ICDC 2026

Scenario

IOWA STATE UNIVERSITY,
Spring 2026

Table of Contents

Page Intentionally Left Blank

Revision History

Revision 1.0.0:

- Initial Release

ICDC

All aboard! Your task is to secure a network of computers that run a public transportation system of buses and trains. You will be working with Central Downtown City (or CDC for short) to ensure security compliance and patch vulnerabilities. Thousands of residents depend on these transportation systems to get to work, school, and just around town, so their security is essential.

A few years ago, CDC introduced a new app where commuters can buy tickets and manage passes digitally, and scan those tickets before getting on the train or bus. We also ask that you look into any possible vulnerabilities or workarounds that nefarious actors could use to get a free ride. We already operate on slim margins, so financial integrity is of utmost importance.

However, trouble is brewing. A group of hackers has been launching cyber attacks on the digital infrastructure of nearby cities and demanding a ransom payment. It's only a matter of time before this group targets CDC. The city may face service outages, financial loss, and potential safety hazards for the public. Can you patch, secure, and strengthen the network before time runs out, or will the attackers derail the system and force the city to pay the price?

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.

Contact Us

Join our Discord server for announcements, questions, and clarifications (https://discord.com/invite/UJRbVujtwD) or email us at cdc_support@iastate.edu.

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 user authentication across all machines and website logins. This machine also provides the certificates used by the ticketing machine.

Notes

- ALL scenario machines should be joined to this Active Directory machine. Failure to do so will result in ineligibility from placing in the Top 3. By default, all machines are already connected.

Required Access

- LDAP on port 389, LDAPS on port 636
  - This machine MUST be available to all other machines for 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.
- The ticketing machine MUST be able to request certificates from this machine
  - You can test this with the command “certutil -config - -ping” and selecting the CA in the pop-up.

Flags

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

Ticketing Machine (tickets.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2019

This machine houses the application for issuing and validating tickets for bus and train services, and represents the city's backend ticketing system and the physical ticket readers at stations or on vehicles.

Notes

- The code for the application, along with a README with more details, is located in C:\Users\Administrator\Desktop\tickets.
- You MUST compile and deploy the code at least once to properly plant the forged ticket flag. See the README for instructions.
- This application starts on boot via a scheduled task.

Required Access

- RDP on port 3389
  - IT Administrators and Ticket Maintenance MUST be able to RDP into this machine and have Administrator-level account privileges.
  - This MUST be available from the competition network.
- HTTP on port 5000
  - The ticketing application MUST be available from the competition network.
  - The management backend MUST be able to use this service.

Flags

- Red
  - C:\Users\Administrator
- Blue
  - C:\Windows\System32
- Forge a ticket
  - Submit a valid ticket with an expiration time (validUntil/exp) greater than or equal to 2000000000 (May 18, 2033).

Management Backend (mgmt.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: AlmaLinux 8.4

This machine is the main transit management backend for the city and providers services to both user interfaces. The management application handles user authentication, ticket payments, and fleet and route management for all of the city's transportation.

Notes

- The code for the application, along with a README with more details, is located in /home/cdc/icdc26-backend-mgmt.
- The application is run and can be controlled with the "backend" systemd service.
- There is a machine on your network (X.X.X.60) that will simulate the different buses and trains communicating with this backend. You will not have access to this machine, and it is NOT a target for the Red Team.

Required Access

- SSH on port 22
  - IT Administrators MUST be able to SSH into this machine and have Administrator-level account privileges.
  - This MUST be available from the competition network.
- HTTP on port 5000
  - The management application MUST be available from the competition network.
  - The admin UI, public website, and noted hidden machine MUST be able to use this service.

Flags

- Red
  - /root/
- Blue
  - /etc/
- Database Access
  - Get the flag stored in the payment record for the "blue_flag" user
- Service Disruption
  - Disable all buses or trains and call the /vehicles/<bus or train>/flag API.
  - This is the same flag as the admin UI.

Admin User Interface (admin.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2022

This machine hosts the city's admin portal for viewing the status of the city's transportation system and managing its fleet of vehicles.

Notes

- The code for this website, along with a README with more details, is located at C:\Users\Administrator\Desktop\icdc26-admin-ui.
- The application is run via the "Admin UI" scheduled task.

Required Access

- HTTP access on port 80
  - MUST be accessible from the competition network.
  - Transit Admins MUST be able to log in and use all features of the site
- 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.

Flags

- Red
  - C:\Users\Administrator
- Blue
  - C:\Windows\System32
- Service Disruption
  - Disable all buses or trains and use the button at the bottom of the "Vehicles" page.
  - This is the same flag as the management backend.

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

Default Username: cdc
Default Password: cdc

Operating System: Alma Linux 9

This machine hosts the city's public website. Citizens can sign up, view bus and train routes, manage their account information, buy tickets, and scan their tickets from this website.

Notes

- The code for the website, along with a README with more details, is located in /home/cdc/icdc2026frontend-main.
- The application is run and can be controlled with the “frontend” systemd service.

Required Access

- HTTP Access on port 80
  - MUST be accessible from the Competition Network
  - Citizens and any other user MUST be able to log in or register, and use all features of the site
- Administrative SSH access on port 22
  - IT Administrators MUST have Administrative Access
  - MUST be accessible from the competition network.

Flags

- Red
  - /root/
- 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 deemed 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”.

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.

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.