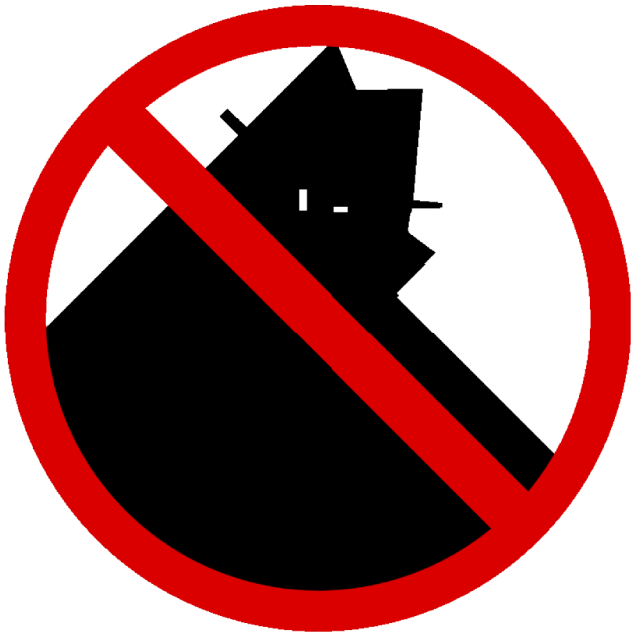
NATIONAL CYBER DEFENSE COMPETITION

Competition Rules



IOWA STATE UNIVERSITY INFORMATION ASSURANCE CENTER
SPRING 2011

Definitions

CDC: Cyber Defense Competition

ISEAGE: Internet Scale Event Attack Generation Environment (a simulated Internet).

Blue Team: Current students from Iowa colleges and the 2010 CDC winners playing the role of the Information Assurance community. This team must identify and defend against various security threats via the ISEAGE network.

Red Team: Comprised of professionals from the Information Assurance community playing the role of hackers. This team must create and implement various attack strategies against the Blue Teams, and capture flags from the Blue Team servers.

White Team: Comprised of respected individuals from the Information Assurance community and ISEAGE. This team is the judging authority for the CDC.

Green Team: This team consists of members with various computer familiarity and skill levels. They play the role of typical network users. The Green Team duties include regular Internet usage and the execution of predefined anomalies.

Flag: Is a PGP-encrypted file placed in a predefined location. The Red Team must capture these flags from teams' systems. The Red Team is also tasked with planting them onto teams' systems.

Anomalies: Random events typical in real-world IT management. These events are injected into the system at various times throughout the competition. Anomalies are designed to test, or simply just complicate, the Blue Team duties during the competition.

CDC Director: Oversees the operation of the overall event, leads the White Team in scoring and adjudication, and coordinates the Red, Green, and Blue Teams.

Objectives

The purpose of the Cyber Defense Competition is to provide students with a simulation of real-life experiences in Information Assurance for the purpose of education. Students play the role of the Blue Team, or Information Assurance community, under fire from the Red Team, simulating the attackers of a network. The White Team oversees the competition, judging (and scoring) each Blue Team based upon Red and Green Team reports received. The Green Team plays the role of general network users, and the strain they place upon ensuring security within a network.

The Blue Team with the most points at the end of the competition will be named the winner.

Blue Teams

- siteN.cdc.com (subnet provided by ISEAGE)
- Minimum 4 persons per team
- Use of an Intrusion Detection System is encouraged, but not required

(we recommend the 'SNORT' IDS with the 'BASE' or 'SNORBY' web interface)

- Required Services
  - Web Server (image is provided)
    - www.siteN.cdc.com
    - This FreeBSD server will be provided, pre-configured, to all teams. Team must patch vulnerabilities on this server
    - Can only be re-installed by incurring a score penalty, so please be careful!
    - Web server must have FTP access for all users (on port 21), users have personal web space located in their 'public_html' directories (such as /home/dave/public_html); this must remain available to all users with system accounts
  - E-mail Server (IMAP and SMTP accessible)

- mail.siteN.cdc.com
- Must accept email for siteN.cdc.com (e.g., bob@site1.cdc.com)
- Must be able to send mail out of the local network (e.g. bob from site1 can send mail to dave@site2.cdc.com)
- Must allow IMAP access to clients
- Must allow SMTP access to clients
- (you may provide webmail access if desired, but you will still be required to provide IMAP and SMTP services)

  - Windows Remote Desktop (image is provided)

- rdp.siteN.cdc.com
- This service will be need to provide all programs listed in the NCDC scenario document. This server was given to you with these programs pre-installed.
- Users cannot be kicked off of this machine, doing so can result in very stiff red team score penalties

- Shell Server (server OS must be a free open-source Linux or BSD distribution)
  - shell.siteN.cdc.com
  - Must provide logins via SSH
  - File system limits may not be set to less than 1GB of total space per user, and a minimum file size of 250MB. Process limits may not be set to less than 25

processes.

- Users cannot be kicked off of this machine, doing so can result in very stiff red team score penalties

- The final list of users and passwords has been provided to each team along with this document

- You cannot change these users' passwords

- Green Team leader may request you change password during the competition, doing so at the Green Team leader's request is required

- These accounts must work for the shell, e-mail, web, and RDP systems

- Required Flags for Red Team Capture.

  - You will be required to maintain one “flag” for each of the required services. Once setup commences, you will be given these flag files. The flags must reside in (and **not** in a subdirectory of):

    - Web Server: Your root's home directory

    - E-Mail Server: C:\Documents and Settings\Administrator (if using Windows) or root's home directory (if using Linux / BSD

    - RDP Server: C:\Windows

    - Shell Server: root's home directory

  - Flags are intended to represent data stored in each of these directories, and thus cannot have more restrictive access permissions that other files in the directory. That means that you can't just remove read rights from the file specifically. They cannot be compressed, encrypted, encoded, or in any other way obfuscated. Violation of any of these rules means you lose all points for that specific flag.

  - If the Red Team determines a flag is missing, it will be considered captured unless the Blue Team can prove it is present.

  - See the Red Team section for scoring information

- Software

  - Must be one of:

    - Free (gratis)

    - Provided by ISEAGE (see Provided Software)

    - Available to students freely (such as MSDNAA software)

- Custom-written by a member of your team. Source code most be developed by your team alone and can not be outsourced to a third party (must be approved by Competition Director at least one week in advance).

- Network Documentation

  - You must provide this prior to the scheduled start of the competition. It may constitute

up to 100 points and should include:

- Network Diagram(s)
- Operating System list (including versions and which service(s) it is running)
- IP address list (including NATed addresses, if applicable)
- Any special measures you've taken to secure your network
- Anything else that you feel demonstrates your preparedness to the White Team

- It may be provided in hard-copy or digital form to the White Team
- Be brief, to the point, and very professional (e.g. no comic sans font)
- It is scored on:
  - Detail (0-40 pts)
  - Professionalism (0-30 pts)
  - Supporting diagrams, figures, and tables (0-20 pts)
  - Effectiveness of plan (0-10 pts)
- The Network Documentation score will decrease by 25% for every 30 minutes it is late, first penalty takes effect at 8:30am sharp.

- Green Team Documentation
  - You must provide this prior to the scheduled start of the competition. It is worth up to 100 points and should include:
    - Instructions for users with little or no computer experience on how to use all of the services you have provided
    - Whom to contact if there is a problem (and how)
  - It must be provided in hard-copy to the Green Team leader prior to the competition. Remember that the usability scores given by Green Teams will be severely affected if this documentation is not present.
  - It is scored on:
    - Detail (0-20 pts)
    - Clarity (0-40 pts)
    - Professionalism (0-20 pts)
    - Supporting graphics, figures, and diagrams (0-20 pts)
  - The Network Documentation score will decrease by 25% for every 30 minutes it is late, first penalty takes effect at 8:30am sharp.
- Hardware
  - Each team will be provided access to a VMWare ESXi server. During the competition there WILL NOT be hardware present to manage the ESXi installation from. This means that your team should bring laptops to the competition as a front-end to the

virtualization system. We will provide a safe network, isolated from the red team attacks, onto which you can connect your personal computers and manage the ESXi server. If this is a problem for your team please let the competition director know

- The Blue Teams will be held accountable for missing or damaged hardware at the end of the competition. If hardware becomes damaged or is missing, contact the Competition Director immediately.
- If hardware fails during the competition, please contact the Competition Directory immediately and White Team will respond accordingly.

- User data is very important! System integrity is essential, and you will be heavily penalized for loss of users' personal data.
- Setup will be available remotely 24/7 via a remote desktop connection into your ESXi installation., but only supported during specific hours of the day, which will be announced and posted in advance. If an ISEAGE staff member is not available on site, you can submit support requests to chris.marczewski@gmail.com. Please always include your team number in correspondence. Rules clarifications or procedural questions should also be sent to that address. Teams are encouraged to seek help from anyone (including white team members) during this phase. If an ISEAGE staff member is available, telephone support will be available at (515) 292-0492.

- Attack Phase
  - You are not allowed to specifically block or ban specific IPs or IP ranges; doing so is unrealistic and completely ineffective in the real world of IT. Automated systems that block after x failed login attempts, however, are allowed. If applicable, please justify any blocks made after x failed login attempts within your network documentation.
  - Service Uptime
    - To compute this score, an automated scanner will be used which checks each service every fifteen minutes. Each service check is worth twelve points. To compute a team's service uptime score at any point during the competition, the White Team will average the uptime percentages for all services for that team, and multiply it by the ratio of service points available at that time.
  - Intrusion Reports
    - Your team may turn in an intrusion summary report every two hours. This report should summarize any intrusions noted (in your IDS, network monitor tools, etc.), your team's assessment of their impact, and the mitigating measures your team took. A simple printout of a log file will not earn any points. Each report is worth up to 25 points and can be submitted via http://www.cdc.net (from inside the competition network) or in hard copy. They are scored on:
      - Detail (0-7 pts)
      - Supporting evidence (0-5 pts)
      - Insightful analysis (0-5 pts)
      - Mitigating actions (0-8 pts)
  - Blue Teams may **NOT** perform any offensive action toward any other participant or

ISEAGE during the competition. This does include members from both the Red Team and the Green Team. Doing so will result in a penalty up to disqualification of the attacking team.

- Blue Teams may **NOT** receive help from anyone whom is not registered on that team, or from advisers or mentors, during the attack phase. Doing so will result in a penalty of up to 500 points.
- Blue Teams may **NOT** make contact with a Green Team member or Red Team member directly. These contacts must go through the Green Team leader or White Team leader.

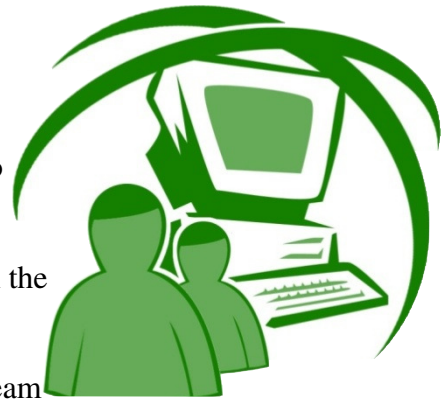
Red Team

- Leader chosen by the competition director
- Skilled members of the Information Assurance community and are selected by the competition director and Red Team leader
- Keep records of every attack for scoring purposes
- No denial-of-service (DoS) attacks
- Must terminate attacks upon request of the White Team
- Attacks cannot leave the ISEAGE environment
- Must obtain flags on each Blue Team's network. Blue Teams start with 200 flags points, and for each of the four flags captured by the Red Team, 50 points are lost. The Red Team must provide the captured flags to the White Team for verification and scoring. Blue Teams may challenge a capture if they feel it is warranted.
- Must plant flags onto Blue Team's network in White Team-designated locations. There are four flags to be planted. Scoring is the same as captured flags (teams start with 200, and lose 50 points for each flag that is planted).
- The Red Team also scores teams on the extent to which they adhere to the spirit of the competition. This accounts for the other 250 Red Team points. This breaks down as:
  - 0-100: Did the team take appropriate measures to secure their network that would hold up in a real-world environment, both technically and politically (e.g., realistic limits on user accounts, appropriate intervention in user activities)?
  - 0-100: Did the team respond to attacks in a rational manner that would be acceptable in a real-world situation (e.g., not blocking large blocks of IP addresses, not killing users' sessions, not removing users' web content)?
  - 0-50: What was the effectiveness of each Blue Team's response to Red Team attacks?
- The Red Team may not have any contact with Blue Teams during the attack phase without direct permission from the White Team Leader. Doing so may result in removal of that Red Team member from the competition.

White Team

- Competition Director and other members chosen by the director
- May not aid or assist teams in any way during the attack phase (other than for judicial or dispute resolution reasons)
- One member must be monitoring the CDC at all times
- Responsible for scoring updates throughout the competition and determining the winner
- Responsible for monitoring service uptime throughout the competition
- Responsible for technical operation of the ISEAGE environment and all CDC systems
- Responsible for resolving disputes during the competition

Green Team



- Leader chosen by the competition director
- Will assess the usability of Blue Team networks by completing normal activities such as browsing the web server, connecting to the shell server, checking and sending email, and opening and editing files via RDP or FTP. Members are not limited to these activities. However, Green Team members must first check with the Green Team Leader before executing any activity that could be defined as malicious or intentionally damaging to a Blue Team network. Failure to do so may result in removal of that Green Team member.
- Various skill levels and backgrounds
- Must fill out a Usability Form upon completion of an evaluation. These forms are available from the Green Team Leader, and must be completed within fifteen minutes of the completion of the evaluation. Each evaluation is worth 50 points.
- The Green Team leader is in charge of executing anomalies, with the assistance of members of the Green, White, and Red Teams. These anomalies will be of various point values depending upon the difficulty of the task.
- The Green Team leader is the custodian of Blue Team password information. This information may not be given to the Red Team without authorization from the White Team. This information should be distributed to Green Team members to use in evaluating Blue Team systems, but Green Team members may not be warned by the Green Team leader about giving this information to the Red Team.
- Members of the Green Team other than the leader may not have direct contact with members of a Blue Team without the Green Team leader present

Parts and Services

Blue Teams will be provided an ESXi server in order to host their network infrastructure and systems. Additional hardware and maintaining an IT budget will not be necessary for this competition.

Software

There is a variety of free software already downloaded and installable over the ISEAGE network (see the Remote Setup handout). Additionally, the following proprietary software is available for installation:

- Windows Server 2003

- Windows XP