

ISU 1 2026

Scenario



**IOWA STATE UNIVERSITY,
Fall 2026**

Table of Contents

[Revision History](#)

[ISU 1](#)

[Note](#)

[Servers](#)

[Active Directory \(ad.team{num}.isucdc.com\)](#)

[Required Access](#)

[Flags](#)

[Website \(www.team{num}.isucdc.com\)](#)

[Notes](#)

[Required Access](#)

[Flags](#)

[Canvas \(can.team{num}.isucdc.com\)](#)

[Notes](#)

[Required Access](#)

[Flags](#)

[Library \(library.team{num}.isucdc.com\)](#)

[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:

- Clarify what is 'public' access for the library computer
- Fix AD's OS

ISU 1

K12 District Challenge

Welcome to the Central Dobson County School District, a mid-sized K12 district serving thousands of students across elementary, middle, and high schools. The district relies heavily on digital infrastructure to manage daily operations, academic services, and communication with families.

Over the past decade, Central Dobson County School District has expanded its technology footprint rapidly. What began as a simple SIS (Student Information System) has grown into a complex network of interconnected services, including:

- A public district website hosting announcements and school resources
- A Canvas LMS used by teachers for assignments, grading, and communication
- A parent/student lunch account portal for payments and balance tracking
- A course registration system for middle and high school scheduling
- A district-wide Active Directory domain managing staff, teachers, and administrative personnel

However, the district's IT department has been stretched thin. Legacy systems remain in production due to budget constraints, and several third-party contractors have rotated through during recent modernization efforts. Some integrations were rushed, documentation is inconsistent, and several systems still rely on outdated or insecure configurations.

Recently, unusual authentication attempts, unexplained service restarts, and suspicious scheduled tasks have raised concerns. With the school year underway, leadership fears that misconfigurations, malware, or disgruntled former employees may have introduced backdoors into critical systems.

Your task is to audit the district's environment, secure vulnerable systems, remove unauthorized access, and stabilize essential services relied upon by students, parents, and staff. The continuity of the district's academic operations depends on your ability to secure the network under pressure.

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 2019

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: Ubuntu Server 24.04 LTS

The WWW is a Next.js application that acts as the public district page. Students and parents can log in to manage course registration and view/edit their lunch balances.

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

Notes

- The application is run and controlled with the “www” system service
- The code for the website is located in /var/www. There is a README with instructions for completing the website’s set up.

Required Access

- HTTP access on port 80
 - Students and parent users **MUST** be able to log in, register, and access features of the site.
 - Middle and High school students **MUST** be able to register and drop classes & top up their lunch balance.
 - Parents **MUST** be able to link students to their account using username and password, and **MUST** be able to top up their student’s lunch account balance.
 - IT 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/

Canvas (can.team{num}.isucdc.com)

Default Username: cdc

Default Password: cdc

Default Canvas Username: root@cdc

Default Canvas Password: cdcistheplaceforyouandm3

Operating System: Ubuntu 22.04.5

This machine shall host the front-facing Canvas LMS system with the exception of its database server.

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

Notes

- Users should be able to complete functionality such as
 - Teachers - Manage course invites, edit Canvas assignments, add new Canvas assignments, and set due dates
 - Students - join courses, submit assignments, view grades
 - IT administrators - manage privileges of 'Accounts' and 'Sub accounts'
- Registration of new users MAY be done through the Website machine
 - Login info MUST be an email address (userName@cdc)
- Server config located at /etc/apache2/sites-available/canvas.conf
 - More canvas config located at /var/canvas/config/*
- If you have issues with the site not working, try checking passenger-status
- The API access token is hardcoded to expire after a week, please remember to regenerate new API tokens as needed
- All courses MUST be published. To do so, sign in to the root account, go to Admin -> Central Dobson County -> Courses. For each course, click on it and then change the Course Status to Published

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 80
 - MUST be accessible from the competition network
- HTTPS access on port 443
 - MUST be accessible from the competition network

Flags

- Red

- Deface Canvas
 - /var/canvas/flag/
- Blue
 - /etc/

Library (library.team{num}.isucdc.com)

Default Username: cdc

Default Password: cdc

Operating System: Hannah Montana Linux 26

This is a public library computer at Dobson Middle School. The Guest account MUST be available for non-AD users of the library.

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

Notes

- This device shares files over SMB with other services, such as DB, via the /srv/CDC folder.
- LibreOffice MUST be installed for users of the library to complete their work and assignments.

Required Access

- SSH access on port 22
 - MUST be accessible from the Competition Network.
 - IT Administrators MUST have Administrative Access.
 - Passwordless access for the 'Guest' user MUST be allowed
- RDP access on port 3389
 - MUST be accessible from the Competition Network by any user except parents.
 - IT Administrators MUST have Administrative Access.
 - Passwordless access for the 'Guest' user MUST be allowed
- SMB access on port 445
 - MUST be accessible from the Competition Network.

Flags

There are no flags for this machine.

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

Default Username: cdc

Default Password: cdc

Postgres Username: postgres

Postgres Password: cdc

Operating System: Debian 11

This box hosts a PostgreSQL server which is connected to both WWW and Canvas for database functionality.

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

Notes

- This device **MUST** access the SMB share from the Library computer to provide Lunch Staff with data at /mnt/CDC.
 - An additional script in /mnt/CDC/IT runs periodically via a cron job to simulate students using their lunch accounts and drain their balance.

Required Access

- IT Admins SSH Access on port 22
 - **MUST** be accessible from the Competition Network
 - Administrators **MUST** have Administrative access
- PostgreSQL access on port 5432
 - **MUST** be accessible from Canvas box
 - **MUST** be accessible from WWW box

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](#).

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.