Table of Contents

[Cornucopia Dive Coasters]

Servers
  Management Console (mgmt.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
Ladies and Gentlemen, Boys and Girls!

Step right up to witness the unveiling of a spectacle that will defy the ordinary and redefine the meaning of thrills! It is with great excitement that we introduce the grand opening of Cornucopia Dive Coasters Amusement Park! (Drum roll, please!). From the pulse-pounding "Git and Split" rollercoaster to the gravity-defying BitTwist Tower, the adrenaline-fueled Recursive Rapids River Ride, and much more, TK promises an unparalleled experience in the world of amusement.

Over the past three years, with the unwavering support of our investors, TK has transformed dreams into reality. We've meticulously planned this grand opening to captivate thrill-seekers from every corner of the globe.

However, in the face of technical challenges and an unfortunate lawsuit, we find ourselves at a crossroads. The setback led to the departure of our main investors and a restructuring of our tech team, resulting in a delay in our grand opening. But fear not, dear patrons, because this is where you come in!

With your expertise and assistance, we can fast-track our journey to a triumphant opening. Your skills are the missing piece of the puzzle, and together, we can ensure a swift and secure launch. To sweeten the deal, we are offering a marvelous paycheck of $150 per week! (Cough - significantly more economical than our previous tech team - cough).

Your minor assistance in setting up our network and fortifying the security of our customers’ data is invaluable. Join us on this adventure, and your contribution will not only
propel Cornucopia Dive Coasters to new heights but will also be met with immense gratitude from both our dedicated employees and eager customers.

Are you ready to be a hero of the Cornucopia Dive Coasters Amusement Park? Join us, and let's make magic happen!

Sincerely,
The Managerial Team

Cornucopia Dive Coasters Amusement Park Management
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.
AD (ad.team{num}.isucdc.com)
Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016 R2

This is the main management console for credentials of employees. This is also the employee management console, and Security Administrators must be able to hire, fire, and alter employees. DNS has not been implemented by our former tech team (something about “DNS is impossible” blah blah…) so DNS implementation falls upon you!

Required Access
- Administrative RDP Access on port 3389
  - Must be accessible from the Competition Network
  - All employees must be able to run the management application, login to the management application, and interact with the management application.
  - Administrators must be able to perform administrative actions on the virtual machine.

Flags
- Red
  - Add a new employee with the name being the flag
- Blue
  - C:\Users\Administrator
Web Application (app.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Microsoft Windows 10 (64-bit)

This server is responsible for hosting the web application used to control the amusement park’s main attraction - the “Git and Split” rollercoaster. The world’s first safe and legal roller coaster filled with conflicts, issues, and worst practices!

DNS must be completed so the web application will resolve at the app.team{num}.isucdc.com address. Additionally, 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

- Source code for the Next.js web application can be found at C:\tmp-main\   
  - Next.js -> v13.5.6, React -> v18
- The web application is deployed using Node.js each time the server is booted. This is done via Task “Scheduler” and a Batch file. The Batch file can be found at C:\launch.bat, and the task that executes the file is named “Launch Web App”.   
  - Node.js -> v20.9.0, npm -> v10.2.3, npx -> v10.2.3
- The web application is currently hosted on port 80   
  - To change which port the web application is deployed to, edit the “start” script in C:\tmp-main\package.json to “next start -p <desiredPort>”

Required Access

- Administrative RDP Access on port 3389   
  - Must be accessible from the competition network   
  - Administrators must be able to perform administrative actions on the server
- HTTP/S to the web application on port 80 or 443 respectively   
  - Owner(s), admins, and ride operators must be able to access the web application. Tellers should not be able to access the web application   
  - Must be accessible from the competition network

Flags

- Red   
  - Web application defacement
- Blue   
  - C:\Windows\System32
WWW (www.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2022

This website server is the gateway to a memorable experience at our amusement park. This website is designed to give our customers a user-friendly and convenient way to reserve tickets for the park's grand opening!

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
- This box contains both the website and a small api that are both hosted using windows IIS. Before the website will correctly run, configurations must be made.
- To set up the API, the default web files location is found under C:\inetpub\www_api
  - Teams must properly modify the queries.js file (line marked “CHANGE ME”) to contain the IP address of their database box. Failure to do so will result in features missing on the website.
- To set up the WWW, the default web files location is found under C:\inetpub\www_web
  - Teams must properly modify and redeploy the static files by doing the following:
    - Start by modifying the API address in the .env file to reflect your team number.
    - After accomplishing this, open a terminal window in the www_web folder and run the command “npm run-script build”. Then restart the site using the IIS manager.
- For unknown reasons, updating windows may cause npm to suddenly stop working. If this occurs, C:\Documents\NPM Installer contains a nodejs installer to repair the files.

Required Access
- Administrative RDP Access on port 3389
  - Must be accessible from the Competition Network
  - Administrators must be able to perform administrative actions on the virtual machine.

Flags
- Red
  - Website defacement
- Blue
  - C:\Windows\System32
DB (db.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2012 R2

This database is the central hub for the Amusement Park's data and operational needs. It is designed to manage and oversee the park's resources and personnel. The database also holds customer information and the amount of reserved tickets before the amusement park opening.

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
- Default postgres credentials are
  - Username: postgres
  - Password: cdc
- Data stored for the API is located in the postgres database. If these credentials or database names are changed, these changes must be reflected in the API queries file for proper website functionality.

Required Access
- Administrative RDP Access on port 3389
  - Must be accessible from the Competition Network
  - Administrators must have access and have root access
- General access on port 8082
  - Must be available on the Competition Network
  - Any user must be able to access
- WWW API access on port 5432
  - Must be able to access DB on the machine from Competition Network

Flags
- Red
  - Create a new table in the database
- Blue
  - C:\Windows\System32
WC (wc.team{num}.isucdc.com)
Default Username: Administrator
Default Password: cdc

Operating System: Windows 12 R2

This Windows Client is for internal users to access the internet as well as for administrators to confirm user-end functionality as needed.

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
- This will need to be able to contact the WWW and DB server for communication and the Active Directory server for authentication.

Required Access
- Administrative RDP Access on port 3389
  - Must be accessible from the Competition Network
  - Administrators must be able to perform administrative actions on the virtual machine.
- The system must be able to connect to the Both the WWW and DB servers
  - All administrative users must be able to access..

Flags
- Red
  - Create a new user named Flag
- Blue
  - C:\Windows\System32
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:
- Owner
- Head IT Admin
- IT Admin
- Ride Operator
- Teller

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 4.2 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](mailto:cdc_support@iastate.edu) or via chat at [https://support.iseage.org](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.