



***Collegiate Cyber  
Defense Competition***

**2007 State of Illinois Competition  
Team Packet**

**Ver 1.0**

*Hosted by*

**Information Systems and Applied Technologies**

**at**

**Southern Illinois University Carbondale**

*“Security Is Not Just Technology”*



## Table of Contents

|   |           |
|---|-----------|
| <b>History .....</b>                        | <b>3</b>  |
| <b>IL-CCDC Mission and Objectives .....</b> | <b>3</b>  |
| <b>Overview.....</b>                        | <b>4</b>  |
| <b>Game Scenario .....</b>                  | <b>5</b>  |
| <b>Network Description .....</b>            | <b>5</b>  |
| <b>Scoring.....</b>                         | <b>10</b> |
| <b>FAQs .....</b>                           | <b>11</b> |



***Collegiate Cyber  
Defense Competition***

## History

In February, 2004, a group of educators, students, government and industry representatives gathered in San Antonio, Texas, to discuss the feasibility and desirability of establishing regular cyber security exercises with a uniform structure for post-secondary level students. During their discussions this group suggested the goals of creating a uniform structure for cyber security exercises might include the following:

1. Providing a template from which any educational institution can build a cyber security exercise
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

The group also identified concerns related to limiting participation to post-secondary students, creating a level playing field to eliminate possible advantages due to hardware and bandwidth differences, having a clear set of rules, implementing a fair and impartial scoring system, and addressing possible legal concerns. In an effort to help facilitate the development of a regular, national level cyber security exercise, the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio hosted the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region in April 2005. While similar to other cyber defense competitions in many aspects, the CCDC is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. While other exercises examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester, this competition is focused on the operational task of assuming administrative and protective duties for an existing “commercial” network.

In the Spring of 2006, through support from the National Science Foundation, the Department of Homeland Security, and many industry sponsors, four Regional Cyber Defense Competitions were held. The winning teams from these competitions and a team from West Point representing the United States armed services competed in the first national Cyber Defense Competition hosted by the originators of the event at University of Texas at San Antonio.

The extreme popularity of the event led the organizers to expand the competition to begin at the State level. Winners of the state competitions will be invited to their regional event. Once again regional competition winners will compete for the National title in San Antonio.

The State of Illinois Collegiate Cyber Defense Competition (IL-CCDC) will invite 6 teams to compete on the campus of Southern Illinois University Carbondale February 23-25, 2007. The winner of this event will face other state winning teams from Minnesota, Wisconsin, Michigan, Iowa, and Indiana at the Center for Systems Security and Information Assurance at Moraine Valley Community College in April.



## IL-CCDC Mission and Objectives

### Mission

The Collegiate Cyber Defense Competition (CCDC) provides institutions with an information assurance or computer security curriculum a controlled competitive environment to assess their student's depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems.

### Event Objectives

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs.
- Provide an educational venue in which students are able to apply the theory and skills they have learned in their course work;
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams;
- Open a dialog and awareness among participating institutions and students.
- Have fun!

## Overview

Teams will be scored based on their ability to detect and respond to outside threats, maintain availability of existing services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs.

### Competition Team Identification:

- Blue Teams - the student team representing an academic institution who will compete in the IL-CCDC
- Red Team – unbiased information security professionals from commercial, military, or governmental organizations who have volunteered their skills to assist in the assessment of a team's ability to defend their network and services. This team on a periodic basis will probe, scan, and attempt to penetrate Blue Team networks. SAVVIS, Inc. will be organizing this team.
- White Team – the group who will serve as room judges and referees in the various competition rooms. This group will be composed of information security academics from the competing institutions and industry representatives. Each competing team will have a White Team member on a rotational basis who will assess the competition team's ability to maintain their networks and service availability based upon a business inject and a scoring instrument.



**Collegiate Cyber  
Defense Competition**

Gold Team – the competition administration composed of faculty and industry professionals who will conduct the exercise. They will be responsible for administering the competition from the master scenario event list, injecting business process events and handle or mediate challenges.

To provide an equitable, fair and even playing field:

- Each team will begin with an identical set of hardware and software: Each team will be given an existing network with 6 servers and 2 clients they must secure and maintain.
- Each team will be located on a dedicated internal network: To remove the variables associated with VPNs and propagation delay each team's network will be connected to a competition network allowing equal bandwidth and access for scoring and red team operations. This also allows tight control over competition traffic.
- Each team will be given the same set of business requirements that must be provided and corporate standards which must be adhered to.
- Each team will be challenged with required business injects (tasks) at the same time during the course of the competition. Teams must adhere to corporate standards while performing the "injects" and mitigating any resulting security threat.
- Only team members and White/Gold Team members will be allowed inside their competition room.
- Each team will be assigned their own room during the competition and only the members of the certified student team will be allowed inside during the competition. This eliminates the potential influence of coaches or mentors during the competition.
- Only team captains will be allowed in the White/Gold Team room.
- Each team's external client will be located in the White/Gold Team room and will occasionally be used to assess business injects.
- A non-biased Red Team will be used: A volunteer, commercially experienced Red Team will be used during the competition.

## Game Scenario

Each team is made up of a group of information technology professionals employed by Edeeyes, an information services consultancy that provides various levels of service to their customers. In this case the customer is Crapht Foods International, and they have decided to outsource the majority of their networking, client/server administration, and security needs to Edeeyes. Edeeyes has agreed to a service level agreement that will provide 99.999% availability for all services. The White Team will represent the Crapht Foods CEO's executive management team, and the Gold Team will represent Crapht Foods corporate IT services group.



## Network Description

The competition network will be completely standalone with no external connectivity. All networks will be connected to a central router that will be maintained by the Gold Team.

The anticipated equipment list per team room will be.

- a. 6 servers
- b. 2 clients
- c. 1 switch
- d. 1 router

(Note: General documentation of team networks will be provided upon equipment finalization prior to the competition. This will include connectivity, domain names, URLs, specific IP addresses for services, etc.)

Each team network will be connected to the central router through their own individual router. Each team will be provided with a standalone PC with Internet access that may be used for research, software downloads, etc. At no time will the Internet access PCs be connected to the competition networks.

Each team will be provided with a CD-folder and thumb drive set containing the software, drivers, and data necessary to administer each site. (Note: The exact composition of this software set will be distributed via the website.)

Note: Reloading of systems is allowed, however, the scoring engine begins monitoring the moment the teams enter their rooms. Also, the teams are not allowed to perform major release upgrades of licensed software (i.e. Microsoft, Oracle), however, patching is permitted.



## Schedule

### **Monday – February 19 through Thursday – February 22, 2007**

Gold-Team – pre-competition preparations.

### **Friday – February 23, 2007**

12:00 PM

Registration opens. Teams will be registered at the College of Applied Sciences and Arts SIUC. Please report to Engineering A131 Alumni Lounge.

12:45 PM

Opening announcements and room selection. Teams led into their rooms.

1:00 PM

Competition Begins

5:30 PM – 7:00 PM

Dinner available in “Commissary” ASA 224.

9:00 PM

Day 1 of Competition Ends



**Collegiate Cyber  
Defense Competition**

**Saturday – February 24, 2007**

7:45AM

Teams gather in Engineering A131 Alumni Lounge. Announcements for day two.

8:00 AM

Day 2 of Competition Starts

11:30 PM - 1:30 PM

Lunch available in “Commissary” ASA 224.

5:30 PM – 7:00 PM

Dinner available in “Commissary” ASA 224.

8:00 PM

Competition ends

**Sunday – February 25, 2007**

10 AM – 1:00 PM Carbondale Civic Center, 200 South University, Carbondale.

Debriefing, presentations, banquet and awards.

10:00 – 11:00 Debrief from the Red Team. They will review attacks that were successful and make suggestions for future improvements.

11:00 – 12:00 One or more presentations from security experts, from sponsor companies, others.

12:00 – 1:00 Awards and luncheon



*Collegiate Cyber  
Defense Competition*

## Competition Rules

### Overview

The competition is designed to test each student team's ability to secure a corporate network while meeting the established business requirements. The scenario involves team members simulating a group of employees from Edeeyes, Inc., an information services consultancy, that has agreed to provide the majority of the information technology services required by Crapht Foods International for their remote sites. The teams are expected to manage the computer network, keep it operational, and control/prevent any unauthorized access. Each team will be expected to maintain and provide all required services. The objective of the competition is to measure a team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations, policy, and procedures. A technical success that adversely impacts the business operation will result in a lower score as will a business success which results in security weaknesses. A detailed business scenario, organizational chart, business requirements, corporate standards, and service level agreement will be distributed along with technical specifications prior to the exercise to allow teams to develop their team and capabilities.

### Competition Play

- All teams are connected to a central router and scoring system.
- Each student team will appoint an official Team Captain who will handle all official inquiries for their team during the competition and protests. This is the only member of the team allowed in the White/Gold Team room.
- A Red Team provided by SAVVIS, Inc. will attempt to infiltrate or disrupt each team's daily operations throughout the competition.
- White Team – the group who will serve as room judges and referees in the various competition rooms. This group will be composed of information security academics from the competing institutions and industry representatives. Each competing team will provide two White Team members who will assess the competition team's ability to maintain their networks and service availability based upon a business inject and a scoring instrument. The Chief Judge and Referee provided by LURHQ will have final authority.
- Gold Team – the competition administration composed of faculty and industry professionals who will conduct the exercise. They will be responsible for administering the competition from the master scenario event list, injecting business process events and handle or mediate challenges.
- Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks in timely manner that will be provided throughout the competition.



- All team members will wear identification badges identifying team affiliation at all times.
- Student team members will not initiate any contact with members of the Red or Gold Team during the hours of live competition.
- Student team members will not enter another team's competition workspace.
- The competition will run over a two day period. (Friday 1pm – 9pm and Saturday 8am – 8pm). Registration will occur on Friday between 12 – 12:55pm.
- Students will be encouraged to monitor the services they are providing in order to ensure they are meeting the service level agreement. Teams may be notified by their “customer” that a service appears to be unavailable.
- Protests by any team will be presented by the Team Captain to their assigned White Team representative as soon as possible. The Chief Judge in consultation with the Gold Team Captain will be the final arbitrators for any protests or questions arising before, during, or after the competition.
- Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a lower score. Should any question arise about specific scripts or how they are functioning, the school's team captain should immediately contact the Gold Team (competition officials) via their White Team representative to address the issue.
- Any team that tampers with or interferes with the scoring or operations of another team's systems will be **“fired” (a.k.a. disqualified)**.
- Team captains are encouraged to work with the contest staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins.
- No additional computers, PDAs, thumb drives, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition. Any violation of these rules will result in disqualification of the team member and a point penalty assigned to the appropriate team.
- Under no circumstances will any Blue Team machines be connected to the Internet, other than the one that has been provided in each team's room. The campus area network will be monitored closely for this activity.

Teams are strongly encouraged to provide incident reports for each red team incident they detect. Incident reports can be completed as needed throughout the competition and presented to the White Team representative for collection.



- Student teams will be given identical hardware and software installations to configure and support.
- Student teams will be provided the system architecture and initial set-up prior to the event to permit planning.
- Student teams (a.k.a. Edeeyes, Inc) should not assume any system is properly functioning or secure. They are assuming the roles of contracted systems administrators and are assuming responsibility for each of their systems.
- Reloading of systems is allowed, however, the scoring engine begins monitoring the moment the teams enter their rooms.
- Teams are not allowed to perform major release upgrades of licensed software (i.e. Microsoft, Oracle), however, patching is permitted.
- Student teams must maintain specific services on the “public” IP addresses assigned to their team.
- All IP Addressing will be between 127.0.0.1 and 255.255.255.255. This includes all “private” (PAT/NAT) internal addressing.
- Current network and system documentation must be maintained by each team and may be requested at any time during the competition for auditing purposes by the White Team. Inaccuracies will result in score deductions. Basic criteria for this documentation will be provided to the teams prior to the competition.

## Student Teams

- Each student team will consist of up to eight (8) members. Each team member must be at the minimum a half time student of the institution the team is representing. To qualify, the team member must be enrolled in 6 or more semester credit hours for undergraduates and 4 or more semester credit hours for graduate students during the semester the competition is held. Student cannot be employed full time as a security professional.
- Each team may have one faculty advisor present. The faculty advisor may not assist or advise the student team during the competition.
- Teams will be given basic details about the network configuration prior the competition.
- Each student team will designate a Team Captain for the duration of the competition and a team liaison to act as the focal contact point between the competition staff and the teams before the competition. The team captain and the team liaison may be the same individual, but both must be members of the student team at the competition.
- The team captain is the only team member that will be allowed in the White/Gold Team room.
- Teams will be issued badges which must be worn at all times by team members while inside the College of Applied Sciences and Arts.



**Collegiate Cyber  
Defense Competition**

## Scoring

The winner will be based on the highest score maintained during the approximately 20 total hours of competition time. During this competition each team will start with a pre-determined number of points, which will represent the 500,000 Euros Edeeyes received from Crapht Foods International as payment for contracted services. Points (a.k.a. Euros) will be subtracted for not meeting business requirements, following corporate standards, or not meeting the service level agreement. The team that is most capable of meeting the requirements of the contract, and losing the least amount of Euros, wins.

- Functional services (based on random polling of required services): Some Red Team attacks will be tracked through service availability monitoring.

Successful completion of business injects: Awarded points will vary by task.

### Functional Services

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate. Services may include but are not limited to:

#### HTTP

A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

#### HTTPS

A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

#### SMTP

Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points.

#### SQL

An SQL request will be made to the database server. The result will be stored and compared against an expected result. Each successfully served SQL request will be awarded points.

#### DNS

DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.



## Business Tasks

Throughout the competition, each team will be presented with identical business taskings. Points will be awarded based upon successful completion of each business task or part of a tasking. Tasks will vary in nature and points will be weighted based upon the difficulty and time sensitivity of the assignment. Tasks may contain multiple parts with point values assigned to each specific part of the tasking.

Some examples:

- Creating/enabling new user accounts to support staffing changes
- Installing new infrastructure hardware to support changes to corporate standards
- Implementing new services to meet new business requirements

Each business tasking will have point values assigned and a specific time period in which the assignment must be completed.

### FAQs:

The <http://www.siu.edu/~isat> website will be the means to distribute information and FAQs. Starting in January 2007, periodic telephone conferences will be conducted for teams as a forum for questions and answers.



**Collegiate Cyber  
Defense Competition**