COMMUNITY COLLEGE CYBER DEFENSE COMPETITION (C3DC)

Competition Rules

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Fall 2009

Definitions

CDC: Cyber Defense Competition

ISEAGE: Internet Scale Event Attack Generation Environment (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 teams.

White Team: Comprised of respected individuals from the Information Assurance community, such as professionals and 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.

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.

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

- site**N**.cdc.com
- 4-6 Students
- Services may have their own IP addresses or be behind NAT
- Use of an Intrusion Detection System is encouraged, but not required
  - (we recommend the 'SNORT' IDS with 'BASE' web interface)
- DNS services will be provided by ISEAGE, your team will provide ISEAGE staff with your desired host names and IPs, and staff will configure ISEAGE DNS for you
  - Teams that would rather set up and run their own DNS servers are welcome to do so
- Required Services
  - Web Server
    - This Linux server will be provided, pre-configured, to all teams. Teams must patch vulnerabilities on this server
    - Web server must have FTP access for all users, users have personal web space located in their 'public_html' directories, and this must remain available to all users
  - Email Server (IMAP and SMTP accessible)
    - You may also provide webmail access if desired, but you will still be required to provide IMAP and SMTP services as well
  - Programming Server
    - Must be a *nix-based server (Linux, FreeBSD, etc) with SSH access
  - Windows Remote Desktop Server (RDP)
    - This Windows 2003 server will be provided, pre-configured, to all teams. Teams must patch vulnerabilities on this server and secure user accounts
    - Users cannot be kicked off of this machine, doing so can result in a very stiff red team score penalty
  - List of users & passwords will be provided by the White Team leader at a later date
    - You cannot change passwords, users should not be allowed to change them either
    - Green Team leader may request you change passwords during the competition, doing so at the Green Team leader's request is fine

- Software
  - Must be one of:
    - Free (gratis)
    - Provided by ISEAGE (see Provided Software)
    - Available to students freely
    - Custom written by a member of team (and approved by Competition Director)
- Network Documentation
  - You must provide this prior to the start of the competition. It must 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 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 (i.e. no comic sans font)
  - Judged upon:
    - 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 must 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
  - Judged upon:
    - Detail (0-20 pts)
    - Clarity (0-40 pts)
    - Professionalism (0-20 pts)
    - Supporting graphics, figures, and diagrams (0-20 pts)

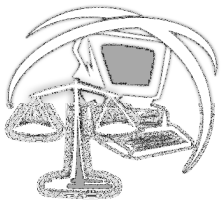
- Required Flags
  - In order to discourage red team from the "slash and burn" approach, we've implemented a form of capture the flag into the competition
  - Before the competition, you will be provided with these flags in the form of a .gpg file, and you will be instructed to place them in specific areas on your various servers; you will not be told where this specific areas are until you receive the flag files prior to the competition
  - You are NOT allowed to simply block access to the flag specifically
  - See the "Read Team" section for more specific scoring information
- Hardware
  - Each team must design their network from scratch within its budget. ISEAGE staff will construct your network as you request.
  - 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 it can be replaced, but service downtime penalties may still apply (at the discretion of the White Team)
- User data is very important! If you lose your user's personal data, there will be anger from your green team users, and that can be bad scores!
- Setup will be available remotely 24/7 via a remote desktop connection into a KVM, but only supported during specific hours of the day, which will be announced and posted in advance. Teams are encouraged to seek help from anyone (including white team members) during this phase.

- Attack Phase
  - Do not block or ban specific IPs or IP ranges, doing so is unrealistic and completely ineffective in the real world of IT.
  - 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
  - Intrusion Reports
    - Your team may turn in an intrusion report every two hours. 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 can **not** make contact with a Green Team member or Red Team member directly during the competition. 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 the competition director and Red Team leader
- Keep records of every attack for scoring purposes
- No distributed (DoS) attacks
- Attacks can not 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
- Must plant flags onto Blue Team's network in White Team-designated locations. When a flag is planted, the White Team should be contacted for verification. There are five flags to be planted. Scoring is the same as captured flags (teams start with 250, and lose 50 points for each flag that is planted)
- 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

White Team



- Competition Director and no more than 5 other members chosen by the director
- May not directly 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

- Leader chosen by the competition director
- Will assess the usability of Blue Team networks by completing normal activities such as checking email, browsing the internet, or opening and editing files via RDP and FTP. Members are not limited to these activities
- Will routinely create data on the various services and check again periodically to ensure that their data has not been removed or lost during a restoration of the system
- 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

Parts and Services

Blue Teams must design their network from scratch within a budget. For a fee, the White Team offers a Web Server and RDP Server Recovery image (for those Oops! moments). Each team is given a budget of $700, which may not be exceeded. For every five dollars a team is under budget, they will receive one point (up to $100).

You are already provided 4 servers at no cost, with 512MB RAM, 40GB HDD, and one 10/100 NIC each. Should you desire more servers, they can be purchased (see price list below).

If hardware fails during the competition (due to a team's own error), or an anomaly requires additional hardware, this will need to come out of their budget, so it is wise to leave a little wiggle room. Cables, power strips, KVMs, chairs, keyboards, monitors, and mice come free of charge.

Item Costs:

Computer with 512MB RAM, 40GB HDD, and one 10/100 NIC	$500
10/100 Hub	$50
10/100 Network Card	$50
Wireless Network Card	$50
Wireless Access Point	$100
256MB RAM (one stick)	$50
512MB RAM (one stick)	$100
40GB Hard Drive	$100
Web / RDP Server Recovery	$200
Backup Power (UPS)	$100

Software:

There is a variety of free software already downloaded and installable over the ISEAGE network. ISEAGE staff will download, burn, and insert installation CDs/DVDs at a team's request. Additionally, the following proprietary software is available for installation:

- Windows 2000
- Windows 2003
- Windows XP