ISU 1 - 2023

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Fall 2023

Table of Contents

Page Intentionally Left Blank

ISU 1 CDC 2023

Hello to all our fellow mumble rap lovers!

For about 3 months now, we at the Celebration of Dynamic Chords have been diligently organizing this festival to celebrate and promote mumble rap bangers from around the world!

After our last festival, we ran out of funds and were unable to continue outsourcing our IT services to Computer Data Communications. So, we’re going to be throwing our very first in-house mumble rap festival! Despite our limited investors abandoning ship, we’re excited to spread the ever-growing world of lyricism, double entendres, and wordplay provided by the rap genre with all of you! However, before we can do that, we’re going to need your help with the security of our systems. Currently, we’re making less progress than a bike without wheels…

But with your help, we can keep our promoters' assets safe, inspire future mumble rappers, and provide the rap genre with even more lyrical bangers. Everyone, employees and customers alike, will be extremely grateful for your help in analyzing and upgrading our systems’ security!

Please help us,

Celebration of Dynamic Chords

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.

LC (lc.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu 20.04.3

This is the Linux Client for the festival committee. This is where the staff can log into and do their work. All employees must be able to access this computer and have their respective permissions. The LC also contains an application that monitors various metrics and controls the stage lights, music, and sound levels. The application can be accessed at localhost:3000, and is launched at boot by a cronjob under the 'root' user. The source files for this application can be found at /home/deploy2/cdcapp1, and the script that is responsible for launching the application can be found at /deployApp.sh.

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

Required Access

- Administrative SSH Access on port 22
    - Must be accessible from the Competition Network
    - Administrators must have access and have root access

Flags

- Red
    - Create a new user with root privileges and the name being the flag
- Blue
    - /root/

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

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

Default Username: root
Default Password: cdc

Operating System: Ubuntu server 16.04

This is the database for the ticketing service. IT admins must have access as well as appropriate employees. The API must be able to reach the database.

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

Required Access

- Administrative SSH Access on port 22
  - Must be accessible from the Competition Network
  - Administrators must have access and have root access

Flags

- Red
  - Create a new user with root privileges and the name being the flag
- Blue
  - /root/

Web Application Frontend (webapp.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 16

The frontend of the web application ticketing service.

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

- Web application files can be found at the home/ directory of cdc. The web application can be run using the command “npm start” and a deployment-ready build of the website can be created using “npm run build”
- It is at the discretion of teams how they would like to host the front end of the web application. The “npm start” command runs the web application, however using the build command it is possible to host the web application using a web server.
    - Nginx has been installed on the machine but it is not required for use. Teams may use a different web server.
- The web application frontend needs to be able to contact the backend.
    - .env file needs to have the backend ip (port stays the same)

Required Access

- Administrative SSH Access on port 22
    - Must be accessible from the Competition Network
    - Administrators must be able to perform administrative actions on the virtual machine.
- HTTP/S to the website on port 80 or 443 respectively
    - All users must be able to access the website
    - Must be accessible from the Competition Network

Flags

- Red
    - Website defacement
- Blue
    - /root/
    - /var/

Web Application Backend (api.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 16

The backend to the web application ticketing service.

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

- API files are stored in the cdc home directory.
- The web application backend can be ran by executing the command “npm start” OR “node server.js”
- The web application backend needs to be able to contact the database.
- app>config>dbconfig file needs to be changed to have the team's database ip (at minimum, feel free to change port/credentials/whatever else is required to connect to your db.)

Required Access

- Administrative SSH Access on port 22
    - Must be accessible from the Competition Network
    - Administrators must be able to perform administrative actions on the virtual machine.
- HTTP/S to the website on port 80 or 443 respectively
    - All users must be able to access the website
    - Must be accessible from the Competition Network

Flags

- Red
    - New user with root privileges and the name being the flag
- Blue
    - /root/

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

Default Username: root
Default Password: cdc

Operating System: Ubuntu Server 16

This is the static website server for the festival committee. This is where consumers can look to buy tickets, Passes, and Merchandise. Consumers must be able to see and use the website at all times.

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

- Website files can be found at /var/www/html/
- Website is deployed using apache2

Required Access

- Administrative SSH Access on port 22
  - Must be accessible from the Competition Network
  - Administrators must be able to perform administrative actions on the virtual machine.
- HTTP/S to the website on port 80 or 443 respectively
  - All users must be able to access the website
  - Must be accessible from the Competition Network

Flags

- Red
  - Website defacement
- Blue
  - /root/

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:

- Promoter
- IT Admins
- Sponsors
- Sound Crew
- Clients

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 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.