

CYBER DEFENSE COMPETITION

Rules



**IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
FALL 2008**

Definitions

CDC- Cyber-Defense Competition

ISEAGE- Internet Scale Event Attack Generation Environment or a simulated Internet.

Blue Team- Students of any participating University 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 or Green teams, and capture flags from the Blue Team servers.

White Team- Comprised of respected individuals from the Information Assurance community, such as professionals and cutting-edge developers. 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 pre-defined anomalies.

Flag – a file in a mandated location which contains a unique string. The Red Team must capture these flags from the teams, and provide the string to the white team to prove their capture.

Anomalies- Random events typical to real world situations. 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. They may require the purchase of additional equipment from the White Team.

Objectives

The purpose 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
- One Station
 - Class-C subnet provided by ISEAGE
- Required Services
 - Web Server (provided)
 - Cannot be reinstalled, only patched and reconfigured
 - Must provide FTP access to web document root
 - Remote Desktop Machine (provided)
 - Users cannot be kicked off of this machine
 - Must provide WinSCP, Eclipse, Firefox, and OpenOffice
 - DNS Server(s) – Consultation Available (see Parts and Services)
 - Must host answer DNS queries for siteN.cdc.com (where N is your team number)
 - IP address given to White Team prior to the competition for registry in the CDC.NET master DNS server
 - CVS Server accessible via SSH. This must host a copy of the web server content for developer access.
 - Intrusion Detection System – Preconfigured Available (see Parts and Services)
 - Required to provide evidence of attacks for White Team reports
- Required Flags for Red Team Capture.
 - You will be required to maintain one “flag” for each of the five required services. Once setup commences, you will be given a unique string for each of these flags. The flag file should contain only this string. The flags must reside in (and **not** in a subdirectory of):
 - Web Server: Your web server’s document root
 - DNS Server: The directory in which your zone files are contained
 - CVS Server: Your CVS root directory
 - Remote Desktop Machine: C:\Windows\System32
 - Intrusion Detection System – The directory containing your intrusion signatures



- See the Red Team section for scoring information
- List of users and their passwords will be provided
 - Must work for Web server FTP, CVS/SSH, and Remote Desktop Machine
 - Neither you, nor any user, may change user passwords
- Software
 - Must be one of:
 - Free (gratis)
 - Provided by ISEAGE (see Provided Software)
 - Custom-written by a member of your team (must be approved by Competition Director at least one-week in advance)
- Network Documentation
 - You must provide this prior to the 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
 - 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)
- Green Team Documentation
 - You must provide this prior to the 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. Late entries will be accepted, for reduced points, up to one hour into the competition.

Entries beyond that window will be accepted (and will indirectly help your green team score), but will not be counted for points.

- It is scored on:
 - Detail (0-20 pts)
 - Clarity (0-40 pts)
 - Professionalism (0-20 pts)
 - Supporting graphics, figures, and diagrams (0-20 pts)
- Hardware
 - Each team will be provided with:
 - 4 computers with a 40GB Hard Drive, a 10/100 Network Card, and 512MB RAM
 - 1 10/100 Hub
 - 4 CAT5/RJ45 (network) cables
 - 1 Power Strip (plus the power strips in the rack)
 - 1 KVM switch
 - 2 sets of monitors, keyboards, and mice
 - Additional hardware can be obtained (see Parts and Services)
 - 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. Your team can replace the hardware out of your team's budget (see Parts and Services).
- Setup will begin three weeks prior to the Attack Phase. Setup will be available remotely (see Remote Setup handout) and will be supported according to the schedule distributed. Teams are encouraged to seek help from anyone (including white team members) during this phase.
- Attack Phase
 - Service Uptime
 - Services will be randomly checked for uptime by an automated scanner. Each successful check gains your team four points. This will be computed periodically.

To compute this score, an automated scanner will be used which checks each service (on average) every five minutes. 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 to that point. For example, if the competition is eight hours long, and

your average service uptime 2 hours into the competition is 95%, your service score at this point would be:

$$\left[\frac{2 \text{ hrs}}{8 \text{ hrs}} * \left(\frac{12 \text{ checks}}{1 \text{ hr}} * \frac{4 \text{ pts}}{1 \text{ check}} * 8 \text{ hrs} \right) * .95 \right] = 92 \text{ pts}$$

Thus, the maximum score possible for service uptime during an eight hour competition is 384.

○ Intrusion Reports

- Your team may turn in a bi-hourly intrusion report. This report should summarize any intrusions noted (in your IDS or otherwise), your team's assessment of their impact, and the mitigating measures your team took. A simple printout of the IDS log will not earn any points. This is worth up to 25 points every other hour 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 team or ISEAGE during the competition. Doing so will result in disqualification of the attacking team.
- Blue Teams may **not** receive help from anyone whom is not registered on that team 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

- Led by a 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 attack for scoring purposes
- No distributed attacks



- Attacks cannot leave the ISEAGE environment
- Must obtain flags on each Blue Team's network. Blue Teams start with 250 flags points, and for every flag captured by the Red Team, 50 points are lost. The Red Team must provide a list of captured flags to the White Team at the end of the competition for scoring.
- The Red Team also scores teams on the extent to which they adhered 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)?
 - 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 efficacy of the team's response to Red Team attacks?
- The Red Team will evaluate each Blue Team at the end of the competition and generate their scores for this area. They will also provide their captured flags to the White Team, who will combine these two scores to generate the Red Team score.

White Team

- Competition Director and no more than 5 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 technical operation of the ISEAGE environment and all CDC systems.



Green Team

- Led by a leader chosen by the competition director
- Will assess the usability of Blue Team networks by completing normal activities such as browsing the internet, utilizing CVS, FTPing to the web server, remoting to the Remote Desktop Environment, or opening and editing files. Members are not limited to these activities
- At least two members and the leader must be present at all times
- 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.
- The Green Team leader is in charge of executing anomalies, with the assistance of members of the Green, White, and Red Teams
- 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
- At the end of the competition, the Green Team leader will rank the teams based upon user reports and completed anomalies throughout the night (accounting for any known technical issues), and assign each team a relative score of 0-500 points.
- Teams will also receive a 50 point bonus if every member of the team fills out a competition survey.



Parts and Services

Each team is given the equipment listed in the Blue Team section above. If additional equipment is required, it may be purchased from the White Team. The White Team also offers a preconfigured Intrusion Detection System, a Web Server Recovery service, and a DNS Consultation service.

Each team is given a budget of \$1000IA. For every dollar a team exceeds this budget, they receive a five point penalty. For every five dollars a team is under budget, they will receive one point (up to 100 points).

Teams should keep in mind that if hardware fails during the competition, or an anomaly requires additional hardware, this will come out of their budget.

Item	Cost (\$IA)
Computer (including power cable)	500
10/100 Hub	50
10/100 Network Card	50
Wireless Network Card	50
Wireless Access Point	100
256MB RAM (one stick)	75
512MB RAM (one stick)	100
40GB Hard Drive	100
Network Cable (Straight Through)	20
Network Cable (Crossover)	25
Monitor (including power cable and VGA cable)	100
Keyboard/Mouse (set)	20
KVM Switch	50
Preconfigured Intrusion Detection System (including cables)	600
Web Server Recovery	200
DNS Consultation	100

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 2000
- Windows 2003
- Windows XP