ISU Cyber Defense Competition

Competition Rules

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER

Fall 2014

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 file placed in a predefined location. The Red Team must 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 Teams' duties during the competition.
Competition Director – Oversees the operation of the CDC, leads the White Team in scoring and adjudication, and coordinates the Red, Green, and Blue Teams.
IScorE – The web-based scoring application tailored to the CDC. IScorE may be used by all teams to submit, view, and alter scores. Located at https://iscore.iseage.org

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. See the scoring document for more information.

Blue Teams

Students will form teams of 4-8 to tackle the challenge laid out in the Scenario document. They will set up and secure a network that is usable by the Green Team while defending it against attacks from the Red Team.

Each Blue Team will be assigned a domain name (teamN.isucdc.com) and a subnet of IPs on which to make their services available on the ISEAGE network. See the “IP Ranges and Network Information” document for more information.

Some of the services in the scenario will be provided and will need to be secured. If a Blue Team damages a provided service beyond the point of recovery, the White Team can provide a fresh image of the system, but the Blue Team will incur a scoring penalty of **75 points** per re-install.

Blue Teams may not perform any offensive action toward any other participant or ISEAGE during setup or the competition. Doing so will result in a penalty up to disqualification of the attacking team.

Blue Team members are responsible for any ISEAGE accounts assigned to them for use in the CDC environment (Remote Desktop, vCenter, chat accounts). Any actions performed on these accounts will be attributed to the team who the account is assigned to, and penalties will be assigned accordingly if necessary. **Therefore, do not share your CDC credentials with anyone.**

Remote Setup

Setup will be available remotely 24/7 (see the Remote Setup document). ISEAGE provides online support via chat, available at https://setup.iseage.org. Setup chat is only staffed during specific hours of the day; these hours will be posted on the calendar located on the setup chat login page. If an ISEAGE staff member is not available to chat, you can submit support requests to cdc_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) during this phase.

Hardware

Each team will be provided access to the VMware vCenter server environment. The white team operates the administrative accounts on vCenter. These accounts will not be used maliciously; you will not need to worry about securing the VMware environment.

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 or there is a suspected network outage, please contact the Competition Director immediately.

Software

All software used in the competition must either be freely available or provided by ISEAGE (see the Remote Setup document). Trials of non-free software that do not exceed the trial period are allowed.

Accounts and passwords

- List of users and their passwords will be provided
- Must work for the services described in the Scenario document
- You may ***NOT*** change the password for any required user unless instructed to by the Green Team Leader
- Users may be fired from the organization and must have their access disabled or removed swiftly if this occurs. See the scenario document for more information.
- Some passwords are specific to individual teams. They are denoted by “********” and will be provided on IScorE.

Required Flags for Red Team Capture

See Scenario for required flag locations

You will be required to maintain a “flag” for some of the required services (see the Scenario document). Once setup commences, you will be given these flag files via IScorE.

Flags are intended to represent data stored in each of these directories, and thus cannot have more restrictive access permissions than other files in the directory. They cannot be compressed, encrypted, encoded, or in any other way obfuscated.

In addition to planted flags, there may also be sensitive data that Red Team will want to capture such as passwords, financial information, etc., which may be located in files or databases. If Red Team manages to capture this sensitive data you will lose flag points for each item lost.

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 and the Scoring document for more details.

Network (White Team) Documentation

White team documentation represents the reports that real-world companies require of their IT staff. In it, you should explain, in detail, your plan for setting up and securing your network. You must provide this prior to the scheduled start of the competition by submitting it on IScorE. It is worth up to **100 points** and should include:

- Details of your network layout (IP addresses, firewalls, whether you have chosen to use NAT)
- Network Diagram(s)
- Discussion of the Operating Systems, Software, etc. you have chosen to run each of your services
- Discussion of special measures you've taken to secure your network (Intrusion Detection Systems, specific firewall rules, mandatory access controls, etc.)
- Anything else that you feel demonstrates your preparedness to the White Team

This document needs to be professional and thorough. 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. The first penalty will take effect 30 minutes after the competition begins.

Green Team Documentation

Green team documentation instructs your users (the Green Team) on how to use your services. You must submit this prior to the scheduled start of the competition on IScorE. Keep in mind that the usability scores given by Green Teams will be severely affected if this documentation is not present! Teams often underestimate the importance of usability - it can easily make or break the competition. Ensure your networks have a good balance between usability and security.

This documentation 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. **HINT:** You may find a screen capture program such as Jing (http://www.techsmith.com/jing.html) extremely helpful in completing your documentation.

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. The first penalty will take effect 30 minutes after the competition begins.

On-Site Setup

During the competition there WILL NOT be hardware present to manage the vCenter environment from. This means that your team should **bring laptops to the competition** as a front-end to the virtualization environment. We will provide a safe network, isolated from the red team attacks, onto which you can connect your personal computers and manage the vCenter environment. If you do not have a computer available, let the Competition Director know before you arrive and the ISEAGE staff can accommodate you.

Attack Phase

During the attack phase, the Red Team will arrive on-site and attempt to gain access to your services in order to capture flags, reduce usability, or take the services offline. This will begin at 8am on the day of the competition. We will announce the start of the attack phase on the competition floor before it begins.

Blue Teams 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 connections for a few minutes after N failed login attempts (e.g. fail2ban) are allowed. If applicable, please justify any blocks made after N failed login attempts within your network documentation. The competition director reserves the right to determine whether an IP blocking policy is beyond realistic and breaking the rules.

Blue Teams may **not** receive help from anyone not registered on that team (including advisors or mentors, professors or friends) 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.

Green Team Anomalies

In the real world of IT there is never a dull moment. Green team anomalies simulate the never-ending stream of requests that everyday IT employees must be prepared to handle. During the competition, anomalies will be released via IScorE. They are worth varying point values based on their difficulty. Blue teams will need to submit anomalies before they expire to gain points.

Completion of anomalies is **optional** unless the anomaly specifies otherwise. However, blue teams that refuse or do not submit an anomaly will not be awarded any points for it. Anomalies will account for a significant amount of points and are highly encouraged.

Green Team Communication

During the event, the Green Team may announce instructions. When an announcement is made, one member of each Blue Team must report to the Green Team Leader for further instructions.

Service Uptime

IScorE's automated service scanner will be used to check if your services are online every few minutes. This data will be automatically incorporated into scoring results.

Intrusion Reports

In real-world IT, management will require regular reports on the security of your network, as well as in-depth analysis of any intrusions. Blue Teams may turn in an intrusion summary report at 10 am, 12pm, 2pm, and 4 pm. This report should cover, in detail, any intrusions noted (in your IDS or otherwise), your team's assessment of their impact, and the mitigating measures your team took, along with evidence to support your analysis. **A simple printout of a log file will not earn any points, nor will a "No Intrusions Detected" without any evidence to back it up.** Each report is worth up to 25 points and must be submitted via IScorE. They are scored on:

- Detail **(0-7 pts)**
- Supporting evidence **(0-5 pts**)
- Insightful analysis **(0-5 pts)**
- Mitigating actions **(0-8 pts)**

Red Team

The Red Team represents the "bad guys" – malicious users, advanced persistent threat, or other agents that may want to cause harm to a Blue Team's infrastructure. The Red Team is staffed by professionals in the Information Assurance community chosen by the Competition Director and the Red Team Leader. The Red Team will evaluate the efforts of the Blue Teams at the completion of the Attack Phase.

Red Team Leader

The Red Team leader is chosen by the Competition Director and will coordinate with the White Team Leader to ensure a fair and successful competition. The Red Team leader will serve as a mediator between the Red Team members and the White Team to settle any scoring disputes, and will, if necessary, set boundaries for attacks to keep the competition running smoothly.

Attack Phase

Red team members will keep detailed accounts of all attacks performed. IScorE will provide a place to document all offensive actions taken. These documents will be made available after the competition.

Requirements

- Attacks cannot leave the ISEAGE environment
- Must terminate attacks upon request of the White Team
- Will attempt to obtain flags on each Blue Team's network (see "Required Flags for Red Team Capture"). Blue Teams start with a given number of flags, and for each of the flags captured by the Red Team, a number of points are lost. The Red Team must submit the captured flags via IScorE for verification and scoring. Blue Teams may challenge a capture if they feel it is warranted.
- Will attempt to plant flags onto each Blue Team's network in White Team-designated locations.
- In addition to required flags, sensitive information (e.g. credit card numbers, Social Security numbers, etc) will be present on some systems; see the scenario document for more information.

Red Team Evaluation

At the conclusion of the attack phase, the Red Team will evaluate teams on the extent to which they adhere to the spirit of the competition. This breaks down as:

- **0-100 points:** 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 of user activities, not breaking functionality such as web-based file uploads, etc)?
- **0-100 points:** Did the team respond to attacks in a rational and appropriate manner that would be acceptable in a real-world situation, even if this was simply by having no response (e.g., not blocking large ranges of IP addresses, not killing users' sessions [whack-a-mole], not removing the users' web content)?
- **0-50 points:** The "non-arbitrary" catch all including: physical security, social engineering, overall conduct (removal of points for derogatory "messages" to red, white, green, or

blue), or any other noteworthy factors.

White Team

The White Team will be led by the Competition Director. The White Team is responsible for setting up and maintaining the ISEAGE network, IScorE, and all CDC infrastructure, as well as running the competition. At least one White Team member must be present at all times during On-Site Setup and the Attack Phase.

White Team Members

White Team members will be chosen by the Competition Director. The White Team may not aid or assist teams in any way during the attack phase except to resolve disputes.

Grading and Scoring

The White Team is in charge of grading all Documentation and Intrusion Reports. They are also the final authority on any scoring disputes and will assign penalties if necessary. At the end of the competition, they will determine the final placement of Blue Teams.

Green Team

The Green Team represents the users of a Blue Team's infrastructure. They will score each Blue Team on the usability of their services.

Green Team Leader

The Green Team Leader will coordinate the efforts of the Green Team members in order to assess the Blue Teams fairly. The Green Team Leader will also coordinate with the Competition Director in the creation of Green Team Anomalies, and with Green, White, and Red Team members in their execution.

The Green Team Leader is the custodian of Blue Team password information and must authorize any password changes by Blue Teams.

The Green Team Leader must be present if a Green Team member wishes to confer with a Blue Team. Blue Team members with questions regarding scoring of Usability or Anomalies should confer with the Green Team Leader.

Green Team Members

Just like in real-world IT, Green Team members will be of varying technical skill and ability. Green Team members will score Blue Teams in several Usability Checks during the attack phase by completing normal activities such as browsing the web server, connecting to the file server, or logging into the remote desktop server. They will fill out a Usability Form on IScorE during evaluation.

Green Team members will also, with the assistance of the Green Team Leader, score Anomaly submissions.

Green Team members may NOT confer with Red Team members during the Attack Phase. They may not, under any circumstances, give passwords or other sensitive Blue Team information to the Red Team. Additionally, Green Team members may NOT intentionally perform attacks or malicious actions against any Blue Team. Unruly Green Team Members may be asked to leave by the Green Team Leader or the Competition Director.