

Southeast Collegiate Cyber Defense Competition Team Packet



SECCDC07 is sponsored by



CHARLOTTE RESEARCH INSTITUTE

College of Computing
and Informatics



Microsoft

Deloitte.



SecureWorks®

Southeast Collegiate Cyber Defense Competition (SECCDC) Team Packet
Version 3. 1/22/2007

TOC

History.....	3
Overview.....	3
Teams.....	3
Case Organization Information.....	4
Pre-Competition Configuration	5
Physical Facilities	5
Support Network.....	5
Logical Network Diagrams.....	7
Specific Team Equipment.....	7
Schedule.....	9
Competition Rules	10
Overview.....	10
Systems	11
Student Teams.....	12
Scoring.....	13
Functional Services.....	14
Business Tasks	14
Logs.....	15
Policies.....	16
Recommended Reading List.....	16
SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGs) and CHECKLISTS	16
NIST Security Configuration Checklists Repository.....	17
NIST Special Publications	17
Microsoft Security Guides for:	17

History

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

From these discussions, the first Collegiate Cyber Defense Competition (CCDC) was formed. The first competition (in the Southwestern region) was held in May 2005. In 2006 the first National Collegiate Cyber Defense competition were held with major sponsorship from the U.S. Department of Homeland Security. Four regional champions and a joint team of U.S. Military Academies competed in San Antonio Texas in April 2006. Kennesaw State University hosted the first Southeastern regional competition in 2006. Special thanks go to the UTSA Center for Infrastructure Assurance and the Center of Security Education at Kennesaw State University for their permission and support in providing materials to support the 2007 SECCDC.

Overview

While similar to other cyber defense competitions in many aspects, the SECCDC, as part of the CCDC, is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. 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.

Teams

Teams involved in this competition include:

- Academic teams – student teams consisting of graduate and undergraduate students from regional institutions who will compete in the SECCDC. Currently teams from the following institutions have indicated interest in participating:
 1. Chattahoochee Technical College, Georgia
 2. Kennesaw State University, Georgia
 3. Mercer University
 4. Mississippi State University
 5. Southern Polytechnic State University, Georgia
 6. University of Louisville, Kentucky
 7. University of North Carolina, Charlotte
 8. University of North Carolina, Wilmington
 9. University of South Carolina
 10. University of South Florida
- Red team – a group of information security professionals from volunteer commercial organizations who have offered their skills to assess the abilities of

the teams to defend their networks and systems. The Red team will conduct periodic probes, scans and attempted penetrations of the academic teams.

- White team – a group of information technology and information security academics and professionals who will serve as judges and referees. Each academic team will be assigned a White team judge, and white team assistant who will assess the academic teams' ability to secure their network segment and systems, and who will periodically query the team as to their actions and provide "injections" designed to challenge the teams' implementation. Academic teams are advised not to argue or question the White team, only answer when queried. The White team also includes individuals who assess the readiness of team services.
- Gold team – the administrative faculty and professionals who will conduct the exercise, control the flow and timing of the events and injections, and who will serve as mediators for disputes and challenges. Academic teams are advised not to interact with the Gold team except during challenges and mediations. White team judges will handle these interactions on behalf of the teams. Dr. Bill Chu is the chief gold team member and competition coordinator.

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 configure, 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 internal network: 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 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 the assigned academic team members, and White and Gold team members will be allowed inside their competition rooms: Each team will be assigned their own workspace during the competition and only the members of the academic student team will be allowed inside during the competition. This eliminates the potential influence of coaches or mentors during the competition.
- The red teams will not know the identity of the teams they assess, only having a range of IP addresses assigned.

Case Organization Information

Established in June 1999, ACME is an Internet service provider operating out of Charlotte, North Carolina, serving the Southeast US region. ACME provides basic Internet access, fast Internet access, and Web registration and hosting alternatives for small office/home office (SOHO) individuals and organizations. ACME is a privately owned company managed by the founder and CEO Arnold Ziffel. ACME has branch offices in surrounding states.

The CIO, Tony Kombol, has over 15 years of technical experience and 10 years of experience as a senior IT manager. Shortly after taking the position as CIO at ACME, he hired Scott Woods as manager of information security. A reorganization in 2003 resulted in an elevated recognition of the role of information security at ACME, and the assignment of the title of chief information security officer to Scott. Along with this increased recognition came the assignment of dedicated personnel and a budget of approximately \$500,000 for equipment, personnel, and training.

Since its founding, the organization has grown to over 10 regional offices throughout the South, with a corporate office maintained in Columbia, South Carolina. Each regional office maintains an identical staff, with internal operations previously managed by a central IT department. Due to budgetary circumstances, the central IT office is being distributed to the branch offices. Your team has been hired as an outside consulting group to assist in the finalization of the network configuration and the protection of the core administrative services vital to each branch headquarters. Even though the regional branch manager runs the operations of the branch, the CIO, Tony Kombol will communicate directly to each regional ITS (Information Technology and Security) team leader via email. Each organization uses email as its primary means of communication with address typically assigned using first initial/last name as the username, with an 8 character restriction. (i.e. Tony Kombol would use tkombol@acme.com (corporate headquarters). Security teams will use ciso@xx.acme.com (the url of their particular branch). The offices and their corresponding Web presence is keyed to their branch office, for example, the South Carolina regional office would be at www.sc.acme.com. The organizational chart at the end of this document shows the employees assigned to your division.

Pre-Competition Configuration

Physical Facilities

The competition will be conducted on the third floor of the Woodward Hall building. All visiting participants are encouraged to use the visitor parking deck (Cone Deck 1).

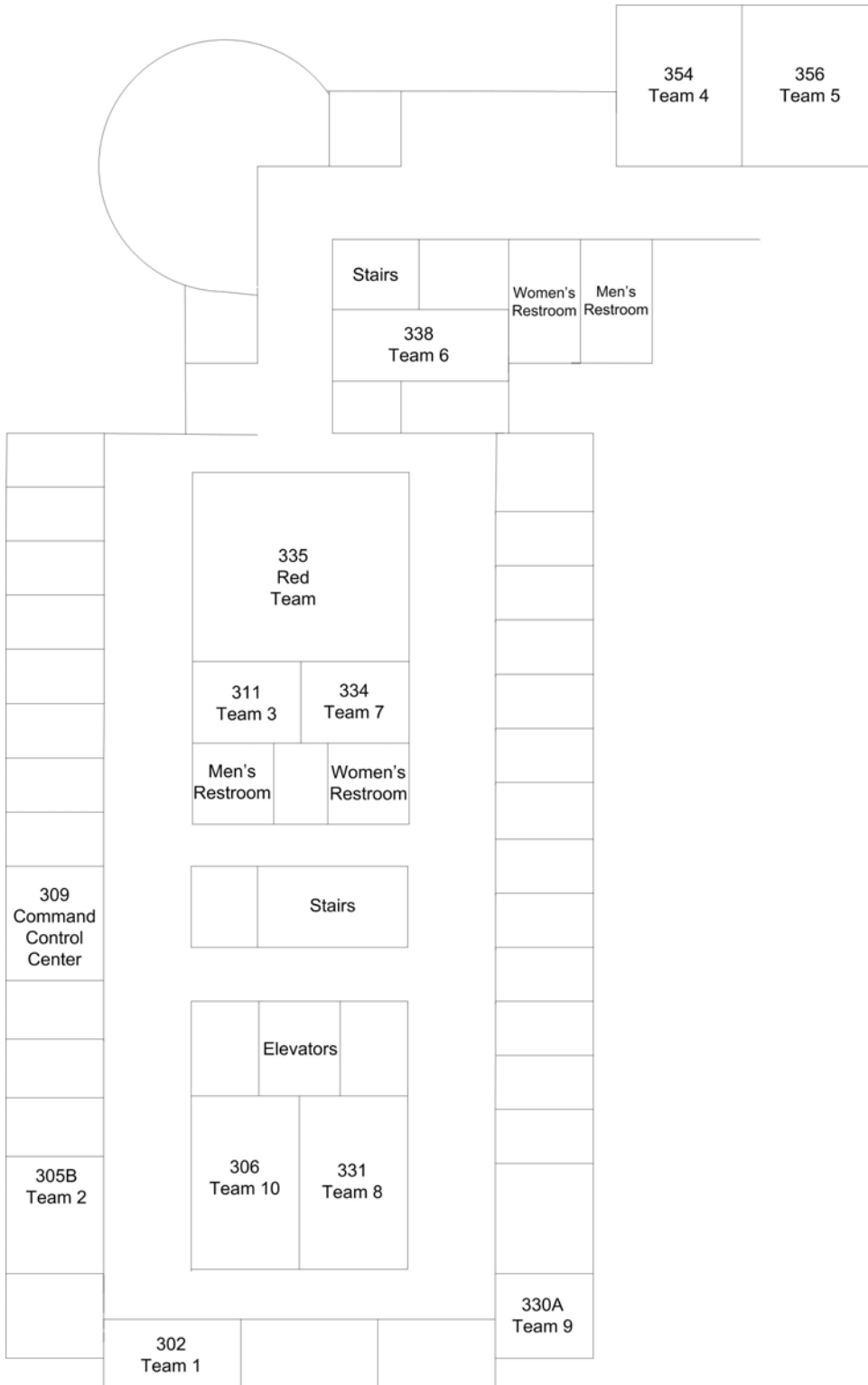
Detailed maps of UNCC campus can be found at

<http://facilities.uncc.edu/maps/>

Initial meeting and opening remarks will be conducted in Woodward Hall room 106.

Signs will be posted in and around the Woodward Hall building advising participants where to go. Included below is a map of the third floor team layout. Physical layout is subject to change prior to the competition dates.

Cyber Defender Team Layout



Logical Network

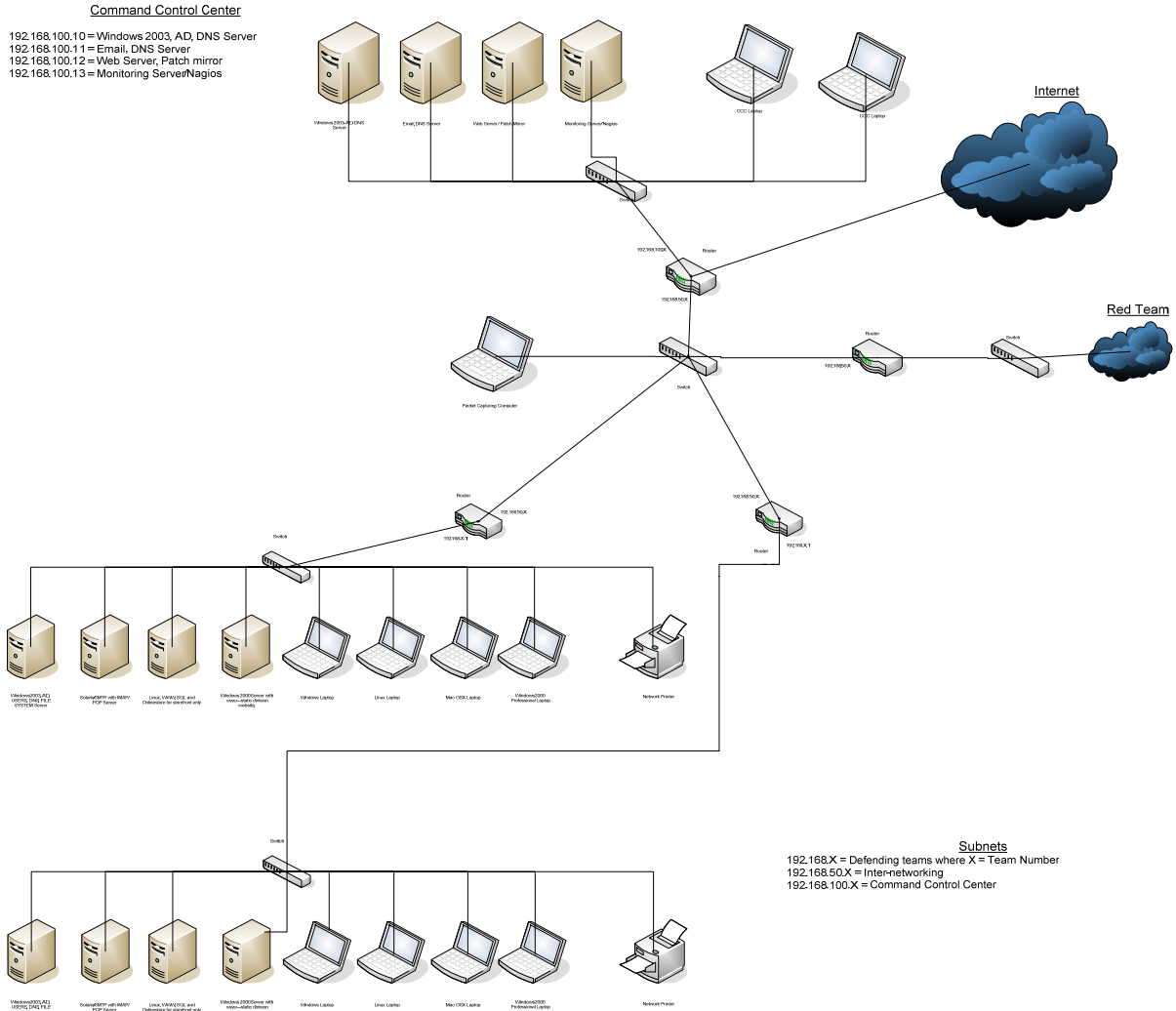
The competition network will be connected to the public internet. Access to many patch updates will be provided on the local competition network which may be used in the competition. There will be a central Command Control Center network running a number of services. There will be numerous operating systems used, including Windows 2003 Server, Windows XP, Solaris, Linux, and Mac OS X. Services running may include Active Directory, DNS, File Services, Web, FTP, and others. Team subnets will not be allowed to communicate with each other. The Red Team is prohibited from running exploratory or hacking tools against any public internet addresses. Network and Systems Layout is subject to change prior to the competition. The Command Control Center network and nodes will be controlled by the white team only.

Individual Team Layouts are identical except for their subnet addressing. Each team will be assigned numerous items of hardware running various operating systems and services. Students will be required to keep these systems functional while protecting them from attacks. The hardware will be Dell Precision series computers and Apple MacBook Pro laptops. The diagram below should explain much of the systems and network layout.

Southeast Collegiate Cyber Defense Competition (SECCDC) Team Packet

Version 3. 1/22/2007

Cyber-Defender Competition



Teams Information

- 192.168.X.1 = Default Gateway/Router
- 192.168.X.10 = Windows 2003, AD, Users, DNS, File System server
- 192.168.X.11 = Solaris/SMTP IMAP/POP
- 192.168.X.12 = Linux, WWW, SQL and online store with store front only.
- 192.168.X.13 = Windows 2000 Server with www- static division website.
- 192.168.X.20 = Windows Laptop.
- 192.168.X.21 = Linux Laptop.
- 192.168.X.22 = Mac OSX.
- 192.168.X.23 = Windows 2000 Professional Laptop.
- 192.168.X.99 = Network Printer

Preliminary Schedule

Friday, March 9th

Note: There will be no food service on campus on Friday. Teams should plan to eat before registration, and after the initial configuration session.

- *12:00 AM*
Woodward Hall 106 - Registration opens. Teams will register and gather in 106
- *12:30 PM*
Welcome and opening announcements. Upon Completion, teams will be led into their rooms.
- *1:00 PM – 6:00 PM*
Team Rooms - Competition begins: Academic teams are provided the opportunity to examine the configuration of their systems and networks, “offline”. Teams may begin updating and modifying their configuration to meet the specifications of their initial requirements.
- *6:00 PM*
Day one concluded for student teams – each team will deliver their day’s report and leave the competition area. White team judges assess team’s performance.

Saturday, March 10th

- *7:50AM*
Teams gathered in Woodward 106 for announcements for day two.
- *8:00 AM*
Team Rooms - Day two of competition begins, all networks connected to the simulated “Internet”.
Lunch & Dinner provided: However, there is no cessation in the day’s events, teams must rotate out to eat: no food or drink is allowed in the competition rooms.
- *7:00 PM*
Competition Ends
 - Dinner
 - White teams meet to tally results

Sunday March 11th

- *10 AM – 12:30 PM*
Woodward 106 - Red, White and Gold Teams meet to tally results.
Student teams present overview of their efforts – 20 minutes per team
Red teams present their findings and assessments
White teams present their finding and assessments
Presentation of winning trophies (1st, 2nd and 3rd place)
- *12:30 PM.* Competition concludes. Lunch boxes to go

Competition Rules

Overview

The competition is designed to test each academic team's ability to secure a networked computer system 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 IT services company/reseller. 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 a workstation 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

- All teams are connected to a central switch and scoring system.
- Each student academic team will start the competition with identically configured systems.
- Each student academic team will appoint an official Team Captain who will handle all protests and official inquiries for their team during the competition.
- Each student academic team will appoint a team change management representative who will ensure all changes to the systems are documented in the team's change management log – including all password changes, software and hardware installations and configuration.
- The Red Team will attempt to infiltrate or disrupt each team's daily operations throughout day two of the competition.
- The White Team is responsible for monitoring the network, implementing scenario events, and refereeing.
- Scoring will be based on keeping required services up, controlling, preventing and reporting unauthorized access, and completing business tasks that will be provided throughout the competition.
- All team members will wear badges and team colors identifying affiliation at all times.
- Student team members will not initiate any contact with members of any other team (student, Red or Gold) during the hours of live competition.
- Student team members will not enter another team's competition workspace.
- The competition will run over a three day period. Registration will occur on Friday between 12 – 12:30pm.

- 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.
- Protests by any team will be presented by the Team Captain to the competition officials through White team to the Gold team, as soon as possible. The Gold team 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 Team Captain should immediately request that their White team judge address the issue with the Gold team.
- Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.
- Any team that scans or probes any IP address outside their own subnet will be disqualified.
- Team captains and team liaisons are encouraged to work with their White team representative and through them the Gold team, to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins.
- No unauthorized electronic devices or media are allowed in the room during the competition. All cellular calls must be made and received outside the designated competition areas. Any violation of these rules will result in disqualification of the team member and a point penalty assigned to the appropriate team.
- Teams are allowed to bring hard copy documentation, checklists, and technical books with them. These are subject to review by the Gold team and may be permitted or disallowed at the Gold team's discretion. If the team has any question about their documentation selection, they may submit a list of titles they intend to bring to the competition to the competition coordinator at least two days prior to 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.
- Software: only software freely and publicly available to all competition teams will be allowed. Open source software is allowed. Free trial software will need to be justified in writing by the team before use. The need and benefit of the trial software must be documented.
- All communication are to be "business-professional" and is to be submitted for judging.

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 approximately one week prior to the event to permit planning.

- Student teams will not be permitted to bring any computing systems with them. However, additional equipment – hardware, software and networking will be available to each team. Only provided open source security tools may be used. No commercial security software will be available and all systems are subject to inspection during and after the competition.
- Student teams should not assume any system is properly functioning or secure; they are assuming recently hired administrators and are assuming responsibility for each of their systems.
- Student teams must maintain specific services on the “public” addresses assigned to their team – for example, if a team’s web service is provided to the “world” on www.sc.acme.com which is mapped via DNS to 10.10.10.2, teams must make sure that URL is accessible, modification of the actual system IP address is at the team’s own risk. The white team assesses the available services, not the specific IP addresses.

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, or as defined by their host institution (subject to verification). Each team can have a maximum of two (2) graduate students.
- Each institution must submit a team roster at least one week prior to the competition. Team rosters must also indicate team captain and team liaison members.
- Each team may have one faculty advisor / coach present at the competition. The faculty advisor may not assist or advise the student team during the competition – even after official competition hours. All advisors / coaches will sign agreements upon arrival.
- Teams must maintain change management logs detailing all modifications and updates to all systems – hardware, software and networking. These logs will be left in the competition rooms for review by the White team judges during scoring. If the team wishes to make a duplicate copy of the log, copy facilities will be available at the end of day one and two.
- 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 (White and Gold team members) and the teams before and during 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. This information must be provided to the competition staff to allow recognition on name badges.

Scoring

The winner will be based on the highest score obtained during competition time. During this competition the team that accumulates the most points wins. The following is an outline of principles for scoring.

Points Awarded

- **Pre-configuration:** Each team will have their systems and networks assessed at the end of day one by their white team judge, with the assistance of other white team members. The teams may expect to receive a maximum of 500 points for their pre-configuration efforts.
- **Functional services (based on periodic polling interval of core services):** Each assessment during which the team maintains mandated services awards that team up to 50 points. Each expected service not present will deduct up to 10 points from this total. The number of assessments will not be disclosed, and will be random throughout day 2 of the exercise. Maximum total points is expected to be between 1000 and 2000 points.
- **Red team assessments:** Red team will rank order the student teams on a scale of best prepared to least prepared, based on their own subjective mechanisms. Best prepared team will receive 100 points, second best 90 points etc. Maximum number of points is expected to be between 1000 and 2000 points.
- **Business taskings (injections):** Teams will receive a number of system and network modification and information requests. Teams must prioritize tasks as each will have a variable time and point value. Awarded points will vary by task for a possible total of between 1000 and 2000 points. Note that sometimes a business task may violate the company's security policy. In such a case, the appropriate response is to point that out and ask for permission from the appropriate authority (e.g., the CIO).

Point deductions:

- **Change management logs:** all activities resulting in modification to the systems and network must be logged in the team change management log. Failure to log an activity, or logging an unimplemented action will result in deductions to the team's totals corresponding to 50 percent of the value of the effort (i.e. a 100 point injection requiring the team to add a service to a server that is not logged, will result in a 50 point penalty assessed to the 100 point completion award).
- **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.
- **Being IT security professionals,** teams are expected not to ask unreasonable questions (e.g. questions that show they do not have clear understanding of technical / ethical concepts). If a team consistently raises unreasonable questions / issues that clearly reflect poor judgments, points may be deducted.

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 periodic intervals, certain services will be tested for function and content where appropriate. Each successfully served request will gain the team points. Note only the services that are operational at the time will be assessed, once injections are issued requesting new services, those services will be added to the assessment server.

Some sample services could include:

- HTTP: A request for a specific web page may be made. Once the request is made, the result will be compared to the expected result. Results must match expected content for points to be awarded.
- HTTPS: A request for a page over SSL may be made. Again, the request will be made, the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.
- SMTP: Email may 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.
- SSH: An SSH session may 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 may 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 may be performed against the DNS server. Each successfully served request will be awarded points.
- Domain Controller/File Services: Individual users need access to the primary domain controller to access and store their key files.

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. When each team is emailed a task (the primary mechanisms for delivery) they are expected to acknowledge receipt within 15 minutes. Failure to do so will result in a penalty.

Some examples:

- Opening an FTP service for 2 hours given a specific user name and password
- Closing the FTP after the 2 hours is up
- Creating/enabling new user accounts
- Auditing a user's activities through system logs
- Installing new software package on CEO's desktop within 30 minutes

Southeast Collegiate Cyber Defense Competition (SECCDC) Team Packet
Version 3. 1/22/2007

Each “injection” tasking will include the point values and time restrictions associated with the task. Teams can prioritize their efforts based on outstanding requests. Upon completion of tasks, the tasks assignment sheets will be signed by the team Captain and returned to the White team judge, who will note the time that the event was completed. The assignments will then be assessed by the Red or White team. Normally the team will only see the email (shown below). The White team will have the injection forms for assessment.

SAMPLE INJECTION
TASK: Install Google Desktop on CEO’s Windows XP Client Computer
TIME OF ASSIGNMENT: 2:15 PM 3/10/2006
TO BE COMPLETED BY: 3:00 PM 3/10/2006
POINTS: 50
CONDITIONS: Given an installation CD, team is to setup Google Desktop on the CEO’s office machine and configure to index only during non-business hours. Business hours are defined as 7AM to 7PM.
TASK COMPLETED WHEN: When the team has successfully completed this task, they are to print a screen capture of the CEO’s Client showing the Google Desktop configuration window, and submit with this form to their White team judge.
TASK COMPLETED BY: (Name)
TASK COMPLETED BY: (Team)
TASK COMPLETED AT: (Time)
WHITE TEAM VERIFICATION: (Name)
WHITE TEAM VERIFICATION: (Time)
WHITE TEAM INSTRUCTIONS: Enter this information into your team log and send this form to the Gold Team Room by runner immediately on completion.

Logs

All student teams will be expected to maintain a change management log (1 log per team). When a student performs a task, they should immediately make an entry to the change management log detailing the following:

- what task was performed, (i.e. changed a password, installed software etc)
- when it was performed (i.e. 12:45 PM 3/10/06)
- on what machine it was performed (i.e. IP 10.10.10.10 or CEO’s Client PC)
- what specifically was done (i.e. changed password from joe to j2ee4me)
- why it was performed (i.e. in response to injection or because it was good business practice) who actually performed the task

Failure to document modifications and updates in the change management log could result in point penalties.

Students are encouraged to maintain a personal journal of their actions, events and perceptions. These journals could be used for review of actions, at the end of each day. Students will be permitted to take their personal logs, and copies of the change

management log with them at the end of the competition for use in professional development.

Policies

In some cases, student teams may submit policy requests to their White team judge to allow an operational or managerial control, in lieu of a technical control. For example, if the team writes an acceptable use policy for a networked photocopier, specifying that no confidential documents should be allowed to be printed on the device, they may be able to avoid having to install password protection on that device.

Note: the judge will determine if the policy is acceptable and may require the technical control anyway.

Recommended Reading List

Note this list is not meant to be comprehensive but a baseline for programs to use in preparing for the SECCDC.

Various publications from:

SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGs) and CHECKLISTS (<http://csrc.nist.gov/pcig/cig.html>)

Application Security Checklist (864 KB)

Database STIG (1,121 KB)

Database Security Checklist Ver. 7 Rel. 1.0 (693 KB)

Desktop Application STIG (714 KB)

Desktop Application Security Checklist Ver. 1 Rel. 1.9 (789 KB)

DoD Domain Name System (DNS) STIG Ver. 2, Rel. 1 Memorandum (185 KB)

Domain Name System (DNS) STIG Ver, 2, Rel. 2 (803 KB)

Domain Name System (DNS) Checklist (1,324 KB)

Network STIG Draft Ver. 6 Rel. 3 (2,184 KB)

Network STIG Comment Matrix (496 KB)

Network Infrastructure STIG (1,500 KB)

Network Infrastructure Security Checklist Ver. 5 Rel. 2.4 (1,483 KB)

Peripheral STIG Ver. 1 Rel. 0 (784 KB)

Secure Remote Computing STIG Ver. 1 Rel. 1 (706 KB)

Sharing Peripherals Across the Network STIG Final Draft Ver. 1, Rel. 1 (769 KB)

UNIX STIG with updated LINUX section (407 KB)

UNIX Security Checklist Ver. 4 Rel. 4 (696 KB)

Web Server STIG (1,672 KB)

Web Server Security Checklist Ver. 4, Rel. 1.6 (490 KB)

NSA Windows NT Guide STIG (1,282 KB)

Addendum to the NSA Guide to Securing Windows NT STIG (1,032 KB)

Windows NT Security Checklist Ver. 4 Rel. 1.15 (683 KB)

Windows XP STIG (2,030 KB)

Windows XP Security Checklist Ver. 4 Rel. 1.12 (1,148 KB)

Windows Server 2003 Checklist Draft - Ver. 4 Rel. 0.0 (1,083 KB)

Windows 2000 Secure Baseline Configuration Standards Checklist (807 KB)

Southeast Collegiate Cyber Defense Competition (SECCDC) Team Packet
Version 3. 1/22/2007

Windows 2000 Security Checklist Ver. 4 Rel. 1.12 (1,399 KB)
Windows NT/2000/XP Addendum Ver. 5, Rel. 0.3 -STIG (202 KB)

NIST Security Configuration Checklists Repository

<http://csrc.nist.gov/checklists/repository/category.html>

NIST Special Publications:

<http://csrc.nist.gov/publications/nistpubs/index.html>
Draft SP 800-83, Guide to Malware Incident Prevention and Handling
Draft SP 800-81, Secure Domain Name System (DNS) Deployment Guide
SP 800-61, Computer Security Incident Handling Guide
SP 800-45, Guidelines on Electronic Mail Security
SP 800-44, Guidelines on Securing Public Web Servers
SP 800-42, Guideline on Network Security Testing
SP 800-41, Guidelines on Firewalls and Firewall Policy
Draft SP 800-40 Version 2, Creating a Patch and Vulnerability Management Program
SP 800-31, Intrusion Detection Systems (IDS)
SP 800-26, Security Self-Assessment Guide for Information Technology Systems,

Microsoft Security Guides for:

Windows XP

<http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.msp>

Windows 2000 Security Hardening Guide

<http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/default.msp>

Windows 2003

<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.msp>

Faculty advisors / coaches should address any questions or concerns to the competition coordinator: Dr. Bill Chu at bchu@uncc.edu.