Team Packet
Competition Dates: March 7-9, 2008
v1.0

Table of Contents

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 the District of Columbia, Maryland, and Virginia. This year's qualifying teams include:

1. Community College of Baltimore County
2. George Washington University
3. James Madison University
4. Towson University

•**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, 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.

•**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.

To create a fair and even playing field:

- Each 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. Team members must qualify as full-time students as defined by the institution they are attending - typically this means 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 no more than two (2) graduate students as team members.
- Each team may have advisors present at the competition – this may be a faculty/staff member of the institution or a team sponsor. The advisor(s) may not assist or advise the team during the competition.
- All team members will wear badges identifying team affiliation at all times

during competition hours.
- Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and the teams before and during the competition.

Network Information

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 Academic team will be provided with a standalone PC and direct 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 AIM/chat/E-mail or any other non-public services. For the purposes of this competition, inappropriate content includes pornography or explicit materials, pirated media files or software, sites containing key generators and pirated software, etc. If there are any questions or concerns during the competition about whether or not specific materials are unauthorized, contact a White team member immediately.
- Internet resources such as FAQs, how-to's, existing forums and responses, and company Web sites are completely valid for competition use 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.
- Teams may not use any external, private electronic staging area or FTP site for patches, software, etc. during the competition. All Internet resources used during the competition must be freely available to all other teams.
- Public sites such as Security Focus or Packetstorm are acceptable. Only public resources that every team could access if they chose to are permitted.
- No P2P or distributed file sharing clients or servers are permitted on competition networks.
- All network activity that takes place on the competition network may be logged and is subject to release. Competition officials are not responsible for the security of any personal information, including login credentials that competitors place on the competition network.

- Teams may not remove any computer, printer, or networking device from the competition area.
- Teams should not assume any competition 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.
- Throughout the competition, White team members will occasionally need access to a team's system(s) for scoring, troubleshooting, etc. Teams must allow the White team members access when requested.
- 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 at that IP address throughout the competition.
- Teams are not permitted to alter the system names of their assigned systems.
- Teams are not permitted to remove or alter any labels/stickers that are present on their assigned systems.

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., SSH, IMAP).

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

- The competition will run over a three day period (Friday, March 7th to Sunday, March 9th). Registration will occur on Friday, March 7th starting at 12 PM and a mandatory meeting for all team members and faculty sponsors will be held prior to the start of the competition.
- During the competition team members are forbidden from entering or attempting to enter another team's competition workspace.

- All requests must be submitted via E-mail to the whitecell@target8x.com account. Requests must clearly show the requesting team, action or item requested, and date/time requested.
- Teams must compete without "outside assistance" from non-team members which includes team advisors and sponsors. All private communications (calls, E-mails, 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.
- Teams may not bring any computer, tablets, PDA, or wireless devices 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. Removable USB thumb drives will also be allowed, but must be blank at the start of the competition.
- Teams are not allowed to bring any software with them to the competition (this includes updates and patches to OSes). All Microsoft updates will be from the internal Windows Server Update Service (WSUS) server, not from the Internet.
- Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
- 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 200 point penalty will be assessed against the team.
- Team members will not initiate any contact with members of the Red team during the hours of live competition. Team members are free to talk to Red team members, White team members, other competitors, etc. outside of competition hours.
- On occasion, the White team members may escort individuals (VIPs, press, etc.) through the competition area.
- All individuals involved with the competition will be issued badges which must be worn at all times individuals are in the competition area.
- Teams are permitted to replace applications and services provided they continue to provide the same content, data, and functionality of the original service.
- 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. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the White team before performing those actions.

- Each team may change passwords for administrator-level and user-level accounts. Any password changes must be sent to the the White team account (whitecell@target8x.com) immediately upon change (unless the password changes are part of a competition tasking). Failure to notify the White team of password changes can result in service check failures. 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, when responding to 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. Any firewall rule, IDS, IPS, or defensive action that interferes with the functionality of the scoring engine or manual scoring checks are exclusively the responsibility of the teams.
- The White team is responsible for monitoring the network, implementing scenario events, and refereeing.
- 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.
- 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).
- All systems on the network diagram must be reachable and respond to ICMP pings.
- ICMP and IP traffic must flow between all the teams.
- All services that are tested for must remain open and functional.
- Teams may block by single source IP, but to do so is to run the risk of blocking the scoring engine. If the scoring engine cannot reach the systems, teams will be penalized accordingly.
- Teams cannot block by IP range.
- A complete list of necessary ports/services will be provided on the day of the competition.
- All password changes 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. Community College of Baltimore County: whitecell@ target81.com
    b. George Washington University: whitecell@target82.com
    c. James Madison University: whitecell@target83.com
    d. Towson University: whitecell@target84.com

  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.

- Only Freeware and/or open source tools can be downloaded and used during the competition. 30-day or limited trial periods of commercial ware is strictly prohibited. No commercial products are allowed without prior written approval of the White Cell. There will be periodic audits of the systems. For each copy of software that does NOT meet with these guidelines, the team will be penalized 10,000 points and the software must be removed within the time frame determined by the White team.
- All communications will be via E-mail or Voice Mail. A complete call list will be available on the day of the competition.
- At the end of the CCDC, all passwords must be reset to Chiapet.

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 5pm on Friday, March 7.
- 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. All teams must complete at least two Network Incident Response forms and open two cases with the attendant Secret Service Agent. Incident Response forms can be downloaded at the following location: www.cyberwatchcenter.org/ccdc/docs/Incident_Response_Form.pdf.

- 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.
- 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 engine 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 a member of the White team to address the issue.
- Any team that tampers with or interferes with the scoring or operations of another team's systems will be disqualified.
- A thorough incident report that correctly identifies a successful Red team attack will reduce the Red team's penalty by up to 50 percent – no partial points will be given for incomplete or vague incident reports.
- Scoring will be a combination of automated tools and manual checking.
- 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.

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 an Intranet We server;
- Performing a zone transfer between a secondary DNS server and the primary DNS server.

Each inject will be delivered via E-mail to a specified account 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

Friday, March 7th

12:00 PM
Registration opens. Teams will be registered and gathered in the competition room at White Wolf Security.

12:45 PM
Opening announcements

1:00 PM
Day one competition begins

5:00-6:00 PM
Dinner

8:00 PM
Day one competition ends; post-competition party (details to follow)

Saturday, March 8th

08:45 AM
Teams gathered in the competition room at White Wolf Security. Announcements for day two.

9:00 AM
Day two competition starts

12:00-1:00 PM
Lunch

5:00-6:00 PM
Dinner

7:00 PM
Day two competition ends; post-competition party (details to follow)

Sunday, March 9th

08:45 AM
Teams gathered in the competition room at White Wolf Security. Announcements for day three.

9:00 AM
Day three competition starts

12:00 PM
Day three competition ends. Lunch

2:00-4:00 PM
De-briefing with U.S. Secret Service, Red team, and White team. Awards ceremony