ISU2 2025

Scenario

IOWA STATE UNIVERSITY,
ISU2 2025

necessary

Table of Contents

Competition Scoring Guide
Competition Rules
Setting Up a Server
Remote Setup Guide

Page Intentionally Left Blank

ISU2 2025

Welcome to the Core Development Collective, an open source software development company. They're launching version 1.0 of their software, Cognitive Data Converter, which uses all of the most cutting-edge technologies to transform image formats.

The team is fairly small, with a few network admins, a project manager, and a handful of volunteer contributors. They recently created an IRC server to communicate with new users who were interested in the big release.

You have been asked to audit their internal network for security flaws and ensure the website is in tip-top shape before their first major release. This is especially important, because of the distributed nature of the development. With dozens of former contributors, it's easy for malicious or backdoored code to slip through the cracks. Can you fortify the network ahead of the increased attention that comes with a big release?

The keywords "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.

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.

Hostname	**Last Octet**
ad	10
git	20
env	30
code	40
irc	50
www	60

AD (ad.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

The domain controller for your network. Domain computers use this server to authenticate users and allow access to various resources in the network.

Notes

The deployed AD does not have any of the users added or groups created for the respective scenario. **YOU MUST ADD** users and groups to ensure usability. As always, it is RECOMMENDED that your team audits this server.

Required Access

- Administrative RDP access on port 3389
  - IT Administrators MUST be able to access RDP
  - IT Administrators MUST have Administrative Access
  - MUST be accessible from the Competition Network
- LDAP access on port 389
  - All scenario users and other Contributors MUST be able to authenticate with the AD server
  - MUST be accessible from the Competition Network

Flags

- Red
  - Add user to domain
  - C:\Users\Administrator\
- Blue
  - C:\Windows\System32\

IRC Server (irc.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Desktop 22.04

The IRC server is used for communication with users in the #support chat for talking with users and the #dev chat for talking with other developers.

Notes

How to use IRC:
ngircd is installed on the IRC machine.

1. Enter HexChat on Windows
2. Edit the settings of CDC server to the IP Address of the IRC server
3. Press the enter key after typing it, exit the config menu, then press connect.
4. Connect to the #support channel (for users) or the #dev (for developers).

You may NOT set a password for either channel. You may NOT change to encrypted IRC.

Required Access

- IRC Access on port 6667 for all users
    - MUST be accessible from the Competition Network
    - Any IRC client should be able to connect to it
    - Customer Support personnel MUST be able to send and receive messages on the #support channel. Access for the #support channel MUST be passwordless.
    - Contributors and Project Maintainers MUST be able to send and receive messages on the #dev channel. Access for the #dev channel MUST be passwordless.
- Administrator SSH access on port 22
    - IT Administrators MUST have Administrative Access
    - MUST be accessible from the Competition Network

Flags

- Red
    - /root/
- Blue
    - /etc/

CODE Server (code.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 20.04

The CODE server is used for development of the application. You can access the CODE server via the FireFox web browser.

Notes

Please use the webIDE only. You MAY NOT link code-server to the desktop VS-Code application. You MAY upgrade the security to HTTPS, but if you choose to do this, you MUST let white team know through email or discord for the service scanner to function correctly. You MAY set a password for entry, but if you choose to do so, you MUST include it in your Green Team Documentation.

You can access code-server by going to http://code.team{num}.isucdc.com:8080

Required Access

- HTTP Access on port 8080
  - Contributors and Project Maintainers MUST be able to access the web IDE MUST be accessible from the Competition Network
- Administrator SSH access on port 22
  - IT Administrators MUST have Administrative Access
  - Project Maintainers MUST have Administrative Access
  - MUST be accessible from the Competition Network

Flags

- Red
  - /root/
- Blue
  - /etc/

GIT Server (git.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc
GitLab Username: cdc
GitLab Password: password

Operating System: Ubuntu Server 22.04

This server hosts the GitLab instance used for storing the Collective's software repositories.

This server must be domain joined to the Active Directory server. Failure to do so can result in point penalty or disqualification from placement.

Notes

- The application is in the Cognitive Data Converter project and available at http://git.team{num}.isucdc.com/cdc_group/cognitive_data_converter
- There is a CI/CD pipeline that tests, packages, and deploys the application to WWW. To view or run the pipeline, go to the project and click CI/CD > Pipelines in the left-hand menu.
- The project's README contains information about building and running the application.
- There is a Python script in /root that runs every minute and adds new GitLab users to the CDC_Group. This is needed to give AD users access to the Cognitive Data Converter project.

Required Access

- Administrative SSH access on port 22
    - MUST be accessible from the Competition Network
    - IT Administrators MUST have Administrative Access
    - Project Maintainers MUST have Administrative Access
- HTTP access to GitLab on port 80
    - MUST be accessible from the Competition Network
    - The project visibility MUST be Public
- GitLab
    - Project Maintainers MUST be Admin users in GitLab
    - Active Directory users MUST be automatically added to the CDC_Group every minute. Project Maintainers MUST have at least Maintainer access. Contributors MUST have at least Developer access. Both MUST be able to push code to the project and run CI/CD pipelines
    - There MUST be a CI/CD pipeline to test, package, and deploy the application
    - GitLab MUST be able to authenticate users with AD using LDAP

    - You MAY enable branch protection, but this MUST be documented in your green team docs, merge requests MUST be reviewed in a timely manner, and any rejected merge request MUST have a valid explanation

Flags

- Red
    - /root/
    - Create a project access token for the Cognitive Data Converter project with the flag as the name
- Blue
    - /etc/

ENV Server (env.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Windows 10

This server hosts the GitLab Runner used for executing CI/CD pipelines.

This server must be domain joined to the Active Directory server. Failure to do so can result in point penalty or disqualification from placement.

Notes

-

Required Access

- Administrative RDP access on port 3389
  - MUST be accessible from the Competition Network
  - IT Administrators MUST have Administrative Access
  - Project Maintainers MUST have Administrative Access
- The GitLab Runner MUST be able to run CI/CD jobs submitted by the main GitLab instance
- MUST be able to transfer the packaged software to WWW

Flags

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

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

Default Username: cdc
Default Password: cdc
Admin Dashboard Username: admin
Admin Dashboard Password: admin

Operating System:

This is the main website for the Core Development Collective. Users can download the latest software releases or sign up to be developers.

This server must be domain joined to the Active Directory server. Failure to do so can result in point penalty or disqualification from placement.

Notes

- The web application can be found in /opt
- You will need to configure the app to work with AD. Configure settings.py to get sign in working, configure the register section in views.py to get registration working. It has some boilerplate code, here's a reference to some rust code that was used in ISU1 for AD auth https://github.com/Januszski/ISU1_Guard_App/blob/main/src-tauri/src/main.rs
- There is an admin dashboard found at /admin
- After making changes you will need to restart gunicorn.service
- The web application is behind an NGINX reverse proxy
- The username field in the deploy/deploy.ps1 script in the Cognitive Data Converter repository should be changed to "cdc"

Required Access

- Administrator SSH access on port 22
    - IT Administrators MUST have Administrative Access
- HTTP access on port 80
    - MUST be accessible from the Competition Network
- MUST be able to receive the packaged software from ENV
- MUST be able to create Contributors in AD with LDAP

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.

List of roles:

- IT Administrators
- Project Maintainers
- User Support
- Contributors

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

The latest version 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.