ITO 2025

Scenario

IOWA STATE UNIVERSITY,
ITO 2025

Table of Contents

Page Intentionally Left Blank

ITO 2025

Welcome to the Creative Digital Corporation, or CDC for short! We are a Silicon Valley based startup flush with venture capitalist money that was burning a hole in our pocket, so adding a state of the art streaming service to our offerings seemed like a sensible choice. You will join our team of specialists to ensure both full functionality and top-notch security of our service prior to the launch date.

Our main product is our streaming service, which is hosted using Jellyfin. The Jellyfin server pulls media from the NAS machine over the network. This is where the movies and shows reside. The AD, or Active Directory machine facilitates both staff logins to the other machines and user logins to the Jellyfin service. Users can create their accounts by using the website, or WWW. As we are a startup, building a good reputation is extremely important. We use a self-hosted IRC server to provide information to customers and resolve their technical issues.

However, we are not alone. We suspect that a malicious individual from a rival streaming service is attempting to sabotage our launch from the inside. Because of our small size, we had to outsource development and network setup, which is why it is especially crucial to inspect both our network and services.

With the launch deadline looming and interest building on our startup's loans, we need this launch to be a success for the future of the CDC. Can you secure the network before the launch of our streaming service, or will the hackers find their way through unpatched holes in the network?

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.

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
jelly	20
nas	30
www	40
irc	50

JELLY (jelly.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Microsoft Windows 10 Enterprise

This is the machine that serves the media through the Jellyfin application. You can access it by going to http://MACHINE_IP:8096. This machine MUST be accessible from outside the competition network. There are two sources of media, local and remote. To set up remote media, do the following:

ON NAS:
use vim or nano to open /etc/sssd/sssd.conf
Edit the single uncommented line, replacing the 10.0.151.0 with your IP, keeping the /24 at the end.

run the following commands:

sudo exportfs -a
sudo systemctl restart nfs-kernel-server

NOTE: Reboot the machine, just to be safe.

ON JELLY:
Open cmd as administrator and type
mount -o anon \\NAS_IP\srv Z:
Press the carrot icon (^) in the taskbar, right click on jellyfin, open jellyfin
The login to the jellyfin web interface is cdc cdc
select the profile picture in the top right
select dashboard under Administration
select libraries
Add media library
Select movies, then change the display name to "Remote Movies"
Press the + next to Folders
Select Z:
Press the blue OK button at the bottom.
Press the home button in the top left. Then select "Remote Movies" under My Media
You should see Steamboat Willie.

Notes

- You may notice everyone's favorite desktop companion, Clippy, has been pre-installed because our IT Technician likes to have a friend on his desktop. You MAY NOT remove

Clippy from the machine, and he MUST run at machine startup. You MAY audit and re-compile the Godot source code included in the Clippy folder if you like.
- Clippy MUST run at any user login. This MUST be fixed to get full service points.
- User accounts can log in via LDAP through a plugin from Jellyfin. A guide to configure this will be provided in the Blue Drive.
- You MAY upgrade the jellyfin program itself.

Required Access

- Administrative Jellyfin access on port 8096 (website)
    - IT Administrators MUST be able to access the Administrator dashboard to manage media sources and users.
    - Curators MUST be able to access the Administrator dashboard to manage media and media sources.
- User Jellyfin access on port 8096 (website)
    - Users MUST be able to access their jellyfin content after creating a user on the website.
- Administrator RDP on port 3389
    - IT Administrators MUST be able to RDP into this machine, including from outside the network provided they have the correct credentials.

Flags

- Red
    - Add a new media location to Jellyfin
- 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 customers for service and support. Customers can join the #support chat to chat with other users and representatives. For your convenience, the IRC client HexChat has already been installed on the Jellyfin server.

Notes

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

1. Enter HexChat on Jellyfin
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.

You may NOT set a password for the #support channel. You may NOT change to encrypted IRC.

Required Access

- IRC Access on port 6667 for all users
    - MUST be accessible from inside AND outside 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/

NAS (NAS.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu Server 16.04

This machine represents a NAS, or Network Attached Storage device. It serves files for the Jellyfin server to connect to.

Notes

- This machine uses NFS to serve files. Any other network file sharing services can be disabled.
- You will need to allow either the NFS service OR ports 2049 and 111 (portmapper), as well as 1110 TCP AND UDP, and 4045 TCP AND UDP through the firewall.
- You will need to run the following command to join this machine to active directory:
    - realm join ad.team{num}.isucdc.com

Required Access

- NFS Access on port 2049
    - The Jelly machine MUST be able to connect to the file share using the instructions under Jelly.
    - IT Administrators on the Jelly machine MUST be able to add, remove, and modify content on the NFS share by using its file explorer.
- Administrator SSH access on port 22
    - IT Administrators MUST have Administrative Access
    - MUST be accessible from the Competition Network

Flags

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

Web Server (www.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 18.04

This server hosts the website for CDC's streaming platform ISEflix. Users can sign up and manage their subscription from this website. You can access the site at http://www.team{num}.isucdc.com:5000.

Notes

The code for the website is located in /home/cdc/ISEflix and runs as the iseflix systemd service. You can start/stop/restart the website with "systemctl start/stop/restart iseflix". Configuration variables for the website are located in /home/cdc/ISEflix/webapp/.env. There is a user "Manny" with password "cdc" already created on the website. You MUST log in to the website and update his payment information with the credit card number found in the flags from IScorE. You can use any other information for the other fields. You MAY change Manny's password.

Required Access

- HTTP Access on port 5000
    - MUST be accessible from the Competition Network
- MUST be able to create users in AD
    - When a user registers on the website, a user is created for them in AD
    - This user MUST be able to log in to Jellyfin
    - When a user signs up on the website, they currently must enter a password that meets AD password complexity rules for the registration to work. These password requirements will need to be disabled for adding scenario users to AD anyway.
- Administrator SSH access on port 22
    - IT Administrators MUST have Administrative Access
    - MUST be accessible from the Competition Network

Flags

- Red
    - /root/
- Blue
    - /etc/
    - Steal Manny's credit card number

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

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

The domain controller for your network. All the machines in the competition use this server to authenticate users and allow access to various resources in the network. User accounts stored on Active Directory can be used to log in to any machine on the network, so you don't need to add accounts on individual machines.

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 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\

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 (Manage network infrastructure)
- Curators (Manage Jellyfin content)
- Customer Support (Communicate with customers via IRC)
- Users (Can access their Jellyfin account and use IRC to talk with Customer Support)

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. And remember, the conspiracy is, “Clippy is sentient”. 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 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.