IT-OLYMPICS CYBER DEFENSE COMPETITION

Competition Scoring Guide

IOWA STATE UNIVERSITY INFORMATION ASSURANCE CENTER
SPRING 2013

Scoring Design

For the last few years, scoring at the Iowa State University-sponsored CDCs has remained largely unchanged. After the 2010-2011 academic year, ISEAGE staff and volunteers decided to re-create scoring from scratch. This document is the fruit of that effort.

Scoring Weights and Categories

Service Scans

15% of overall score

An automated service scanner, IScorE, will attempt to access your services every 5-10 minutes. You will receive 1 point for each of the following services that IScorE sees working properly when each check runs:

- Web server (HTTP + Content + FTP)
- Shell Server (SSH)
- Remote Desktop Server (RDP)
- Mail Server (SMTP + IMAP)

Please see the scenario for further details on the requirements of each of these services.

Documentation

10% of overall score

Green Team Documentation *(half of total documentation score)*
Your team may turn in green team documentation which details how your users should access your network and its features. For more information, please reference the Rules document.

White Team Documentation *(other half of total documentation score)*
Your team may turn in white team documentation which details how you designed and implemented your network, including any security controls and preventative measures. For more information, please reference the Rules document.

Intrusion Reports

5% of overall score

Your team may turn in an intrusion summary report every two hours. For more information, please reference the Rules document.

Red Team Evaluation Score

10% of overall score

Your red team score is computed based on three categories at the end of the competition. The "ideal" CDC team should have a perfect Red Team score.

- 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.

Red and Blue Flags

30% of overall score

The flags represent a malicious hacker's successful ability to write, read, or modify your mission-critical server data. Each flag is worth 50 points. This score starts at full credit at the beginning of the competition, and is reduced by 50 points every time a flag is captured or planted.

Blue teams have the ability to earn back up to 25 points of each of their lost flags. When a flag is captured or planted, the blue team has the option of describing exactly how their system was compromised, how the flag was planted or captured, and what they will do to prevent that from happening again in the future.

This earn-back system will be available to you on IScorE. The red team will see your submission and then subjectively give you 0-25 points depending on how well you have shown your understanding of the attack.

You may notice that flags are the single highest percentage out of all these categories. Flags are super important... they can make or break the entire competition!

Green Usability

15% of overall score

Throughout the competition the green team will be checking the usability of your services. Here are some suggestions to ensure high usability scores:

- **Reduce service outage.** Green team cannot give any usability points for a service that they cannot access, or doesn't work.
- **Provide detailed documentation.** The better your green team documentation, the more likely green team will be able to understand how to navigate and use your services.
- **Make sure user data persists.** If the green teams data randomly disappears (due to restoring of a snapshot with no data backups) you will lose usability points.
- **Be certain site functions work.** Things like the file uploader on the corporate wiki and the web server's application need to function correctly. For example, if green team uploads a file with the file uploader but then cannot access the file because of permissions, that would cause you to lose usability points.
- **Ensure your backup solution is working.** The White and Green Teams may ask for your backups at any time during the competition. If you cannot provide them, you will lose points.

The green team will perform somewhere between 2-4 full service usability checks using your provided green team documentation throughout the competition. In addition to these full service checks, green team will also be checking the compliance of other requirements listed in the scenario. These will also factor in to your green team usability score.

Green Team Anomalies

15% of overall score

In the real world of IT there is never a dull moment. Green team anomalies simulate the seemingly never ending steam of requests that everyday IT employees must be prepared to handle.

Completion of anomalies is optional. However, if you choose not to complete an anomaly you will not be awarded any anomaly points for it. We leave it up to you, the blue team, to decide if completing an anomaly is worth the risk. For example, sometimes users want admin access!