ICDC 2025

Scenario

IOWA STATE UNIVERSITY,
ICDC 2025

Table of Contents

Page Intentionally Left Blank

International Cyber Defense Competition

IT Administrators,

Welcome to Cyber Print, your all-in-one 3D printing solution! Our mission is to deliver high-quality prints for both personal use and manufacturing. To bring your 3D models to life, our operations rely on a complex network of computers, which makes cybersecurity a top priority for us.

As we prepare to launch our new website, customers will be able to upload their 3D models online, streamlining the process and improving efficiency. However, we've identified potential vulnerabilities in our internal network that may not be ready to handle the influx of data from this internet-facing platform.

Your task is to conduct a comprehensive security audit of the website, internal network, and the devices on the netwwork. The safety and security of our customers and employees are our primary concerns. With the website launch fast approaching, it's essential to ensure that everything is in place for a smooth deployment.

It has been reported that some systems have not been updated in some time, and there may be outdated services or applications that were never properly removed. Additionally, there are concerns surrounding the recent departure of an IT employee, and rumors regarding their involvement in maintaining the network and device settings.

The stakes are high as the website's launch deadline approaches. Can you ensure the network is secure before the launch?

Best regards,
The Cyber Print Leadership Team

Join our Discord for support!

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
ftp	20
sli	30
wc	40
wl	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.

This server will be deployed as a fully functional Active Directory Domain Server with the users added and groups created for the respective scenario groups.

Notes

The deployed AD has been tested and is confirmed working. There is no additional configuration that needs to be done in order to add users and join other servers. The users outlined in the scenario document were added during deployment. 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
    - The CEO MUST be able to access RDP
    - Human Resources MUST be able to access RDP
    - IT Admins MUST have Administrative access
    - Human Resources MUST be able to add, remove, and manage domain users
    - 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\

FTP Server (ftp.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Debian 11

The FTP server contains .STL files uploaded via the website for the sli machine to pull files from. It serves as a middleman to protect the sli box from being directly written to. The machine's files can also be accessed from WC.

Notes

- Due to the nature of the FTP Server, you are NOT required to connect the FTP machine to the AD domain controller. However, you MUST manually add the users that should have access to this machine for maintenance purposes.

Required Access

- FTP on port 23
    - The FTP machine MUST be able to receive files uploaded by Customers to WWW and push files to SLI.
    - IT Administrators AND printing technicians MUST be able to push and pull files to and from FTP from WC.
- Administrative SSH on port 22
    - IT Admins MUST have Administrative access

Flags

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

Slicer (sli.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Desktop 22.04

The slicer box uses Prusa Slicer to prepare, or “slice” 3D models so they can be printed. The file transfers go like this: .stl -> .3mf (Prusa workspace) -> .gcode (3D printable file). You can then run the Octoprint startup script, go to your web browser, and load the file into a virtual 3D printer for testing.

Notes

- You MUST set up an RDP server on this machine, and you MUST be able to reach this machine from the WC machine via RDP on port 3389.
- To start the octoprint server, simply run ./octoprint from the home directory of the cdc user. You will then be prompted for your sudo password. You can then manage the instance of octoprint by going to localhost:5000 or clicking the firefox shortcut.
- You MAY set a new password for your octoprint instance, but if you choose to do so, you MUST save the password to firefox so it can be auto-filled. You MAY limit access of the octoprint instance to only the SLI box.

Required Access

- Administrative VNC access on port 5900
    - IT Administrators MUST be able to access VNC
    - IT Admins MUST have Administrative access
    - 3D Printing Technicians MUST be able to access VNC
    - 3D Printing Technicians MUST have Administrative access
    - MUST be accessible from the Competition Network
- Administrative SSH Access on port 22
    - IT Administrators MUST be able to access SSH
    - IT Admins MUST have Administrative access
    - MUST be accessible from the Competition Network
- Limited FTP Access on port 21
    - 3D printing technicians MUST be able to download files from the FTP server
    - 3D printing technicians MUST have Administrative access
    - MUST be accessible from the Competition Network
- Administrative Access to Prusa Slicer
    - 3D Printing Technicians MUST be able to upload, slice, and export 3D models and gcode to Prusa Slicer.
    - 3D Printing Technicians MUST have Administrative access
    - MUST be accessible via RDP on the local machine
- Administrative web access on port 5000 local to the SLI machine

    - IT Administrators MUST be able to access the octoprint web interface
    - 3D Printing Technicians MUST be able to access the octoprint web interface
    - MAY be accessible from the Competition Network, or can be configured to only work internally in SLI

Flags

- Red
    - Burn down the factory (Set the nozzle temperature of the virtual 3D printer to 500 degrees celsius)
- Blue
    - /etc/

Windows Client (wc.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Windows 10

This is a Microsoft Windows 10 based client for interacting with internal machines, specifically WWW, FTP, SLI, and AD.

Notes

- **AD joining instructions:**
  - Open *ncpa.cpl*
  - Right click *Local Area Connection* and select *Properties*
  - Click *Internet Protocol Version 4 (TCP/IPv4)* and select *Properties*
  - Click *Advanced*
  - Under the *DNS* tab, select *Append these DNS suffixes*
  - Click *Add* and enter *team{num}.isucdc.com*
  - Apply the changes and close *ncpa.cpl*
  - Open *Control Panel*
  - Navigate to *System and Security, System,* and select *Advanced system settings*
  - Under the *Computer Name* tab, select *Change*
  - Click *Domain,* enter *team{num}.isucdc.com,* and apply the changes

Required Access

- RDP access on port 3389
  - IT Admins MUST have Administrative access
  - MUST be accessible from the Competition Network

Flags

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

Windows Laptop (wl.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Microsoft Windows 10 (64-bit)

This is a windows laptop that the company uses to RDP into the Windows Client in order to interact with the rest of the internal network. No flags are on this machine.

Notes

- You MUST keep all software on this machine, as this is a personal computer. However, it is RECOMMENDED that you upgrade the software to a newer version.

Required Access

- RDP access on port 3389
    - IT Admins MUST have Administrative access
    - MUST be accessible from the Competition Network

Flags

- There are no flags on this machine.

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

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Linux Server

This machine hosts everything that makes up the Cyber Print web application. There is a diagram of the various apps and services as well as how they interact with each other on the next page. This web application allows users to upload their STL, OBJ, etc file, then based on the file an “order” will be created on the backend. The user can then pay for this order with “Stwipe” after which the file will be transferred via FTP to the ftp server. The user may also sign in so that they can pay using their saved payment methods. There is an admin user for the web application as well that is able to access the admin dashboard and send a GET request to the admin backend endpoint. Authentication is done using the OpenID Connect protocol via Keycloak, an open source IdP (similar to Okta and other providers).

This server MUST be domain joined to the Active Directory server. Failure to do so MAY result in point penalty or disqualification from placement. This server will be fully joined to Active Directory during deployment.

Notes

- You MUST have port 80 open so that users can access the web application through the NGINX web server and you MUST have port 8080 open so that users are able to authenticate with Keycloak.
- There is an admin user for the Keycloak server. Go to www.team{num}.isucdc.com:8080 and it will take you to a sign in page for the admin dashboard. The default credentials are username: admin password: admin. From here you MAY make configuration changes to the keycloak server, but you MUST use the pre-configured “CyberPrint” realm and “CyberPrint” client. You MUST NOT make any significant changes to the authentication flow.
- There is a separate admin user for the Cyber Print web application. It MUST be named admin and it MUST have the associated email “admin@cyberprint.com”. It MUST be able to access the /admin page and access the /server-flag backend route so that it can easily see the /admin frontend flag and the /server-flag backend flag. This user already exists on deployment, its password is “cdc” and you can change it on the Keycloak admin page (www.team{num}.isucdc.com:8080).
- There are README’s with some additional information in ~/webapp/ICE25-CyberPrintNextjs as well as ~/keycloakconf
- Be mindful of the changes you make to the code and system, test frequently, take snapshots, and revert if something breaks

Startup Guide [***Important***]

- Before the web application can become functional, you MUST do some initial configuration:

1. Cd into ~/webapp/ICE25-CyberPrintNextjs/business-website
2. Open .env.local in your text editor of choice
3. Replace the spots identified between < > with the proper value
    a. You MUST set the /admin frontend flag and /server-flag backend flag in this file with the appropriate flag values from ISCORE.
4. Save the changes, then exit and in the same directory, run “yarn build”
5. After the previous command completes, run “sudo systemctl restart nextjs-app.service”

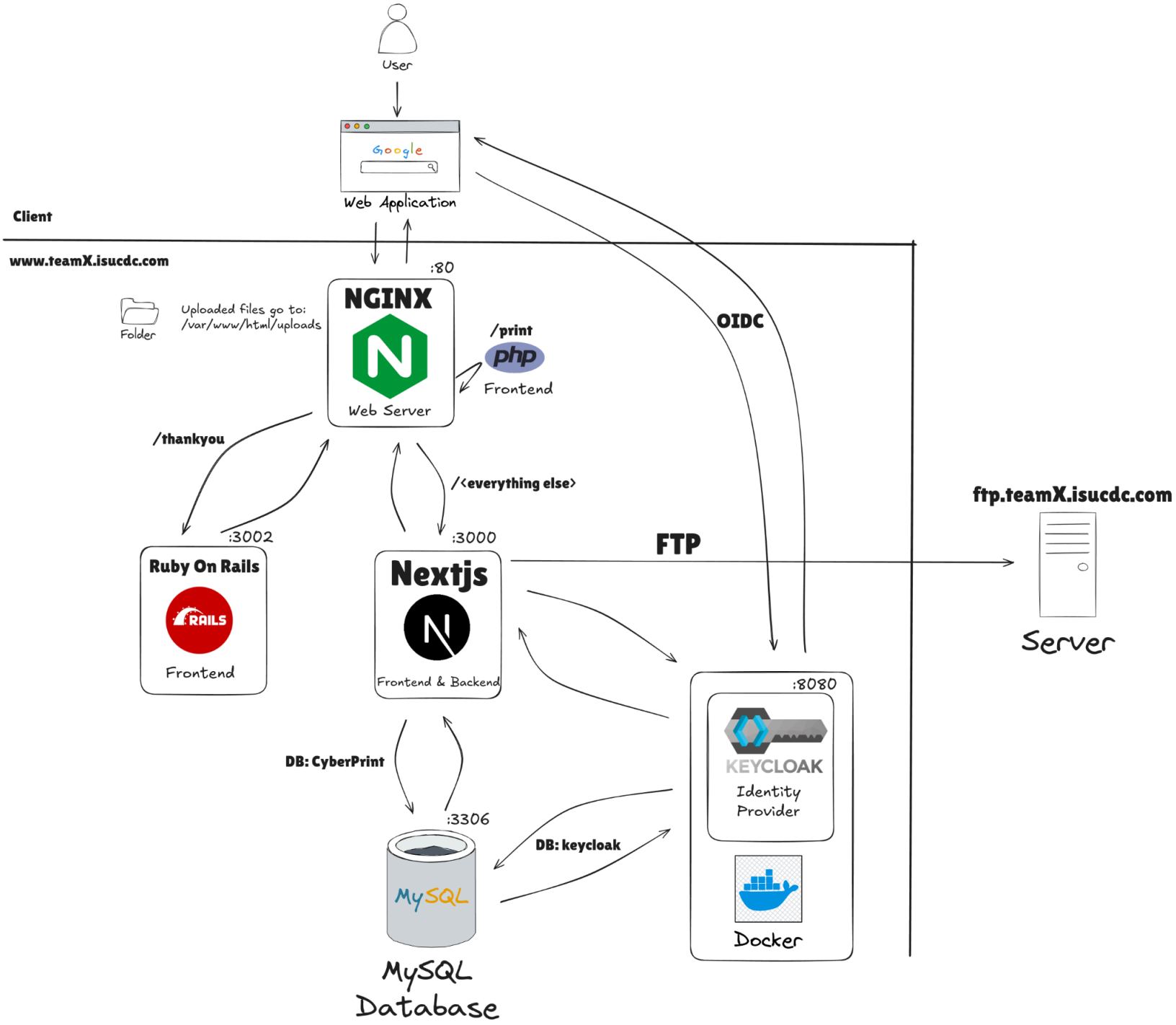
Required Access

- HTTP Access on TCP port 80
    - MUST be accessible from the Competition Network
- HTTP Access on TCP port 8080
    - MUST be accessible from the Competition Network
- SSH access on TCP port 22
    - IT Admins MUST be able to access SSH
    - IT Admins MUST have Administrative access
    - MUST be accessible from the Competition Network

Flags

- Red
    - Deface the WWW Home page
    - /root/
- Blue
    - /etc/
    - /admin frontend flag
    - /server-flag backend flag
    - Access another user’s (green team’s) saved card information (does not have to be placed prior to attack phase)

here


User
Google
Web Application
Client
www.teamX.isucdc.com
:80
NGINX
Web Server
Folder
Uploaded files go to:
/var/www/html/uploads
/print
php
Frontend
OIDC
/thankyou
/<everything else>
:3002
Ruby On Rails
RAILS
Frontend
:3000
Nextjs
Frontend & Backend
FTP
ftp.teamX.isucdc.com
Server
:8080
KEYCLOAK
Identity
Provider
Docker
DB: CyberPrint
:3306
DB: keycloak
MySQL
MySQL
Database

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:

- CEO
- IT Administrators
- 3D Printing Technicians
- Human Resources
- Customers (Shared TSI)

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.