Collegiate Cyber Defense Competition

Team Packet
Competition Date: 01/12/08
V2.0

Table of Contents

Background

This document provides the background information and rules governing the teams that will participate in the 3rd Mid-Atlantic Regional CCDC State Qualifying round.

Any questions or concerns associated with these rules and regulations should be directed to Casey W. O'Brien, Associate Professor and Network Technology Program Coordinator, Community College of Baltimore County (cobrien@ccbcmd.edu). Comments from team coaches are encouraged; however, CCBC and White Wolf Security reserve the right to formulate the competition in a manner best suiting their interpretation of the CCDC.

The Mid-Atlantic Regional CCDC is funded through a National Science Foundation (NSF) Advanced Technological Education (ATE) grant, as part of the CyberWATCH project (www.cyberwatchcenter.org).

Overview

While similar to other cyber defense competitions in many aspects, the Mid-Atlantic Regional CCDC, as part of the National 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.

The teams will be physically co-located in the same room. Each team is given close to identical system configurations as possible at the start of the competition. Throughout the competition, the teams have to ensure the systems supply the specified services while under attack from a volunteer Red team. In addition, the teams have to satisfy periodic "injects" that simulate business activities IT staff must deal with in the real world.

Mission

"The goal of a Cyber Defense Competition is to provide hands-on application of information assurance skills; as such, they enhance students' understanding of both theory and practice. They provide students a laboratory in which to experiment, just as in other fields of science. They fulfill the same role as capstone projects in a traditional engineering program (i.e., projects that allow students to synthesize and integrate knowledge acquired through course work and other learning experiences into a project usually conducted in a workplace). The competition combines legal, ethical, forensics, and technical components while emphasizing a team approach. Such experiential education increases the knowledge and expertise of future professionals who may be in a position to contribute to the secure design and operation of critical information and its supporting infrastructure" (from *Exploring a National Cyber Security Exercise for Colleges and Universities*, Lance J. Hoffman and Daniel Ragsdale, 2004).

Event Objectives

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

Teams

Teams involved in this year's competition include:

•**Academic Teams**: student teams consisting of full-time, undergraduate and graduate, degree-seeking students, representing four year universities and community colleges from Maryland and Pennsylvania. This year's participating teams include:

1. Anne Arundel Community College
2. Community College of Baltimore County
3. Howard Community College
4. Johns Hopkins University
5. Millersville University
6. Towson University
7. University of Pittsburgh

•**Red Team (AKA Red Cell)**: 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.

•**Gold Team**: a group of IT and information security academics and professionals who will serve as judges and referees. Each academic team will be assigned a Gold team judge and assistants, who will periodically query the team as to their actions and score "injects" designed to challenge the teams' implementation. Academic teams are advised not to argue or question the Gold team, only answer when queried.

1

•**White 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 White team except during challenges and mediations.

To create a fair and even playing field:

1• Each team will begin with as close to an identical set of hardware and software as possible: Each team will be given a pre-configured, operational network they must configure, secure, and maintain. This eliminates any potential advantage for larger schools that may have better equipment or a larger budget.

2• 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.

3• 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.

4• Each team will be assigned their own workspace during the competition and only the members of the Academic team, the Gold team members, and any representatives of the White team will be allowed inside that space during the competition. This eliminates the potential influence of coaches or mentors during the competition.

5• A non-biased, volunteer, commercially experienced Red team will be used during the competition.

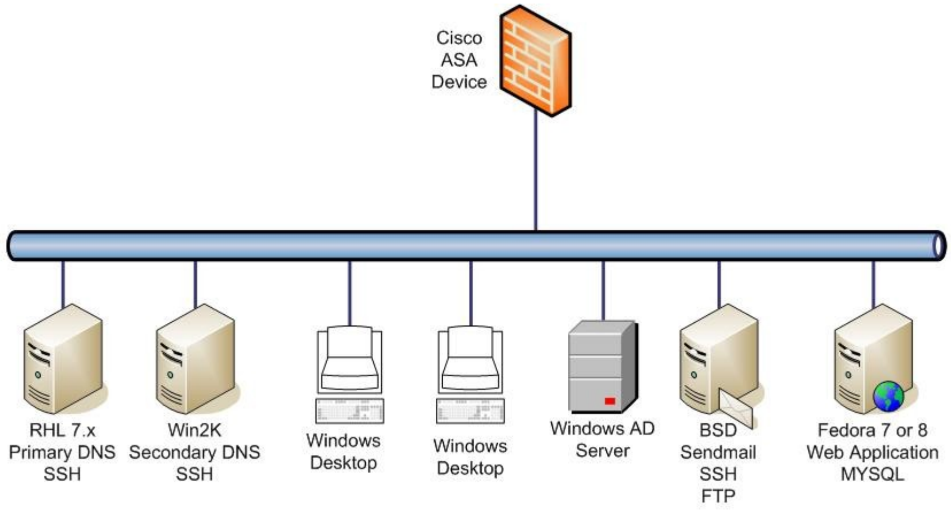
Network Information

As stated previously, the competition network will be completely standalone with no external connectivity. Global servers, the Red team network, the White team network, and each Academic team network will be connected to a central router that will be maintained by the White team.

Each team's network consists of the following:

1 Router (White team controlled)
1 Cisco ASA 5505 firewall (Academic team controlled)
Any number of PCs, all of which will be virtualized. VMware player will be used.

Each Academic team will be provided with a standalone PC with Internet access that may be used for research, software downloads, etc. At no time will this PC be connected to the competition network - **doing so is automatic grounds for disqualification**.



© 2007 White Wolf Security
Team Distribution ONLY

Draft: October 31, 2007
Actual infrastructure may vary

Rules of Engagement

Overview

The competition is designed to test each Academic 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 gaming 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 certain services (i.e., HTTP, SMTP).

The competition measures each Academic team's ability to maintain secure 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 higher score, as will a business success which results in security weaknesses.

Competition Play

1. The White team is responsible for monitoring the network, implementing scenario events, and refereeing.
2. All teams are connected to a central router and scoring system.
3. Each student team will appoint an official Team Captain who will handle all protests and official inquiries for their team during the competition.
4. Each student team will be assigned a rotating Gold team representative. All inquiries for the White team will be directed through this Gold team member.
5. Protests by any team will be presented by the Team Captain to their representative Gold team member as soon as possible. The Gold team representative will then convey the issue to the White team. The White team will be the final arbitrators for any protests or questions arising before, during, or after the competition.
6. Team Captains are encouraged to direct and resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins. Queries should be sent to Casey O'Brien (cobrien@ccbcmd.edu).
7. All CCDC participants will wear badges identifying team affiliation at all times. Badges will be handed out at check-in.
8. Academic team members will not initiate any contact with members of the Red team during the hours of live competition and vice versa.
9. Academic team members and Red team participants will not enter another team's competition workspace.
10. Scores will be maintained by the White team. No running totals will be provided during the competition.
11. Scoring will be a combination of automated tools and manual checking.

12. Scoring will be based on controlling/preventing unauthorized access, completing business injects in a timely and accurate manner, filing incident reports, and keeping necessary service up and running throughout the duration of the competition.
13. Failure to maintain service availability, as well as the integrity and confidentiality of information will result in penalties being assessed against the offending Academic team.
14. Penalties will take the form of points being added to an Academic team's overall score. The team with the lowest score will win the competition.
15. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a higher score. Should any question arise about specific scripts or how they are functioning, the Team Captain should immediately contact their Gold team representative to address the issue with the White team.
16. Any team that tampers with or interferes with the scoring or operations of another team's systems will be **disqualified**.
17. Points will be deducted from a team's score if evidence of un-authorized access and/or compromise can be proved.
18. All systems on the network diagram must be reachable and respond to ICMP pings.
19. All services that are tested for must remain open and functional.
20. A Red team will attempt to infiltrate or disrupt each team's daily operations throughout the competition. The Red team will provide evidence of compromise.
21. Team-to-Domain Name Assignments:
    a. Anne Arundel Community College: target81.com
    b. Community College of Baltimore County: target82.com
    c. Howard Community College: target83.com
    d. Johns Hopkins University: target84.com
    e. Millersville University: target85.com
    f. Towson University: target86.com
    g. University of Pittsburgh: target87.com
22. Teams may block by source IP, but to do so is to run the risk of blocking the Score Bot. If the Score Bot cannot reach your systems, you will be penalized accordingly.
23. Each team must keep syslogs.
24. The systems are to remain plugged in to the network at all times.
25. ICMP and IP traffic must flow between all the teams.
26. The systems are to maintain the same IP addresses during the course of the event.
27. A complete list of necessary ports/services will be provided on the day of the competition.
28. The services provided on the day of the competition are to be up and reachable. If you turn off a service or move the service to another system, you will be penalized accordingly.

29. All password changes, except for accounts named ‘root’ or ‘administrator’ MUST be emailed to the White Cell accounts for each team. Failure to do so will result in an inability to test for services and therefore result in a scoring penalty:
    a. Anne Arundel Community College: whitecell@ target81.com
    b. Community College of Baltimore County: whitecell@target82.com
    c. Howard Community College: whitecell@target83.com
    d. Johns Hopkins University: whitecell@target84.com
    e. Millersville University: whitecell@target85.com
    f. Towson University: whitecell@target86.com
    g. University of Pittsburgh: whitecell@target87.com
30. There is to be NO counter-hacking or offensive operations conducted by ANY team. **Failure to adhere to this rule will result in team disqualification**.
31. 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.
32. Academic teams are not allowed to bring electronic copies of configuration files (e.g., iptables) or scripts (e.g., script to change passwords) to the competition (hard copies are allowed however). These must be created during the competition.
33. Academic teams are allowed to bring hard copy documentation, checklists, and technical books with them. These are subject to review by the Gold and White teams and may be permitted or disallowed at the White team’s discretion. If a team has any questions about their documentation selection, they may submit a list of titles they intend to bring to Casey O’Brien (cobrien@ccbcmd.edu) seven days prior to the competition.
34. Teams are required 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 Gold team representative for collection.

Systems

Academic teams will be given close to identical hardware and software installations to configure and support.

Academic teams will not be permitted to bring any computing systems with them.

There will be no software allowed the morning of the State Qualifying Round. After that, teams can use open source and free software (NO trial commercial ware; all software must be 100% free).

Academic teams should not assume any system is properly functioning or secure; they are assuming the role of recently hired administrators and also are assuming responsibility for each of their systems.

Academic 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 10.10.10.4, the Web service must remain available 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 or IP addresses of their assigned systems.

Student teams are not allowed to change service providers (e.g., a wu-ftpd server must stay a wu-ftpd server).

Academic Teams

Each Academic team will consist of up to eight (8) members. Each team member must be a degree-seeking, undergraduate student of the institution the team is representing. Each team is allowed two (2) graduate students from the institution the team is representing.

Each institution must complete the online team roster form by **December 12, 2007**. The form is available at **http://www.cyberwatchcenter.org/ccdc/qual/2008/mdpa/**.

The team members from the State Qualifying Round MUST be the same team members at the Regional CCDC. No substitutions.

Each Academic team may have up to two alternates present at the competition, in the event that a team member becomes ill or injured.

Each Academic team may have one-two (1-2) faculty advisors/coaches present at the competition. The faculty advisor(s) may not assist or advise the student team during the competition.

Each Academic team will designate a Team Captain for the duration of the competition to act as the focal contact point between the Gold team volunteer and the team during the competition.

Red Team Guidelines

The following are guidelines for Red team participation during the CCDC. The primary purpose of this competition is educational and the Red team should keep that in mind throughout the competition. The purpose is not to eradicate the competition or to overwhelm the students – the Red team is to provide a credible, realistic threat to help exercise the student team’s ability to manage and secure their operational networks.

The Red team will be allowed to begin probing the student networks at the start of the competition.

All attacks should be balanced against all the Academic teams, when possible (e.g. attacks used against Team A should be run against the other teams whenever possible).

Anytime unauthorized access is gained, a Red team member will fill out a Red Team Exploit Record Form and submit it to a White team member. The White team will verify access and assess the appropriate penalty for the Academic team.

Careful notes should be taken during the competition so that a debriefing can be conducted at the end of the competition. The Red team should note what techniques were used, when/how they were used, and why those techniques or tools were successful.

Denial of Service attacks are not allowed.

The collection of interesting/sensitive information – such as credit card numbers or employee information – is encouraged. The systems for each team will contain sensitive data the Academic teams should be protecting. When interesting information is obtained, a Red team member should fill out a Red Team Exploit Record Form and submit it to a White team member.

White team members should be notified if any questions should arise.

Scoring

The Red team will be attempting to find and exploit weaknesses in each Academic team's environment. Points will be added to the appropriate team's score based on the severity and type of compromise. For certain categories of compromise, such as root access, points will be added for each *unique* method used by the Red team to compromise the targeted systems. For example, if the Red team is able to gain root access on an Academic team's system using a buffer overflow and by brute forcing an administrator account, each compromise will be scored separately and points will be applied for each.

The winning Academic team will be based on the lowest score obtained during the competition time. Academic teams will not be rewarded for doing their job; that is, keeping functional services running and completing the business "injects" accurately and on time. In addition, academic teams can have points deducted from their score for identifying and reporting un-authorized accesses and compromises. Teams are required to provide incident reports for each Red team incident they detect. **Incident Response forms can be downloaded at the following location: http://www.cyberwatchcenter.org/ccdc/qual/2008/mdpa/**.

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 functionality and content where appropriate. Points will be given for services not meeting these criteria.

Business Injects

Throughout the competition, each team will be presented with identical business injects. These injects will vary in nature and be weighted based upon the difficulty and time sensitivity of the tasking. Tasks may contain multiple parts.

Some examples:

Setting up a secondary DNS server;
Performing a zone transfer between newly created secondary DNS server and the primary DNS server.

Each inject will be delivered via E-mail to the whitecell@target8x.com account (where 8x = your team's target designation. For example, Anne Arundel Community College would be whitecell@target81.com; etc.) and will include the point values and time restrictions associated with the task (e.g., in the event a team doesn't complete the business tasking, the team will know how many points will be added to their score). Teams can prioritize their efforts based on outstanding requests. Upon completion of the injects, a scoring sheet will be signed by the Team Captain and returned to the Gold team judge, who will note the time that the event was/was not completed .

Event Schedule

Saturday, January 12th

08:00 AM
Registration opens. Teams will be registered and gathered in the main room at White Wolf Security.

08:45 AM-12:00 PM
Period 1

12:00-12:30 PM
Lunch

12:30-4:00 PM
Period 2

5:00 PM
Dinner
Presentation and discussion by Red team
Awards ceremony awards