ISU 2 2026

Scenario

IOWA STATE UNIVERSITY,
Spring 2026

Table of Contents

- Revision History
- ISU 2
- Servers
  - Active Directory (ad.team{num}.isucdc.com)
    - Notes
    - Required Access
    - Flags
  - Website (www.team{num}.isucdc.com)
    - Notes
    - Required Access
    - Flags
  - Label Printer (lp.team{num}.isucdc.com)
    - Notes
    - Required Access
    - Flags
  - Warehouse Management (wms.team{num}.isucdc.com)
    - Notes
    - Required Access
    - Flags
  - Database (db.team{num}.isucdc.com)
    - Notes
    - Required Access
    - Flags
- Notes
  - Flags
  - Migrating Systems
  - User Roles
  - Administrator Accounts
  - Documentation
  - Optional Systems
  - DNS
  - ISEPhone
  - Competition Rules
  - Additional Documents
    - Getting Started
    - Competition Scoring Guide
    - Competition Rules
    - Setting Up a Server
    - Remote Setup Guide

Page Intentionally Left Blank

Revision History

Revision 1.0.0:

- Initial Release

Revision 1.1.0:

- Clarified AD LDAP and RDP access

ISU 2

Fahrenheit Launch Challenge

Welcome, new team!

We here at **Combustion Dynamics Corporation (CDC)™** are thrilled to have you on board. As you may know, we recently acquired the once-struggling energy drink company Rankine and are gearing up to launch our bold new energy drink line, Fahrenheit: *"Feel the burn."*

These are exciting times!

As part of the merge, we made some…tough decisions. The old IT and security teams, along with many other departments, are no longer with us. While it was a difficult process, we are confident that outsourcing IT and security to a top-notch team like yours will set us up for success. That said, some former employees aren't exactly thrilled about their sudden departure, a mere two weeks before our launch, and they still know a lot about the old systems. Which is where you come in!

With only two weeks to the launch, your mission is critical: secure our network, protect sensitive launch plans, safeguard proprietary formulas, and make sure nothing, and we mean nothing, goes wrong in the lead-up to the Fahrenheit launch, March 28th, 8:00 am. Cyber threats and disgruntled insiders alike could cause serious disruptions if vulnerabilities go unchecked.

We're counting on you to patch, defend, and strengthen the infrastructure so the Fahrenheit launch goes off without a hitch. Let's show the world that CDC knows how to feel the burn…and handle the heat.

Welcome to the team!
Michael J. Scott

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Note

This scenario document is subject to change leading up to the release of the scenario VMs for you to secure. Changes will be noted in the Revision History section.

Servers

The servers listed below have been provided (unless specified otherwise) and have various access requirements that must be met by your team. While you may make major configuration changes for the sake of security or usability, your servers must provide all required and original functionality.

Active Directory (ad.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

The Active Directory (AD) machine manages scenario users across all machines. Be sure to properly configure permissions on your AD users!

ALL scenario machines should be joined to the Active Directory machine.

Required Access

- LDAP on port 389
  - This machine MUST be contacted by all other machines on port 389 for the purpose of LDAP user authentication.
  - This MUST be available from the competition network.
- RDP on port 3389
  - IT Administrators MUST be able to RDP into this machine and have Administrator-level account privileges.
  - This MUST be available from the competition network.

Flags

- Red
  - C:\Users\Administrator
- Blue
  - C:\Windows\System32

Website (www.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Alma Linux 8

This machine hosts the company's public website. Customers can sign up, view loyalty points, manage their account information, place store orders, and view current orders.

This server must be domain joined to the Active Directory server.

Notes

- The application is run and controlled with the "frontend" system service
- The code for the website, along with a README with further details, is located in /home/cdc/www

Required Access

- HTTP access on port 80
    - Customers and any public user MUST be able to login, register, and access features of the site.
    - Website Admins MUST be able to perform admin features on the Website.
    - MUST be accessible from the Competition Network.
- Administrative SSH access on port 22
    - IT Administrators MUST have Administrative Access.
    - MUST be accessible from the Competition Network.

Flags

- Red
    - /root/
    - Deface public website
- Blue
    - /etc/

Label Printer (lp.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2019

This machine hosts, stores, and creates the labels for outgoing orders. The labels are also viewable or printable from this machine.

This server must be domain joined to the Active Directory server.

Notes

- This server shares files over SMB with other services, such as WMS and WWW, via the C:\Labels folder.
- Labels and barcodes are printed and generated using ZPL.
- The LabelWatcher Service uses the zplService.ps1 script to check if a new .json file has been add to the WMS Data folder and then creates a barcode using the data with the template.
    - Barcodes can be found in the Barcodes folder.
    - ZPL code and template can be found in the ZPL folder.
    - Once processed, the .json file moves to the Processed folder.

Required Access

- RDP on port 3389
    - IT Administrators MUST be able to RDP into this machine and have Administrator-level account privileges.
    - MUST be accessible from the competition network.
- SMB on port 445
    - The warehouse management system MUST be able to access the SMB share.
    - Warehouse workers MUST be able to access the SMB share.
    - MUST be accessible from the competition network.

Flags

- Red
    - C:\Users\Administrator
- Blue
    - C:\Windows\System32

Warehouse Management System (wms.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu 24.04

This is the warehouse backend for the WWW Storefront. It connects to the database and performs CRUD operations for stock and order management. It also generates files for label printing by retrieving and consolidating details from both the WWW frontend and the database.

This server must be domain-joined to the Active Directory server.

Notes

- The application is run and controlled with the “wms” system service
- The code for the application, along with a README with further details, is located in /home/cdc/wms
- Accesses the shared SMB directory for label printing.

Required Access

- Administrative SSH access on port 22
    - MUST be accessible from the Competition Network.
    - IT Administrators MUST have Administrative Access.
- HTTP access on port 8080
    - MUST be accessible from the Competition Network.

Flags

- Red
    - /root/
    - Alter the Order Number
        - Alter the order number to 00000000.
- Blue
    - /etc/

Database (db.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Mysql Username: richard
Mysql Password: cdc

Operating System: Ubuntu 16.04

This server hosts the central MySQL database for the WWW Storefront and Warehouse Management System (WMS). It stores and manages WWW and WMS data including user authentication records, loyalty points, payment information, shipping details, inventory items, and order transactions.

- The WWW connects to the database to authenticate users, manage accounts, process payments, and retrieve product information.
- The WMS connects to the database to create order records and update stock information.

This server must be domain joined to the Active Directory server.

Required Access

- IT Admins SSH Access on port 22
    - Must be accessible from the Competition Network
    - Administrators MUST have access and have root access
- MySQL on port 3306
    - Must be accessible from the Competition Network
    - Warehouse works MUST have access to update the stock of items
    - WWW and WMS MUST be able to access the database

Flags

- Red
    - /root/
    - Create a new table in the database with the flag as a record
- Blue
    - /etc/

Notes

Flags

This scenario includes two types of flags. Blue Flags must be placed by you onto your server prior to the beginning of the attack phase. These Blue Flags can be files, in which case the flag file must be placed in the given directory. These flags can be protected but must have realistic permissions for the directory they are in. They cannot be hidden or otherwise obfuscated from a standard directory listing. Blue Flags are sometimes database entries instead of files, in which case the table, column, and row for the flag will be detailed by the scenario. The table for the flag will be described in terms of the application which uses the table, not the server which hosts the database. Red flags are planted by the Red Team if they are able to gain write access to the appropriate directory (usually requiring superuser access).

In this scenario, Blue Flags placed in the */etc/* directory must have the permissions:

rw-r--r--

(ie. 644).

These act as a “foothold” flag, indicating that Red Team has been able to access your systems. On systems where many users can sign in, we use a flag in */root/* to check if Red Team has gained elevated permissions on your box.

All file flags must have the same name as downloaded from IScorE.

Migrating Systems

You are not allowed to migrate ***any*** of the provided servers in this competition, unless otherwise specified. Migration includes building another virtual machine and transferring the application to that virtual machine, replacing the operating system with another operating system, performing a clean installation of the current operating system, upgrading the operating system to a different major operating system version, and other similar processes that may result in the current installation being significantly changed.

In addition, the provided applications *may not* be completely rewritten or modified to use a different framework or language. However, you are allowed to modify the application code, and it is *highly recommended* that you do so, as the provided applications may be poorly secured.

User Roles

User information can be found in the “Users” document. Team specific passwords are available on your dashboard on IScorE.

List of roles:

- TODO

As always, it is up to you to decide how to implement these requirements, however if the access is determined to be insufficient, a penalty may be assessed.

Administrator Accounts

Administrator accounts are required to have realistic privileges; i.e. an Administrator should be able to use *sudo* (on Linux servers) or run programs as an administrator (on Windows systems), perform common tasks such as adding/removing users, change system files, install programs, and anything else that would be realistically required of an administrator, without restriction.

Documentation

You will need to provide documentation for White and Green Teams. Documentation is due at the beginning of the attack phase. See the “Rules” document for more information on grading, expectations, and penalties.

Optional Systems

You may choose to implement additional servers such as a firewall, but it is not required. You may deploy systems running on open source or proprietary software running on a trial or academic license. Please refer to the “Remote Setup” document when creating new VMs.

DNS

DNS will be provided for you and will be controlled via IScorE (https://iscore.iseage.org).
You must enter the external IP addresses of your servers into IScorE under “DNS Records”.

ISEPhone

ISEPhone will be used in this competition. The director may require that the phone system is the only allowable method of communication with Green Team during the attack phase; this decision need not be announced prior to the attack phase. Please see the ”Rules” document for more information on the ISEPhone system.

Competition Rules

Version 5.0 of the competition rules will be used for this competition.

Additional Documents

In addition to this scenario document, the competition is governed by competition rules, scoring guide, and other documents. Below is an explanation of each document. **Please remember: in case of a conflict between the additional documents and scenario document, the scenario document takes precedence.** Please review the Competition Rules, and specifically the "Requirements for Services" section for additional details on what is expected from your services.

As always, contact White Team if you have any questions or concerns about rules, scoring, or the competition. You may reach us via email at cdc_support@iastate.edu or via chat at https://support.iseage.org.

Getting Started

If this is your first CDC, please read this document. This document defines terms and explains how the competition will work. This document is designed to be the starting point of reading if you are a "first timer." Also, if this is not your first time, you may find some interesting points in the Getting Started guide.

Competition Scoring Guide

The purpose of this document is to describe how this competition will be scored. The weights and categories are defined here. This document gives a general idea on how you will be scored.

Competition Rules

These are overall rules for the competition. Blue, Red, Green, and White teams are expected to follow these rules. The Competition Rules define the rules of engagement for the CDC. The Competition Rules also define the baseline requirements for services. Your services must follow the expectations for services and all rules. These are subject to change at any point up to the start of competition, and will likely change in between each competition, so please review them each time you compete.

Setting Up a Server

This guide will help you set up the networking and proxy. This document also provides details on how networking works inside of the ISEAGE environment. This document provides links on how to set up static IP addresses in various operating systems.

Remote Setup Guide

This guide will help you gain access to our systems and assist you in setting up remotely. It provides help on how to use vCenter to create VMs, how to connect to your services via RDP and VPN, and how to create a VM.