IT-ADVENTURES: CYBER DEFENSE COMPETITION

Rules

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
SPRING 2010

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. 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.

Blue Teams

- site**N**.cdc.com (subnet provided by ISEAGE)
- Required Services
  - Web Server (provided)
    - www.siteN.cdc.com (your.sub.net.50)
    - Cannot be reinstalled, only patched and reconfigured
    - Comes with a certificate signed by CDC corporate for HTTPS (don't lose this!)
  - Mail Server
    - mail.siteN.cdc.com (your.sub.net.100)
    - Must accept email for siteN.cdc.com (e.g., bob@site1.cdc.com)
    - Must be able to send mail out of the local network
    - Must allow IMAP/S access to clients
    - Comes with a certificate signed by CDC corporate for IMAP/S (don't lose this!)
  - File Server
    - file.siteN.cdc.com (your.sub.net.150)
    - Must provide logins via SSH and SCP
    - File system limits may not be set to less than 1GB of total space per user, and a minimum file size of 100MB. Process limits may not be set to less than 25 processes.
- 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 web server’s document root
    - Mail Server: Kathy’s home directory
    - File Server: Robert'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. 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 mail server and file server
  - Passwords cannot be changed without approval from the White Team
- 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 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
  - 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 5% for every 15 minutes it is late
- 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 10% for every 15 minutes it is late

- Hardware
    - Each team will be provided with a common set of hardware. See the end of this document (Parts and Services) for more information.
    - 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.

- Setup will begin on April 5th. Setup will be available remotely (see Remote Setup handout) and will be supported to the extent possible 8-5 M-F. Support requests should be sent to itacdc10_support@iastate.edu. Rules clarifications or procedural questions should be sent to itacdc10_director@iastate.edu. Teams are encouraged to seek help from anyone during this phase. Telephone support is available at 515-292-0492.

- Attack Phase
    - Service Uptime
        - To compute this score, an automated scanner will be used which checks each service every five minutes. Each service check is worth four 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 to that point. For example, if the competition is 8 hours long, and your average service uptime after 2 hours is 95%, your service score at this point would be:

          $$\left\lceil \left(8\,hrs \cdot \frac{4\,pts}{chk} \cdot \frac{12\,chks}{hr} \right) \cdot \frac{2\,hrs}{8\,hrs} \cdot 0.95 \right\rceil = 92\,points$$

          Thus, the maximum score possible for service uptime during the eight hour competition is 384.
    - Intrusion Reports
        - Your team may turn in an intrusion summary report once every other hour. 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, or from advisors 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 distributed 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 150 flags points, and for each of the three 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 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 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 efficacy 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
- Will assess the usability of Blue Team networks by completing normal activities such as browsing the web server, connecting to the file server, or checking and sending email. 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. 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

Teams are provided with:

- A web server with 512MB RAM, 40GB hard drive, and a 10/100 network card
- A firewall with 512MB RAM, 40GB hard drive, and two 10/100 network cards
- Two open computers with 512MB RAM, 40GB hard drive, and a 10/100 network card
- One Gigabit switch
- One 10/100 Hub
- Three sets of monitor/keyboard/mouse
- Two KVM switches
- Cables, power strips, and furniture as needed.

Software

There is a variety of free software already downloaded and installable over the ISEAGE network (see the Remote Setup handout). You may ask the ISEAGE staff to download other disc images and burn them to CD for you. Additionally, Windows 2003 is available for installation by the ISEAGE staff.