

Collegiate Cyber Defense Competition

2007 Southwest Regional Collegiate Cyber Defense Competition

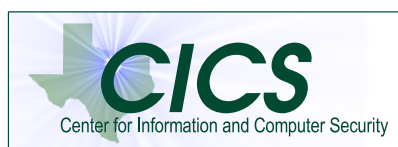
March 23 – 25, 2007

**University of North Texas Research Park
Denton, Texas**

Team Packet

Part 1: Contest Overview and Rules

Hosted By



UNIVERSITY OF NORTH TEXAS™
Discover the power of ideas
COLLEGE of ENGINEERING

Table of Contents

About This Document.....	3
Competition Schedule.....	3
Acknowledgments.....	3
Overview.....	4
2007 Regional CCDC Mission and Objectives.....	5
Competition Rules.....	5
Scoring.....	9
Functional Services.....	9
Business Tasks.....	10
Questions and Disputes.....	11

About This Document

This is Part 1 of the 2-part team packet for the 2007 Southwest Regional Collegiate Cyber Defense Competition (CCDC). This part gives an overview of the contest and gives contest rules. Part 2 provides detailed technical information on the contest network setup, including systems, devices, and software used in the contest.

Competition Schedule

All contest-wide activities (announcements, food, etc.) will be in Research Park Room B-185.

Friday – March 23

12:00 PM	Registration opens – UNT Research Park Hallway
12:35 PM	Opening announcements
1:00 PM	Competition Day 1 begins
6:00 PM – 7:30 PM	Dinner available
8:00 PM	Competition Day 1 complete

Saturday – March 24

8:30 AM	Continental Breakfast available
8:45 AM	Day 2 Announcements
9:00 AM	Competition Day 2 begins
12:00 PM – 1:00 PM	Lunch available
7:00 PM	Competition Day 2 complete

Sunday – March 25

8:30 AM	Continental Breakfast available
8:45 AM	Day 3 Announcements
9:00 AM	Competition Day 3 begins
12:00 PM	Competition Day 3 complete
12:15 PM – 1:00 PM	Feedback session
1:00 PM – 3:00 PM	Lunch and awards ceremony

Acknowledgments

This contest is patterned after the 2006 Southwest Regional CCDC and the 2006 National CCDC, and much of the material we provide here was originally prepared for those contests. Without being able to use the excellent previous work of the teams from Del Mar College and the University of Texas at San Antonio, this contest would not have been possible.

Overview

On February 27 and 28, 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 agreed to host the first Collegiate Cyber Defense Competition (CCDC) for the Southwestern region. 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 more operational task of assuming administrative and protective duties for an existing “commercial” network. 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. To create a fair and even playing field:

- Each team will begin with an identical set of hardware and software: Each team will be given a small, pre-configured, operational network they must secure and maintain. This eliminates any potential advantage for larger schools or organizations that may have better equipment or a larger budget.
- Each team will be located on a dedicated virtual network: Each team’s network will be connected through tunneling boxes 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 provided with the same objectives and tasks: Each team will be given the same set of business objectives and tasks at the same time during the course of the competition.
- Only team members and white team members will be allowed inside their competition rooms: Each team will be assigned their own room during the competition and only the members of the student team will be allowed inside during the competition. This eliminates the potential influence of coaches or mentors during the competition.
- A non-biased, volunteer red team will be used during the competition.

2007 Regional CCDC Mission and Objectives

Mission

The Collegiate Cyber Defense Competition (CCDC) system 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 enterprise network infrastructure and business information systems.

Event Objectives

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

Competition Rules

Overview

The competition is designed to test each student team's ability to secure networked computer systems while maintaining standard business functionality. The scenario involves team members simulating a group of new employees that have been brought in to manage and protect the IT infrastructure at a small to medium sized company. 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 public services: a web site, an email server, a database server, an application server, and workstations used by simulated sales, marketing, and research staff. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure each 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. A technical success that impacts the business operation will result in a lower score as will a business success which results in security weaknesses. A detailed business scenario will be distributed along with technical specifications prior to the exercise to allow teams to develop their team and capabilities.

Competition Play

- The competition will run over a three day period (Friday March 23rd to Sunday March 25th). Registration will occur on Friday March 23rd between 12:00 – 12:45 PM.
- The White Team is responsible for monitoring the network, implementing scenario events, and refereeing.
- Throughout the competition an unbiased Red Team, comprised of information security professionals from commercial, military, or governmental organizations who have volunteered their time and skills to assist in the assessment of a team's ability to defend their network and services, will probe, scan, and attempt to penetrate or disrupt each team's daily operations throughout the competition.
- All student requests, comments, and communication with contest officials should be made through the White Team, and should be done in writing as a "memo" containing the requesting team number. The White Team member who receives the written request/communication will record the time that it was received.
- Student team members will not initiate any contact with members of the Red Team during the hours of live competition.
- Throughout the competition, operations and white team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must allow operations and white team members access when requested.
- On occasion, operations team members may escort individuals (VIPs, press, etc) through the competition area including team rooms.
- All individuals involved with the competition (competitors, officials, and visitors) will be issued badges which must be worn at all times individuals are in the competition area. Badges may not be altered in any way – if a badge is found to have a mistake, contact contest officials and a replacement will be provided.

Student Teams

- Each student team will consist of up to eight (8) members. Each team member must be a full-time student of the institution the team is representing. To qualify as a full-time student, the team member must be enrolled in 12 or more semester credit hours for undergraduates and 9 or more semester credit hours for graduate students during the semester the competition is held.
- Each team may have one faculty advisor present. The faculty advisor may not assist or advise the student team during 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.
- Student team members will not enter another team's competition workspace.
- Internet resources such as FAQs, how-to, existing forums and responses, and company websites, are completely valid provided there is no fee required to access those resources and access to those resources has not been granted based on a previous purchase or fee. Only resources that could reasonably be available to all teams are permitted. For example, accessing Cisco resources through a CCO account would not be permitted but searching a public Cisco support forum would be permitted.

- Competition systems will have direct web-only access to the Internet for the purposes of research and downloading patches. Internet activity will be monitored and any team member caught viewing inappropriate or unauthorized content will be immediately **disqualified** from the competition. This includes direct contact with outside sources through chat/email or any other non-public services.
- Teams must compete without “outside assistance” from non-team members. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members including team sponsors that would help the team gain an unfair advantage are not allowed and are grounds for **disqualification**.
- No PDAs, memory sticks, CDRoms, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the white team in advance. All cellular calls must be made and received in the designated area. Any violation of these rules will result in **disqualification of the team member and a 400 point penalty assigned to the appropriate team**.
- Teams may not bring any computer, tablets, PDA, or wireless device into the competition area. MP3 players with headphones will be allowed in the competition area provided they are not connected to any system or computer in the competition area.
- Teams may not remove any computer or networking device from the competition area.
- Printed reference materials (books, magazines, checklists) are permitted in competition areas. Team sponsors and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, “suggestions”, or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and a 400 point penalty will be assessed against the team.
- Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access are permitted.

Systems

- 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 should not assume any system is properly functioning or secure; they are assuming recently hired administrator positions and are assuming responsibility for each of their systems.
- All teams will be connected to a central router and scoring system.
- Each room contains a gateway box which the team network is connected to. This box is part of the contest infrastructure and not the team network, and should not be disrupted in any way. Any attempt to tamper with this box or to disrupt the tunneling functionality of the contest network is grounds for **disqualification**.
- Network traffic generators will be used throughout the competition to generate traffic on each team’s network.
- Teams are permitted to replace applications and services provided they continue to provide the same content, data, and functionality of the original service. For example, one mail service may be replaced with another provided the new service still supports standard SMTP commands, supports the same user set, and preserves any pre-existing messages users may

have stored in the original service. Failure to preserve pre-existing data during a service migration will result in a 50 point penalty for each service.

- All SMTP services using authorization must support AUTH LOGIN and base64 encoded userids and passwords.
- Teams are free to examine their own systems but no offensive activity against other teams, the white team, or the red team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the white team, the red team, or any global asset will be immediately **disqualified** from the competition.
- 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 for collection. Incident reports must contain a description of what occurred, a discussion of what was affected, and a remediation plan. A thorough incident report that correctly identifies a successful red team attack will reduce the red team penalty by 50 percent.
- Each student team may change passwords for administrator level and user level accounts. Any password changes to user accounts must be provided to the white team with a minimum of 15 minutes advance warning prior to the changes being implemented (unless the password changes are part of a competition tasking). Failure to notify the white team of user level password changes could result in service check failures. Teams are required to provide modified passwords in the electronic format specified. Please note that the white team will not error check the provided password changes – they will simply upload the provided changes.
- Teams are allowed to use active response mechanisms such as TCP resets for suspicious/malicious activity. Any active mechanisms that interfere with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
- Student teams must maintain specific services on the “public” IP addresses assigned to their team – for example if a team’s web service is provided to the “world” on 10.10.10.2, the web service must remain available from the contest network at that IP address throughout the competition. Moving services from one public IP to another is not permitted.
- Student teams are not permitted to alter the system names of their assigned systems.
- The white team will provide a mechanism to show teams the official status of their critical services during the last scored service check.
- Teams will have access to a “Restore from Backup” capability that will reset any system to its initial starting configuration. This service will be performed by the white team and will cost the team 50 points per system recovered.
- Each student team will be provided with a set of install disks for the operating systems and major applications used in the competition network. These may be used to reload systems, add/remove functionality, reinstall, etc.
- No software may be brought in by the teams. Software may be downloaded and installed during the contest, but only if it is free and downloaded from a public web site or ftp server (not a server set up by the team before the contest).
- Systems designated as “workstations” are to be treated as user workstations and may not be re-tasked for any other purpose by student teams. They must remain user workstations throughout the entire competition unless otherwise directed by a white team member. Other hardware platforms, such as servers and networking equipment, may be re-tasked or reconfigured as needed.

Scoring

- Scoring will be based on keeping required services up, controlling/preventing un-authorized access, and completing business tasks that will be provided throughout the competition. Teams accumulate points by successfully completing injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by the red team.
- Scores will be maintained by the White Team, but will not be shared until the end of the competition. There will be no running totals provided during the competition. Team standings will be provided at the beginning of day two and three but without specific scores.
- 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 Team Captain should immediately contact the competition officials to address the issue.
- Any team that tampers with or interferes with the scoring or operations of another team's systems will be **disqualified**.

Scoring

The winner will be based on the highest cumulative score at the end of the competition. During this competition a team may accumulate a total maximum of 5,000 points. Approximately half of the points are based on tests of functional services (based on a random polling interval of core services), and half of the points are based on successful completion of business tasks. Successful red team actions will result in point deductions from a team's total score based on the level of access obtained, the sensitivity of information retrieved, etc.

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 5 minute intervals, certain services will be tested for function and content where appropriate. Each successfully served request will gain the team the specified number of points.

The following are representative examples of services which must be available.

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 specific page 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. SMTP services must be able to support either unauthenticated sessions or sessions using AUTH LOGIN (base64) at all times.

SSH

An SSH session will be initiated to simulate a vendor account logging in on a regular basis to check error logs. Each successful login and log check 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.

There may also be custom services provided by your company, for example through the company web site, which you must keep available. The official list of required services will be provided before the start of the competition.

Each of the required services operates under a Service Level Agreement and teams will be assessed penalties for extended outages of critical services. For example, if a critical service is down continuously for over 1 hour, the team will be assessed a 20 point penalty. If the service is down for over two hours the team will be assessed a 40 point penalty. If the service is down for over 3 hours the team will be assessed a 50 point penalty for **each additional hour** the service is down.

Business Tasks

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

Some examples:

- Opening an FTP service for 2 hours given a specific user name and password: 200 points
- Closing the FTP after the 2 hours is up: 50 points
- Creating/enabling new user accounts: 100 points
- Installing new software package on CEO's desktop within 30 minutes: 100 points

Every team must make an effort to complete each tasking. Failure to attempt any tasking will result in a team penalty and could result in a "firing" of team members.

Red Team Actions

Successful red team actions will result in penalties that reduce the affected team's score. Red team actions include:

- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points

- Recovery of userids and passwords from a team system (encrypted or unencrypted): -50 points
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points
- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points

Red team actions are cumulative. For example, a successful attack that yields root level access and allows the downloading of userids and passwords would result in a -150 point penalty. Red team actions are scored on a **per system** and **per method** basis – a buffer overflow attack that allows the red team to penetrate a team’s system will only be scored once for that system; however, a different attack that allows the red team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the red team compromises a single user account and obtains root access in the same attack the penalty will be -100 points for root level access and not -125 points for root and user level access.

Questions and Disputes

- 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.
- Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
- In the event of an individual disqualification, that team member must leave the competition area immediately upon notification of disqualification and must not re-enter the competition area at any time. Disqualified individuals are also ineligible for individual awards or team trophies.

In the event of a team disqualification, the entire team must leave the competition area immediately upon notice of disqualification and is ineligible for any individual or team award.