COMMUNITY COLLEGE CYBER DEFENSE COMPETITION

Competition Rules

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
FALL 2011

Definitions

CDC – Cyber Defense Competition

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

Blue Teams - Competitors playing the role of the Information Assurance community. These teams 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. 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 - a PGP-encrypted file placed in a predefined location. The Red Team much capture these flags from or plant them onto teams' systems.

Anomalies - These events are injected into the system at various times throughout the competition. The Anomalies are designed to test, or simply just complicate, the Blue Team duties during the competition.

CDC Director - Oversees the operation of the CDC portion of IT Adventures, leads the White Team in scoring and adjudication, and coordinates the Red, Green, and Blue Teams.

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.

Scoring

Historically this document has detailed scoring methodology. To foster a better understanding of our scoring system, this information has been condensed and moved to another dedicated scoring document which you will receive with your bundle of initial materials.

Blue Teams

- site**N**.cdc.com (subnet provided by ISEAGE)
- Minimum of 4 persons per team, maximum of 6
- Must allow access to all services from any IP or network
- If your team damages a 'provided' service beyond the point of recovery, the white team can restore an image of the system, but your team will incur a scoring penalty of 75 points per re-install.
- Required Services
  - Web Server **(openSUSE, already provided)**
    - www.siteN.cdc.com
    - Cannot be re-installed, only patched and reconfigured
      - Things allowed: all package/kernel/OS updates
      - Not allowed: installing a whole new operating system from scratch and migrating the content over from the old system
        - Ask the director if you need further clarification!
    - Must provide FTP access for all users to access their home directories on port 21
    - Apache must allow users to create home pages in /home/username/public_html that are accessible from http://www.siteN.cdc.com/~username
  - Cloud Desktop Server **(eyeOS, already provided)**
    - cloud.siteN.cdc.com
    - Cannot be re-installed, only patched and reconfigured
      - Things allowed: all packages and manual kernel patching
      - Must stay in core OS version 1.9.0
        - Ask the director if you need further clarification!
    - Must allow access to all user accounts
  - Shell Server
    - shell.siteN.cdc.com
    - Must provide access via SSH and SFTP (for file transfers)
    - 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.
    - Must provide access to GCC and be able to compile a 'Hello World' program in C++

- 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 to the greater ISEAGE network, including green team users (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.
  - Incoming and outgoing messages should be checked for viruses and other malware. The sender of the e-mail should be notified if an e-mail is deemed malicious if an action is taken against that e-mail. For example, the whole e-mail may be dropped and a notification sent to the sender. Or the text of the e-mail may be sent untouched, but the attachment should be removed. The exact method is left up to Blue Teams. Green Team will use a harmless standard test virus to test for this functionality. Note that compressed archives should be checked as well, so that the virus can't be hidden inside a .zip, .gzip, or .bz2, etc. If a compression format can't be handled it should be rejected, and the sender told to resend the attachment using a compression format that can be scanned.

- NTP (Network Time Protocol) Synchronization
  - All systems are required to have accurate time within 10 seconds of the provided NTP server at: ntp.cdc.net (this server is only available on the competition network).
  - The built-in time keeping and syncing capabilities of Windows may be used, so it won't be necessary to install NTP separately on Windows systems. We leave it up to your team to determine how you want to sync time on any Windows servers you may have with our central NTP server.
  - The shell server must allow regular users to run the "ntpq" command, and then run the "pe" command (within ntpq) to see the list of NTP peers.
  - You may sync all your systems with the provided NTP server at ntp.cdc.net, or set up one of your own that provides NTP to your network. A firewall system would be a good system to run an NTP server from. Just be sure that your time throughout the network remains in synchronization with our NTP server at ntp.cdc.net

- 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 sub-directory of):
    - Web Server: Root's home directory (usually "/root")

        - Cloud Desktop Server: /root/system/kernel
        - Shell Server: Root's home directory (usually "/root")
        - E-Mail Server: C:\Documents and Settings[or "Users" in 2k8]\Administrator (if using Windows) or /root/ (if using Linux / BSD)
    - 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. They cannot be compressed, encrypted, encoded, or in any other way obfuscated.
    - 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
- List of users and their passwords will be provided
    - Must work for web (for FTP), cloud desktop, mail, and shell server
    - Passwords cannot be changed unless you are instructed to by the Green Team Leaders
    - Users can be fired from the company and must have their access removed swiftly if this occurs. See the scenario document for more information.
- Software
    - Must be one of:
        - Freeware or Open-Source
        - Provided by ISEAGE (see Provided Software)
- 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 30 minutes after the competition begins.
- 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
        - An e-mail address to contact if there is a problem. If you do not provide this information green team will not make you aware of issues. You've been warned!
    - 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. We will have a printer available on-site for PDFs.
    - 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 Green Team Documentation score will decrease by 25% for every 30 minutes it is late, first penalty takes effect 30 minutes after the competition begins.
    - 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.
- Green Team Communication
    - During the event, the Green Team may communicate with the Blue Teams either through an announcement or e-mail. When an announcement is made, one member of each Blue Team must report to the Green Team Leader for instructions. E-mail accounts will be provided for each team. They will be IMAP based, so that more than one person may monitor them at a time. Anomalies and other information may be sent via e-mail to these address, so they MUST be monitored through the event. More information on the e-mail accounts will be given at a later time.
- Hardware
    - Each team will be provided access to a VMWare ESXi 5.0 server. During the competition there WILL NOT be hardware present to manage the ESXi installation from. This means that your team should bring Windows laptops to the competition as

a front-end to the virtualization environment. Mac and Linux users will have an RDP server available with management software preinstalled; more details will be provided at the competition. 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 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 Director immediately and White Team will respond accordingly.

- Setup will begin on Friday, Nov 11th. 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 c3dc11_support@iastate.edu. Always include your team number in correspondence. Rule clarification or procedural questions should also be sent to that e-mail address. Teams are encouraged to seek help from anyone (including White Team members) during this phase.
- 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 connects for a few minutes after N failed login attempts, however, are allowed. If applicable, please justify any blocks made after N failed login attempts within your network documentation.
  - Service Uptime
    - An automated scanner will be used to check if your services are online. This data will be processed and incorporated into scoring results.
  - Intrusion Reports
    - Your team may turn in an intrusion summary report once every 2 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 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. 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 (excluding 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

- Led by a leader chosen by the Competition Director
- Are skilled members of the Information Assurance community and are selected by the Competition Director and Red Team leader
- Keep records of attacks
- No denial-of-service 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 400 flags points, and for each of the four flags captured by the Red Team, 100 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 400, and lose 100 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. 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

- Led by a leader chosen by the Competition Director
- Assess the usability of Blue Team networks by completing normal activities such as browsing the web server, connecting to the file server, or logging into the remote desktop server. Members are not limited to these activities.
- 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. 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.