International Cybersecurity Exercise (ICE) 2024

Scenario

IOWA STATE UNIVERSITY
Center for Cybersecurity Innovation & Outreach
Spring 2024

Table of Contents

ICE 2024

Servers

- Generator (gen.team{num}.isucdc.com)
  - Required Access
  - Flags
- MQTT (mqtt.team{num}.isucdc.com)
  - Required Access
  - Flags
- Frontend (frontend.team{num}.isucdc.com)
  - Required Access
  - Flags
- Backend (backend.team{num}.isucdc.com)
  - Required Access
  - Flags
- AD (ad.team{num}.isucdc.com)
  - Required Access
  - Flags
- Camera (cam.team{num}.isucdc.com)
  - 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

Page Intentionally Left Blank

International Cybersecurity Exercise

(ICE) 2024

A tremor of darkness ripples through our promise of light. Millions in Ivory City rely on ISEtricity, and a recent intrusion within our core systems threatens to plunge our vibrant hub into chaos. Fear not, for at the heart of this crisis lies opportunity. You, our valued team member, are now called upon to be a spark of defiance against the shadows. Rogue elements within our IT and security teams attempted to manipulate the very pulse of our city's lifeblood: the power grid. This blatant attack on our integrity, on the trust of millions, demands more than just repair. We need your expertise, your dedication, your unwavering commitment to innovation. As a critical member of our defense team, you'll spearhead the mission to fortify our digital armor, identify and neutralize any lingering sabotage, and ensure the uninterrupted flow of energy upon which our city thrives.

This won't be easy. There will be challenges, moments of doubt, and the gnawing fear of the unknown. But remember, every line of code you write, every firewall you strengthen, every vulnerability you patch is a victory song for the light. You are not just safeguarding homes and businesses; you are safeguarding the future of progress, the engine of dreams that fuels our city's spirit. In the face of adversity, ISEtricity has always emerged stronger. And this time will be no different. Together, we will not only overcome this threat but emerge as a beacon of security, a testament to the unwavering human spirit. So join us, raise your torch of resolve, and let's turn this chapter of darkness into a dazzling saga of resilience. The future of Ivory City's energy, and beyond, rests in your hands. Step forward, and become the hero this moment demands.

Link to scenario video: ▶ ICE 2024 Scenario Video

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.

Power Grid

The “Power Grid” service check determines whether or not your power grid is producing enough to fulfill the requested power level from the substations. In order for your power grid to function properly, the Backend, MQTT, and Generator servers MUST all be functioning properly and have the required access listed in the server descriptions. At each service check, you will get 1 of 3 statuses:

Green: Indicates your grid is functioning and producing enough power, this will cause full points [50] to be awarded for that portion of the service check.

Yellow: Indicates your grid is functioning but not producing enough power, this indication means your system is running, but not producing enough power. This partially working system causes the team to be awarded 50% of the points [25] for this portion of the service check.

Red: Indicates your grid is not functioning properly and IScorE is not receiving updates from your Generator, this causes no points to be awarded for this portion of the service check

Substations

The substations that determine the power draw on your grid are hosted by ISEAGE and are not controlled by or visible to your team. Every 5-7 minutes the substations will generate a new power level and update your team’s Backend server. Each team will receive the same requested power level.

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.

Generator (gen.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows 7 Embedded

This is the generator for the power grid. It receives control signals from the Backend server and adjusts its power output accordingly. It also reports its power output back to the Backend server for logging and IScorE for grading. The power output of the Generator can be adjusted through the Frontend web interface.

This server does not need to be domain joined to the Active Directory server, but the users that need access MUST have accounts with the proper credentials provided in IScorE. NOTE: The RDP check will time-out if the users are not added to this server.

Notes

- You can start the generator by opening a command prompt and using the command *generator-start* or by calling the generator-config.ps1 script
- The generator binary can be found in C:\Generator
- The generator is set to communicate with your MQTT server at x.x.x.20 by default. If you change the address of your MQTT server you will need to update the generator-config file found at C:\Generator\generator-config and restart the generator.

Required Access

- MQTT access on TCP port 1883
  - The generator MUST be able to communicate with the MQTT server on port 1883
  - Both inbound and outbound traffic are REQUIRED
- RDP access on TCP port 3389
  - Technicians and IT Admins MUST be able to RDP into the box.
  - Must be accessible from the Competition Network

Flags

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

MQTT Broker (mqtt.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu 20.04

This is the MQTT Broker that handles the communication between the Generator and the Backend server. It runs Eclipse Mosquitto. This server is already configured and ready to use.

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

- Mosquitto can be controlled using *systemctl <command> mosquitto*
- No configuration is needed for the Generator and Backend to communicate

Required Access

- SSH access on port 22
    - CISO and IT Admins MUST be able to SSH and have sudo privileges
    - MUST be accessible from the Competition Network
- MQTT access on port 1883
    - The Generator and Backend MUST have access to this port
    - MUST be accessible from the Competition Network

Flags

- Red
    - Create a new user with sudo privileges
- Blue
    - /root/

Frontend (frontend.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows 10

This is the frontend web application for the power grid. From web page you are able to view logs stored on the Backend, view the current powerdraw requested from the Substations, view the Camera feeds from around the plant, and control the Generators power levels. This application uses your AD server for user authentication and the video feeds from the Camera.

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 program files are contained in the C:\Frontend directory
- To rebuild the program, run “npm run build” in the C:\Frontend directory or by using the “Frontend Initialize” shortcut on the desktop
- To start the web server, run “npm run start” in the C:\Frontend directory or by using the “Frontend Start” shortcut on the desktop
- Before starting the program for the first time, you MUST configure the C:\Frontend\.env.local file. Replace the four <> fields with their corresponding values
- Your frontend webpage can be accessed by searching either localhost:3000 when on the box or frontend.team{num}.isucdc.com:3000 from the Competition Network.

Required Access

- Administrative RDP access on TCP port 3389
    - Admins MUST be able to RDP and do administrative tasks on the system such as adding/removing users with administrator privileges
    - MUST be accessible from the Competition Network
- HTTP access on TCP port 3000
    - The Frontend and Backend MUST be able to communicate
    - The following roles MUST be able to log in and use the Frontend web application
        - CEO
        - CISO
        - IT Admin
        - Head Technician
        - Technician
        - Developer
    - MUST be accessible from the Competition Network

- LDAP on TCP port 389
  - The Frontend MUST be able to contact the AD for user authentication
- HTTP access on TCP port 8000
  - The Frontend MUST be able to contact the Camera for video feeds

Flags

- Red
  - Website defacement
- Blue
  - C:\Windows\System32

Backend (backend.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu 16.04

This server facilitates communication between between the Substations, Frontend, and the Generator. The Backend logs the current Substation values and the current Generator output. The program runs on boot with a service named “backend.service”, more information regarding the Backend service can be found in the Notes section.

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 JAR file can be found in the /etc/backend directory
- The backend server can either be started with “/bin/backend” or “systemctl start backend”
- If you change the IP address of your MQTT server you MUST update the **IP=”x.x.x.x”** line in the /bin/backend file
- To restart the Backend (i.e. after changing the /bin/backend file) you MUST run “systemctl restart backend” for the changes to take effect

Required Access

- SSH access on TCP port 22
    - IT Admins and the CISO MUST be able to SSH and have sudo privileges
    - MUST be accessible from the Competition Network
- HTTP access on TCP port 8080
    - The Frontend and Backend MUST be able to communicate
    - MUST be accessible from the Competition Network

Flags

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

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

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

This is the main management console for credentials of employees. This is also the employee management console, and IT Administrators must be able to hire, fire, and alter employee accounts.

Required Access

- Administrative RDP Access on port 3389
    - IT Admins and CISO MUST be able to perform administrative actions such as adding/removing users with Administrator privileges.
    - The Frontend MUST be able to reach the AD for user authentication
    - MUST be accessible from the Competition Network

Flags

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

Camera (cam.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu Server 22.04

This is the security camera system for the building. The company recently discovered that the former security guard was attempting to sabotage the system! The company has given you permission to review the security camera feeds and remove any that are deemed a risk to the companies security. The removal of a camera feed MUST be documented in your WHITE docs with a justification for the removal. The camera feeds can be viewed in the Frontend web application.

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 camera feeds are accessed through the Frontend website
- The camera feed can be started with: systemctl start camera
- The camera feeds are stored as .mp4 files in the /Camera_Feeds directory
- The removal of any camera feed MUST be noted in your White Documentation

Required Access

- SSH access on TCP port 22
    - IT Admins and the CISO MUST be able to SSH and have sudo privileges
    - MUST be accessible from the Competition Network
- HTTP access on TCP port 8000
    - The Frontend MUST be able to reach the Camera for video feeds
    - MUST be accessible from the Competition Network

Flags

- Red
    - Add a new camera feed
- Blue
    - /etc/flag/

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 any application code on the server, 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
- CISO
- IT Admin
- Head Technician
- Technician
- Developer
- Security Guard
- Customer

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 not 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.