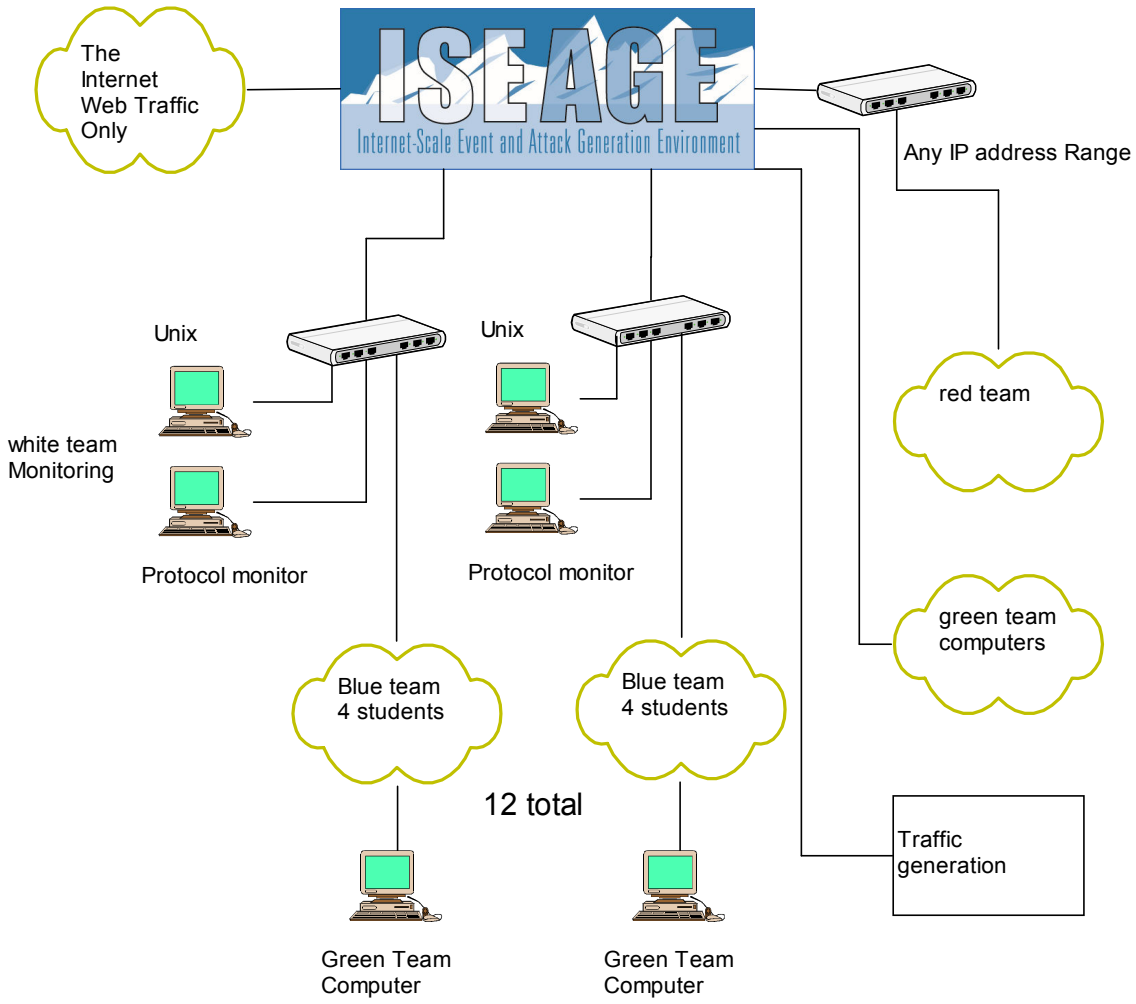

Figure 1 Competition network overview

The scoring system for the competition is based on demerits. Each team starts the competition with no demerits. The winning team is determined by whoever has the fewest demerits. Demerits will be added and subtracted from the team's score based on the criteria listed in Appendix B.

The testbed network

The cyber defense competition is held at the ISEAGE testbed network, which is housed at the Iowa State University research park in a 3000 sq. ft. facility. Iowa State University has created the **Internet-Scale Event and Attack Generation Environment** (ISEAGE)[6] (pronounced "ice age"). ISEAGE is a first of its kind facility in a public university dedicated to creating a virtual Internet for the purpose of researching, designing, and testing cyber defense mechanisms as well as analysis of cyber attacks. Unlike computer-based simulations, real attacks will be played out against real equipment. Researchers and vendors are working hard to provide products and services to help defend against cyber attacks, but users of these technologies often do not have any mechanisms to test or even try out these defenses. Law enforcement agencies and forensics analysts have no way to replay attacks or recreate a cyber crime scene. The ISEAGE facility provides a controlled environment where real world attacks can be played out against different configurations of equipment. ISEAGE contains a vast warehouse of attack tools that will be able to simulate point-to-point and distributed attacks. ISEAGE represents a new paradigm in the area of security research, cyber forensics, and will enable new and innovative research needed to solve the current security problems facing the world today.

Figure 2 shows a block diagram of ISEAGE and how it is connected to support the CDC. As shown in the figure, ISEAGE is a 64 node computer cluster that is capable of representing any IP address space. In addition to IP address space mapping, ISEAGE also provides tools to generate background traffic and background attacks. This helps create a realistic environment where not all traffic seen by the blue teams is coming from green or red teams. We also collected all of the traffic from the CDC and are using that in security research projects.

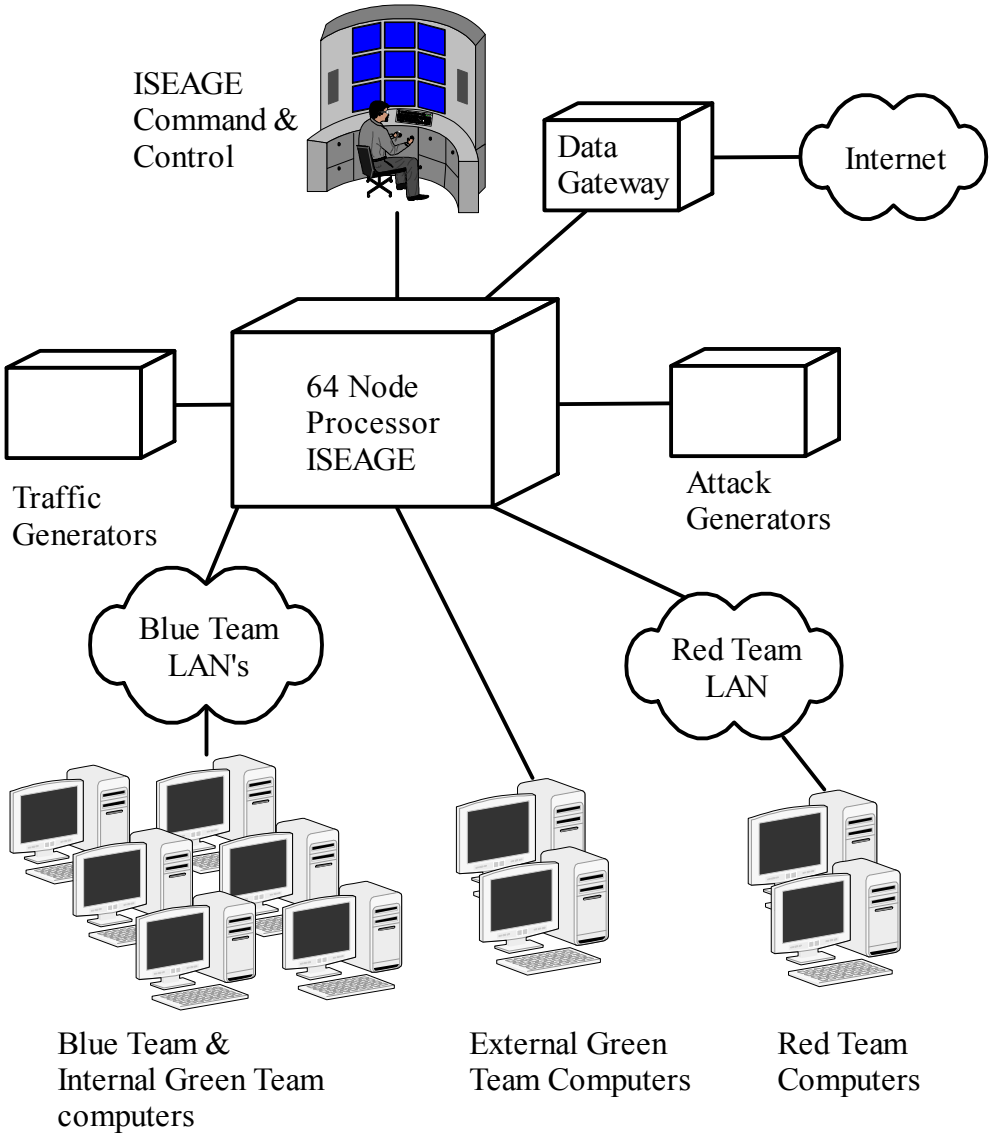

Figure 2. ISEAGE overview

Student setup

Each team is given a 10 foot by 10 foot cubicle with 9 computers, only the Macintosh and the pre-built legacy system have software installed. They also have several LCD monitors, keyboards, and mice. The also have a wireless access point. They must also configure and install an additional computer for the Green Team. This computer is housed in a different part of the facility but is wired into the inside of the blue team network. This computer allows the green team to be an inside user of the blue team network. The students are responsible for designing the network required to provide the scenario and the security system to protect the network. They are free to choose any public domain tool. There are given access to several Microsoft operating systems. During the setup they are given access to the Internet so they can download software. During the competition they only have web based access to the Internet through ISEAGE. Figure 3 shows a typical configuration of a blue team security system.

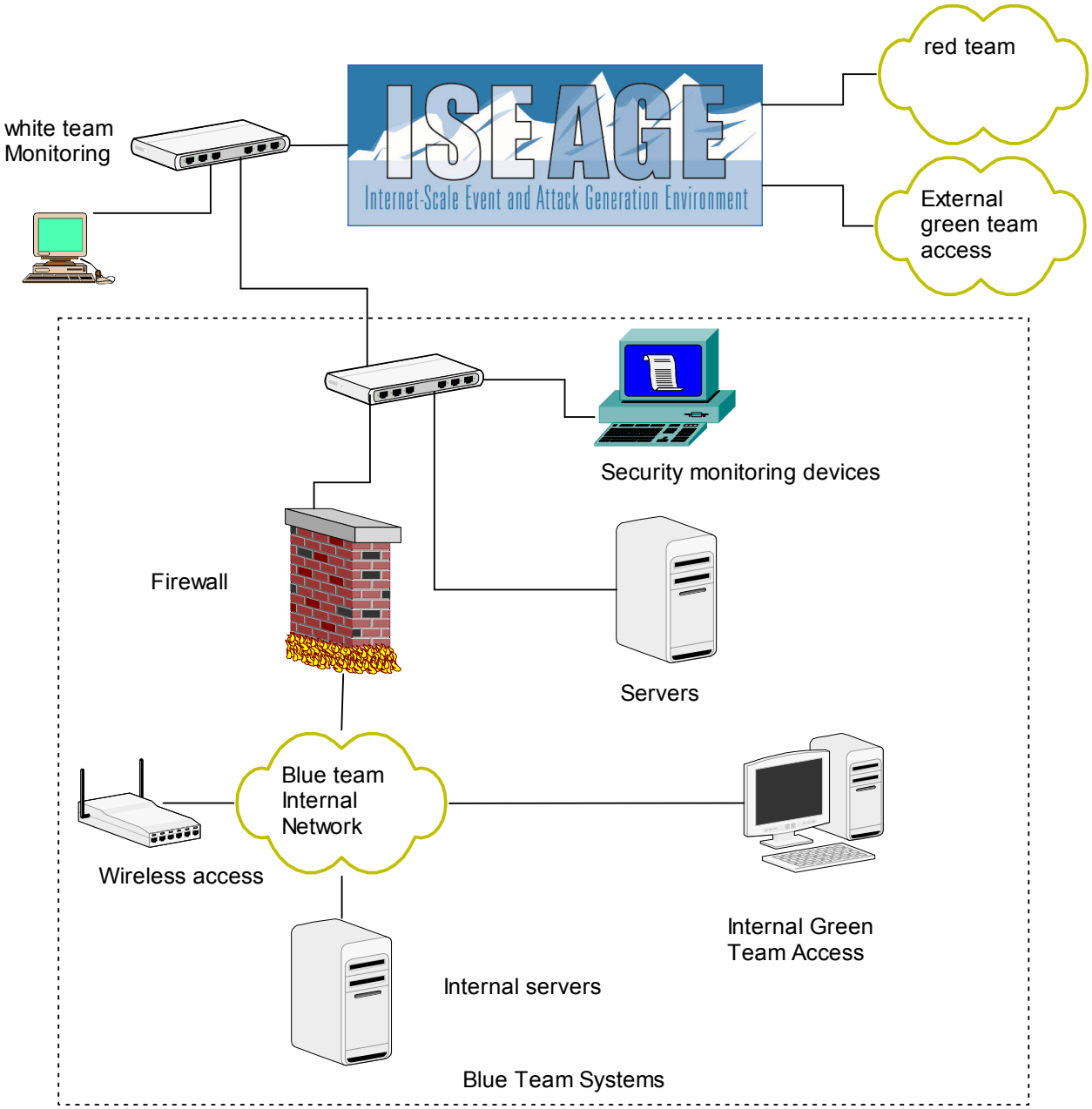

Figure 3. Typical Blue Team Configuration.

Each Blue team is given two IP address ranges as if they were connected to an Internet Service Provider. These addresses are not disclosed to the Red Team. The Red Team must find out on its own the addresses of the Blue Teams. Each Blue Team has a DNS server which is connected to the ISEAGE DNS server. The Red Team is given a large number of address ranges, which allowed them to change addresses several times during the competition. The White Team maintains a public email server that was used for the blue team members to send reports to the White Team. The White Team also ran a Peer to Peer file sharing system that was used during one of the anomalies.

As discussed above, the student teams are given access to the ISEAGE facility three weeks before the competition. The IASG provides students to help monitor the facility at night and to help provide access to supplies. The evening access schedule is posted in advance so students can plan their schedules. During the setup time the students can also access the internet directly. During the first competition we allowed the students to setup their computers right up to the start of the competition. The problem we encountered was that the students stayed up all night the day before the competition and therefore were unable to stay up the second night during the competition. For the second competition we closed the facility on Wednesday night and the reopened it at noon on Friday (the day of the competition). This also gave us a day to make the final changes to the ISEAGE configuration and to get the facility cleaned up and ready for the competition.

The competition

The competition started on a Friday at 6 pm and ran for 18 hours. The first competition was scheduled for 27 hours, but was shortened to 18 hours after feedback from the Red Team during the competition. After 18 hours the Red Team had managed to compromise most of the Blue Teams and everyone was getting tired. For the second competition the Red Team arrived at noon and started to set up and the students were also allowed in at noon. A rough schedule of the second competition is shown in the table below. The Green Team started to arrive about 5 pm. Many of the Green Team members were either students or IT and security professionals.

Times	Event
Friday November 18th	
5:00 PM	Introductions
5:30 PM	Dinner
6:00 PM	Start the 18 hour Event
11:00 PM	Pizza
Saturday, November 19th	
7:00 AM	Breakfast
11:00 AM	Red Team Scoring
12:00 PM	Lunch & Debriefing Session
1:00 PM	Awards

Table 1. Competition schedule

One of the challenges of running a competition is finding ways to keep non participants interested and entertained. We use several methods to provide an entertaining and educational experience. One of the focal points is the visualization system that shows the current scores and team standing along with real time traffic displays. Figure 4 shows the visualization display. The first competition had each team in two cubes that were configured to provide privacy for the teams. This configuration kept the Blue Team isolated from the spectators. In the second competition the cubes were reconfigured to open up on to a large open space. The new physical layout of the room also helped provide interaction between the blue teams and the spectators. This interaction not only keeps the spectators involved but also provides some amount of

distraction for the blue teams, which simulates real life. The Red Team was given a conference room where they could interact in private.

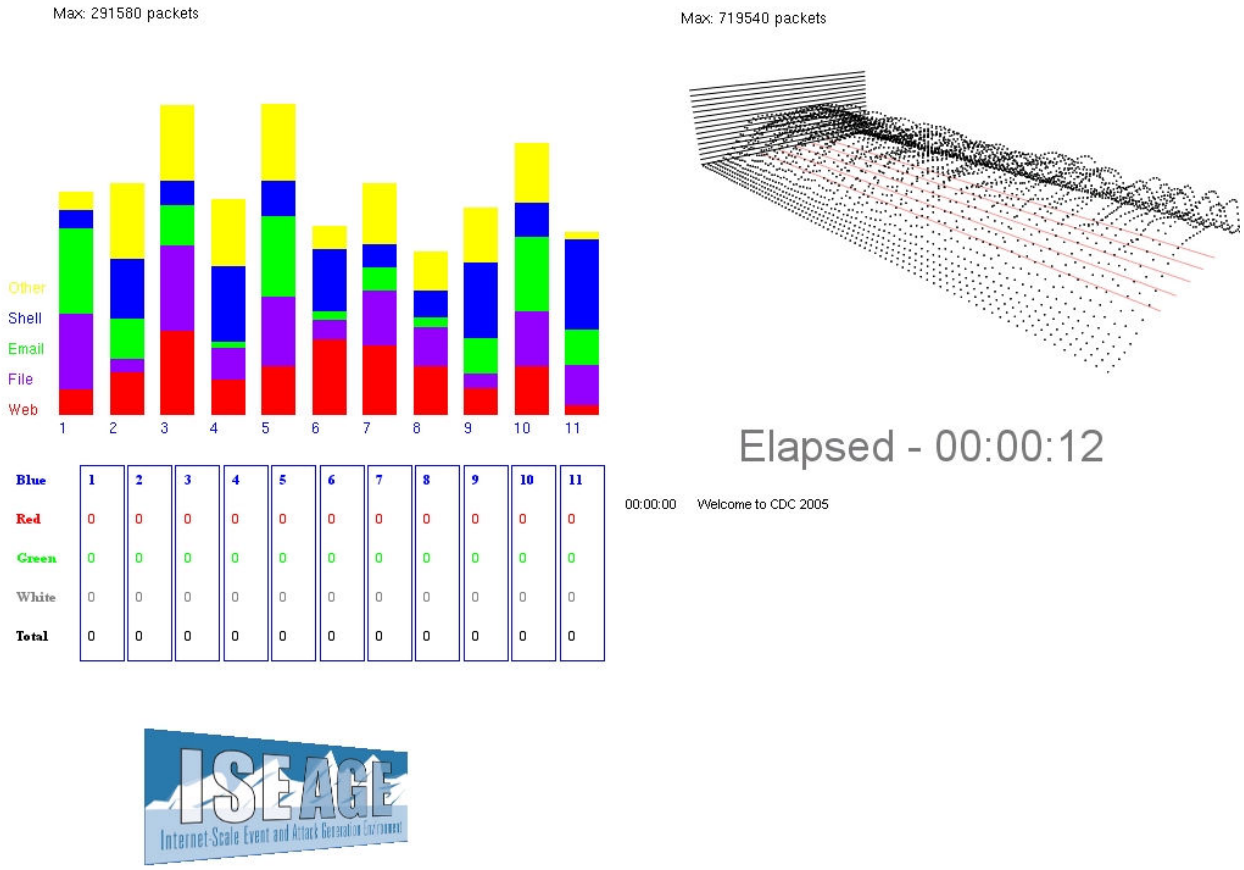

Figure 4. Visualization display

The competition starts off slowly while the Red Team starts to scan the network looking for systems to attack. The Green Team does not get started until about 30 minutes into the competition. In the second competition we added a Green Team leader who helped keep the Green on task and helped answer questions from the Green Team members. By around 8 pm the competition starts to heat up and the Red Team attacks start to take effect. It stays very crowded until around 11 PM when the Green Team members and spectators start to go home. The quiet time is from about 2 in the morning until 7 in the morning. However during this time several of Blue Team's networks are often compromised. Of course during the entire time the competition director is creating anomalies like fire drills, where every one in the Blue Team must leave the cube for about 15 minutes. At one point all of the teams are told to install peer to peer networking clients because the CIO of the university wants it. These anomalies help keep things exciting for the Blue Team and provide potential security vulnerabilities that the Red Team might exploit. The Red Team does not know about the anomalies. Table 2 provides a list of the anomalies used in the second competition.

- A fire drill, where the teams had to leave their cubes for about 15 minutes.
- Peer-to-peer software install, where the CIO gave them 45 minutes to install and connect to a peer-to-peer client outside their network.
- Provide remote desktop access to outside users
- Handle a traffic flood against their network
- Identify security changes after physical tampering of their networks
- Add new users with a certain amount of time.
- Change the passwords of current users to something simple.
- Turn off the firewalls

Table 2 List of anomalies

The competition starts to wind down around 9 AM and most of the security weaknesses have been discovered by the Red Team. Around 10 am all of the firewalls were turned off for one last attack by the Red Team. At 11 am the Red Team starts to compile the final score sheets which are added to the scores from the Green Team, and from the anomalies.

Once the Red Team has completed its scoring they have a debriefing session with the students. This gives the Red Team a chance to talk to the students about what they saw as hackers and a chance for the students to ask questions of the Red Team. This has been one of the highlights of the competition for both the students and the Red Team. During this time the white time adds up all of the scores and determines a winner. Once the Red Team has completed the debriefing every team is acknowledged and given a certificate. Then the winning teams are announced. During the second competition we also had a company install monitoring software into one of the Blue Team's networks. This software was designed to detect attacks. The company gave a short presentation on the software to the students.

In addition to the monetary prizes given to each member of the winning team, everyone is given a tee shirt. The Green Team and Red Team members along with many of the spectators are also given tee shirts. We also provided food for everyone attending the event. The total cost to run each event is about $3500 which does not include any of the equipment costs. The equipment costs are harder to identify since most of the equipment is part of the ISEAGE environment. Each Blue Team computer was purchased as parts and assembled by the students. This reduced the cost to under $350 per computer (not including monitors). With the network hubs, cables, monitors and other miscellaneous parts, the best estimate is about $5000 per Blue Team. The Red Team needed 6 computers plus monitors, and networking devices. The estimated cost for the Red Team equipment is about $5,000. The White Team needed just a couple of computers with an estimated cost of $1,000. This equipment can be reused for future competitions.

Conclusions, feedback, and next steps

This section highlights the results and feedback of the last two competitions and looks into the future of the competition. The competition has received a fair amount of press both local and national. This has helped to find corporate sponsors of the competition. One of the issues is how to use the corporate sponsors. To date companies have sent people to be part of the Red and Green Teams. We have had companies ask about using their technology in the competition. We

will consider this on a case by case basis. One of the issues with using company technologies is the students might not have the experience they gain from installing their own public domain software.

As far as the actual competitions we have several issues that have come up in both competitions that need to be addressed. One of the issues is the use of wireless technologies. We added wireless to the second competition but there was no Green Team use of the wireless access points and very little wireless traffic was produced during the competition. Therefore the Red Team was unable to take advantage of the vulnerabilities of wireless networks. For the next competition the White Team will produce wireless traffic to each of the Blue Teams.

There has been differing views on the length of the competition. The first year we tried to go 27 hours and quit after 18 hours. The second competition was scheduled for 18 hours, but the last couple of hours very few new attacks took place. With more than fifteen attackers focusing on 11 teams most successful attacks were discovered within 12 hours. We need to rethink the length of the event, most students like the idea of a long event. We are working on ways to provide either a shorter event or providing anomalies or other challenges toward the end of the competition.

Another issue that has been brought up by the Red team is that the Blue Team's environment is unrealistic. This led to the introduction of the legacy system during the second competition. However, the Blue Teams where disabling user accounts and blocking access to entire subnets during the competition. In the real world these actions would not be allowed. We plan on working with the Red Team to develop a set of rules that govern what the Blue Team can do. One idea is to introduce a CIO for each Blue Team that must approve certain actions. This could be done by email and the White Team would act as CIO for each team.

We had several teams that failed to have all services running before the competition started which caused them a large number of demerits and also made it difficult for the Red Team to attack when some teams had almost no services running. For the next competition we are planning on having the Green Team start first before the Red Team starts. They will help verify all services are running.

In spite of the issues raised above, the overall feedback from the competition is very positive. An informal survey of the Red and Green team members indicated they will be back for the next competition. We have also been contacted by several companies that want to be involved in the next competition. The feedback from the students was overwhelmingly positive. The competition gives them a change to use real tools in a live fire exercise. Given the number of hours the students put into the exercise and the level of commitment defending their networks we have to conclude the competition is a great success. It was great to see almost 50 students working together to solve some very complex problems in a short period of time. It also helps create a cooperative atmosphere among the students interested in security when we had over 20 students as Green Team members.

The red team, blue team and the green teams were given an informal survey after the event. The surveys provided an opportunity to provide written feedback was well as answering several

questions. The teams were asked to comment on the timing, difficulty, length, fairness, documents, success, benefit, social aspect and the green team aspect. On a five point scale the teams rated the successfulness of the competition as a 4.53 and on the question would they participate in the next CDC 90% indicated they would participate. In the competition we held last spring (Spring '05), teams commented that the competition was too long (2.88) and the timing was bad being the week before finals (2.00), so we focused on fixing these for the next competition. During that competition (Fall '05) the biggest two complaints concerned the green team handling (2.67) and the documents produced (2.89) while the benefit (4.5) and success (4.8) of the event stayed very high.

Our plans for the future are three fold. We will hold a regional competition in the spring of 2006. Work is under way to create a network environment that can be remotely configured and run. This way the teams from the other schools will be able to work on their designs as if they were in Ames Iowa. They will come to ISU for the actual competition. We will then hold the ISU competitions in the fall semesters and the regional competition in the spring.

We are also planning several competitions for local IT professionals. This competition would be different in that each team would be both Blue and Red. They would remotely configure their defenses and then during the competition they would both attack other teams and defend their own network from attacks. We are planning at least two competitions during 2006, one for the ISU IT professionals and one for members of InfraGard.

Work is also underway to create a high school competition with the goal of getting more kids interested in computer security. This competition would be modeled after the college CDC. The first year we are targeting 12 schools. Each school will have an industrial mentor and will receive instruction from ISU for several weeks prior to the competition. They will access the competition equipment remotely and will travel to Ames for the competition. Each school will be given 2 to 3 computers that they will keep, for the students to experiment with different security mechanisms. It is out hope that this competition will grow into larger event with possibly regional competitions feeding in to a state competition.

Our only real concern is how to handle the increased demands on the Red Teams and the ISEAGE facilities if we start to run a large number of competitions a year. We do believe these types of competitions provide a valuable learning experience for the participants (students, faculty, IT professionals, and the general public).

Appendix A: Team Rules

Blue Team:

The Blue Team rules and responsibilities are listed below:

I. Each team will consist of 3- 4 students enrolled at Iowa State University in at least a part time status.
II. Each team will be required to run a major service on all three Operating Systems: Macintosh, Windows, and Linux/ UNIX. They are also required to run a re-built

legacy image and an "unsecure" OS of the team's choice. The version does not matter but it must fit within guidelines for allowed software.

III. Each team will be provided with the same hardware.
   a. Hardware List 9 Desktop Computers (1 Macintosh, 8 IBM compatibles) Hubs Ethernet Cable Power Strips Extra NICs Monitors
   b. Additional Hardware may be added to a team's equipment if approved by the White Team and the director by the first day of the competition.
   c. All supplied hardware is the responsibility of each Blue Team and must be returned in the condition issued at the end of the competition. If the hardware becomes damaged while under Blue Team responsibility, they need to contact the director immediately.
   d. If hardware breaks during the competition it can be replaced with a penalty determined by the scoring guidelines.

IV. One computer must be set aside for Green Team access. This computer cannot be monitored physically, but can undergo monitoring through digital means.

V. Each Blue Team will receive the assignment 60 days in advance from the Attack Phase of the CDC and will be allowed to setup their hardware immediately.

VI. Each Blue Team will be required to submit a report before the "Attack Phase" detailing their network setup. This document will explain while certain choices were made from a security standpoint and will include supportive diagrams.

VII. After each attack the Blue Team has the opportunity to submit a report detailing the attack that will be used to determine scoring.

VIII. After the activity each team will also be requested to submit a report entailing how vulnerabilities where caught and anomalies handled. This final report will be used to determine the winner of the competition in the situation of a tie.

IX. The Blue Team cannot perform any offensive actions towards any other team. Doing so will disqualify that team from the competition.

X. All software used must be on the list provided to each team or personally created by a member of the team. Software which was created by a member of the team must be documented and sent to the CDC committee before the competition.

XI. The Blue team is not allowed to receive or request assistance from anyone not registered on the Blue Team.

Red Team

The Red Team rules and responsibilities are listed below:

I. Red Team candidates are skilled members of the Information Assurance community and selected by the competition director and faculty advisor.

II. Fill out the Attack Evaluation form for each successful attack. This form will be provided at the competition. A student scribe is provided to aid in the filling out the form.

III. No personal contact with the Green Team or Blue Team is allowed within the context of the competition. Internet-related communication is appropriate (such as email, etc).

IV. No DDOS attacks can be used against any team.

V. Offensive security breaches are limited to the testbed (ISEAGE) environment.

VI. A final evaluation of each Blue Team must to be filled out by the Red Team at the end of the competition. This form will be provided at the competition.
VII. The Red Team will hold a debriefing session at the end of the competition to talk about the attacks and to answer any questions from the teams.

White Team

The White Team rules and responsibilities are listed below:

I. White Team candidates are faculty or skilled members of the Information Assurance community.
II. The duties of the White Team do not permit aiding or assisting any team in accomplishing tasks.
III. One member of the White Team must be monitoring the CDC at any given time.
IV. The White Team is responsible for scoring updates throughout the event.

Green Team

The Green Team rules and responsibilities are listed below:

I. Green Team candidates consist of a variety of different computer familiarity and skill level backgrounds.
II. The Green Team is expected to complete daily activities (such as checking e-mail, general internet browsing, etc), but are not limited in activities. This team can even attempt to attack systems on their own.
III. Fill out a Usability Form hourly. This form will be provided at the competition and must be completed within a 15- minute time period.
IV. The Green Team must be responsible for the initiation and testing of the predefined anomalies.
V. Green Team users may only log in under their assigned User ID.

Appendix B: Scoring

Demerits will be added and subtracted from the team's score through 1 of the 6 criteria listed below:

I. Before the competition, each team must submit a report detailing their respective system setup. This submission will detail each team's specific design choices regarding information security and should include complementary diagrams (network diagrams etc) explaining their setup. If the report is not completed and submitted by the start of the competition, a penalty of up to 250 demerits will be applied to that team's score. This penalty will be determined by the White Team, which will review each submission individually to determine the necessity (and extent) of penalty.
II. Blue Teams will be penalized rule infraction at White Team discretion. There will be no limit to the amount of demerits a team may be penalized in this way.

A. All hardware used in the CDC must be included in the Approved Hardware List. Team leaders are allowed to introduce new hardware with the approval of both the White Team and the competition director.
B. Penalty of up to 250 demerits per offending device found will be added to the team's score. Additionally, the illegal device will be removed from the competition.
C. All software used to participate in the CDC must be included in the Approved Software List. Team leaders are allowed to introduce new software with the approval of both the White Team and the competition director. A penalty of up to 250 demerits per offending software incident found will be added to the team's score. Additionally, the illegal software will be deleted.
D. If a team has a hardware failure in a machine, that team will have one hour to get the machine back online. If more then one hour is taken, a penalty of 50 demerits per hour will be added to that team's score. All other penalties still apply during this time. The one-hour grace period privilege may be relinquished or extended at the discretion of the White Team.
E. Faculty, staff and moderating personal are limited to "background" support during the attack phase of the CDC. Background support is defined as any task that does not give an unfair advantage to any Blue Team. If the White Team determines a violation of the code has occurred then the offending team will be applied a penalty of 200 demerits.

III. A Blue Team can be penalized for not providing the services listed on the scenario. These services include (but are not necessarily limited to): web serving, file serving, email, remotely accessible programming environment and routable Internet to the clients. For each service that is unavailable, demerits will be added to that team's score. The amount of demerits added will be based on the list below and determined by the Green Team's reports. The maximum amount a team can be penalized in this way is 700 demerits.
   A. If a service is degraded or down for less then one hour then a 50 point penalty will apply. The appropriate demerit penalty will be determined by the White Team (based upon the Green Team reports).
   B. If a service is degraded of down for 1-3 hours consecutively, 100 demerits will be added to the team's score.
   C. If a service is degraded of down for more then 3 hours consecutively, 200 demerits will be added to the team's score.

IV. Teams will be subject to demerits based on Green Team usability reports. A maximum of 400 demerits can be applied in this way.

V. The team can be penalized with demerits as vulnerabilities are found and exploited. The White Team, based on the Red Team's final evaluation of each team, will determine the amount of demerits added. A maximum of 700 demerits can be penalized in the way.

VI. If a member of the Red Team intercepts and reads the Blue Team's incident report, a penalty of 50 demerits will be added to the team's score (per each report read).

A team may also improve their score in one of two ways. This means demerits will be subtracted from the teams score. The following actions will result in scoring:

I. Effective dealing of "Anomalies" will improve a team's score by 50 demerits per anomaly.

II. Each team is allowed to reduce the penalty applied from part V above by up to 50%. This is done by submitting a report via e-mail to the White Team. This report must contain 4 headings explaining the intrusion through the following conventions: Type of Attack (port, vulnerability), Response Taken, Information about the attacker (IP address, MAC address, OS) and expected activity from the attacker. The amount the penalty reduction is determined by the White Team and based upon the reports from the Blue and Red Teams (assuming the reports were not intercepted).

Bibliography

1. Doug Jacobson, "Teaching Information Warfare with a Break-in Laboratory", Proceedings of the 2004 American Society for Engineering Education, Salt Lake City, June 2004.
2. L.J. Hoffman and D. Ragsdale, "Exploring a National Cyber Security Exercise for Colleges and Universities", tech. report CSPRI-04-08, Cyber Security Policy and Research Inst. Aug 2004, www.cpi.seas.gwu.edu/library/docs/2004-08.pdf
3. L.J Hoffman and D. Ragsdale, "Exploring a National Cybersecurity Exercise for Universities", IEEE Security and Privacy, Volume 3, Number 5, September 2005, pg27-33.
4. InfraGard, www.infragard.net
5. Iowa State University Information Assurance Student Group, http://iasg.ece.iastate.edu
6. ISEAGE, www.iac.iastate.edu/iseage