

**COMMUNITY COLLEGE CYBER DEFENSE COMPETITION**

**Competition Scoring Guide**



**IOWA STATE UNIVERSITY INFORMATION ASSURANCE CENTER  
FALL 2011**

## 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

*200 points (11.43% of overall score)*

An automated service scanner, Nagios, will attempt to access your services every 15 minutes. You will receive 1 point for each of the following services that Nagios sees working properly when each check runs:

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

### Green Team Documentation

*100 points (5.71% of overall 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

*100 points (5.71% of overall 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**

*100 points (5.71% of overall score)*

Your team may turn in an intrusion summary report every two hours. Each report is worth up to 25 points. For more information, please reference the Rules document.

## **Red Team Score**

*250 points (14.29% 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 Flags (flags planted by red team on your server)**

*400 points (22.86% of overall score)*

The red flags represent a malicious hacker's successful ability to write or modify your mission-critical server data. This score is computed at the end of the competition and is added to your overall score. It is calculated by:

1. Summing the availability and usability of your services as rated by green team over the past hour and dividing it by the maximum available points for that hour to find a percentage of your green team score for that hour.
2. This subtotal is then multiplied by 1/8 (1 hour of 8 total hours of competition).
3. At the end of the competition, your subtotals will be added up to find the total percentage of your uptime.
4. This value is then multiplied by your subtotal flag score to find your final flag score.

*For example:*

Your team has 80% of your services working for green team the entire competition, and you have lost half of your 400 possible red team flag points. This means you have:

- 200 unweighted red flag points
- 0.8 service availability subtotal
- Total Red Flag Points:  $200 * 0.8 = 160$  points (of 400 possible)

The “too long; didn't read” (TL;DR) version:

Flags and usability are super important... they can make or break the entire competition!

### **Blue Flags (flags planted by you that red team wants to get)**

*400 points (22.86% of overall score)*

This score is calculated in a similar manner to the Red Flags score; please refer to the description above for details.

### **Green Team Anomalies**

*200 points (11.43% of overall score)*

In the real world of IT there is never a dull moment. Green team anomalies simulate the seemingly never ending stream 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!