ISU 1 2025

Scenario

IOWA STATE UNIVERSITY,
Fall 2025

Table of Contents

Competition Scoring Guide
Competition Rules
Setting Up a Server
Remote Setup Guide

Page Intentionally Left Blank

Revision History

Revision 1.0.0:

- Initial Release

ISU 1

Welcome to CDC Channel 4 News, a small local news station in the quaint college town of Ames, Iowa. We look to serve our community with a local over-the-air and cable broadcast, website, and live weather updates. We employ Meteorologists, Journalists, HR staff, and IT Administrators to ensure news is efficiently and accurately shared with the townspeople.

In this digital age, we need more than just a broadcasting setup to achieve this goal. We also use an Active Directory server for user management, a lobby TV computer playing the broadcast, and a web server to host our website, along with computers for journalists to write and publish news articles for the website. Additionally, we've partnered with a college group to bring real-time weather information to our website via a weather station.

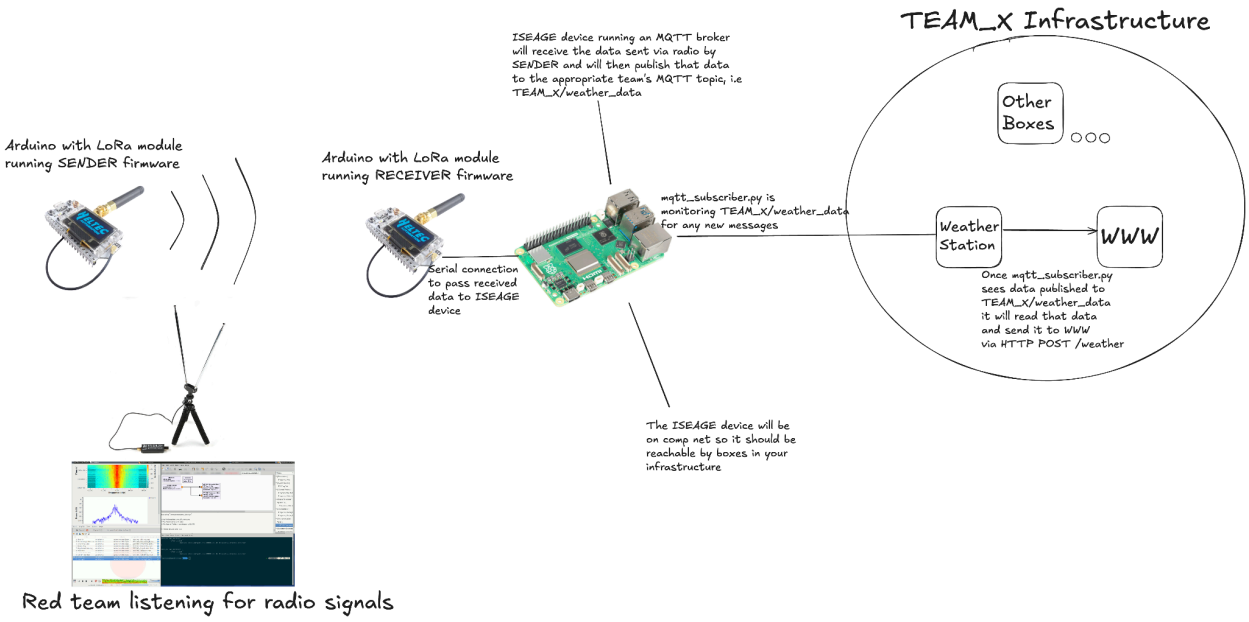
However, with the rise of cybercrime and "script kiddies" looking to make a name for themselves, we fear that the exploitation of our outdated systems may pose a risk to our reputation and disrupt our operations. Recently, an employee accidentally clicked a malicious link from a "vishing" email and ended up downloading and running malware on his computer. While our network activity hasn't seen anything out of the ordinary yet, we worry that APTs, or Advanced Persistent Threats which serve as backdoors for hackers to exploit later, were planted throughout our network.

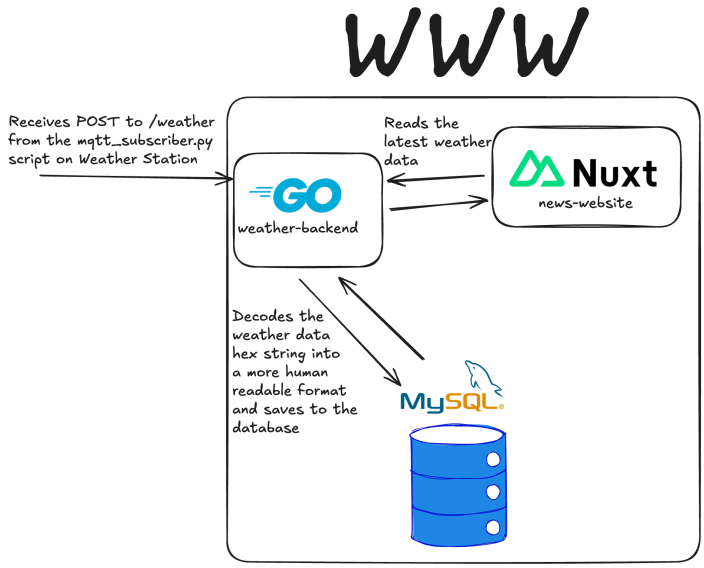
Additionally, due to recent layoffs and industry strikes, we worry about disgruntled employees adding backdoors or tampering with our network.

Your task is to audit the network, patch vulnerable systems, and remove hacker backdoors. Due to the volatile nature of APTs, swiftness is essential. Secure our network before it's too late!

Big Picture:

This scenario includes an active directory to manage identities, a journalist desktop to simulate an employee's computer, a lobby TV that adversaries will have "physical" access to, a News channel box that hosts some API endpoints, a weather station which receives radio communications from the weather balloon, and a web server box to host the news web application. Here is a diagram of how the weather data (along with a flag) will be transmitted over radio and be received by the weather station box.





Notice how red team is able to listen to the radio broadcasts which is broadcasting weather data (and a flag) for your team? You will have the chance to implement a manipulateOutgoingPayloadData function (described below) that ISEAGE will then flash onto the Arduino before broadcasting your team's weather data. Here you can choose to manipulate the data as you wish, but you will then have to convert it back to its original form someplace before it gets used by the website, which needs to be able to use the weather data.

What is LoRa? LoRa (**Long Range**) is a low-power wireless communication technology designed for sending small amounts of data over long distances (kilometers) with minimal energy use.

What is MQTT? MQTT (**Message Queuing Telemetry Transport**) is a lightweight messaging protocol that uses a publish/subscribe model to exchange data between devices, optimized for low bandwidth and unreliable networks.

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.

Active Directory (ad.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2019

The Active Directory (AD) machine manages scenario users across all machines. This means that creating an AD user allows that user to log in to any machines in the domain. Be sure to properly configure permissions on your AD users!

Notes

- ALL scenario machines should be joined to this Active Directory machine. Failure to do so will result in ineligibility from placing in the Top 3. By default, all machines are already connected.

Required Access

- LDAP on port 389
  - This machine MUST be contacted by all other machines on port 389 for the purpose of LDAP user authentication.
- RDP on port 3389
  - IT Administrators MUST be able to RDP into this machine and have Administrator-level account privileges.
  - HR Staff MUST be able to RDP into this machine.
- HR Staff MUST be able to add and remove users from this machine,

Flags

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

Journalist Desktop (jd.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Windows 11

This is the desktop computer that the journalists use to create, revise, and publish news stories to the website.

This server must be domain joined to the Active Directory server. Failure to do so will result in your team being unable to place in the Top 3. This server is joined to the AD by default.

Notes

- The purpose of this machine is to act as a point to log in to the website, where users can manage articles.

Required Access

- RDP on port 3389
    - IT Administrators MUST be able to RDP into this machine and have Administrator-level account privileges.
    - Journalists MUST be able to RDP into this machine

Flags

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

Lobby TV (ltv.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu 14.04

This represents a TV in the studio lobby that plays the news stream from the news channel machine. This is also what a viewer would see live.

This server must be domain joined to the Active Directory server. Failure to do so will result in your team being unable to place in the Top 3. This server is joined to the AD by default.

Notes

- This computer would be connected to a TV in the lobby, which serves as a way to view the news broadcast. Because this would be connected to the TV, the broadcast MUST be displayed on the screen at all times. You will need to do any investigation or monitoring remotely instead of via the console in vCenter.
- To display the broadcast run: mpv --ontop --fullscreen --loop=inf http://news.team#.isucdc.com:8080/broadcast/news/live
- The lobby is a semi-public area, so Red team WILL HAVE PHYSICAL ACCESS to this machine. Since it is a virtual machine, this means that they will have access to this VM's console in vCenter and be able to modify a limited number of settings and hardware configurations. If you notice someone "PHYSICALLY" tampering with your machine (not over the network, but through vCenter), you may call security (White team) to escort the user out of the lobby.

Required Access

- Administrative SSH Access on port 22
    - IT Administrators MUST be able to access this machine via SSH for system administration purposes. They MUST have Administrator access.
- News broadcast MUST be displayed on the screen

Flags

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

News Channel (news.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 18.04

This computer represents the news station's API service. The machine provides a "live broadcast" of the news and a public API to access its weather data.

This server must be domain joined to the Active Directory server. Failure to do so will result in your team being unable to place in the Top 3. This server is joined to the AD by default.

Notes

- The newsapi systemd service runs the JAR located in the cdc user's home directory for the backend API.
- You MAY modify the API application according to the Migrating Systems rules detailed below, provided all legitimate functionality is preserved.

Required Access

- Administrative SSH Access on port 22
    - IT Administrators MUST be able to access this machine via SSH for system administration purposes. They MUST have Administrator access.
- The website and weather station MUST be able to use the HTTP API hosted on port 8080.
- HTTP access on port 8080 MUST be available from the competition network.

Flags

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

Weather Station (wstn.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Debian 11

The weather station provides “real time” weather information that is pushed to the website and API.

This server must be domain joined to the Active Directory server. Failure to do so will result in your team being unable to place in the Top 3. This server is joined to the AD by default.

Notes

- The python script to push the weather data is located at /opt/weather_station/mqtt_subscriber.py and the startup script is located at /etc/systemd/system/weather-station.service
- The box comes with a publish_mqtt_test.py script in /opt/weather_station/ as well as Mosquitto (a MQTT broker service). This is provided for testing purposes. To test, run the publish_mqtt_test.py. This script will publish data to the MQTT broker, which the mqtt_subscriber.py script should pick up and then send in a POST request to the weather backend.
- On comp day, you will not be using the test script but instead will be receiving the data from an external MQTT broker. Because of this, you will need to change the MQTT broker IP address variable in the subscriber script to the external MQTT broker (TBD).

Required Access

- Administrative SSH Access on port 22
    - IT Administrators MUST be able to access this machine via SSH for system administration purposes. They MUST have Administrator access.
    - Meteorologists MUST be able to access this machine via SSH and modify the weather program.
- The Weather station MUST be able to push new weather data to the news backend and website.
- MQTT Access on port 1883

Flags

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

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

Default Username: cdc
Default Password: cdc

Operating System: Debian 12

The website hosts news stories, temperature data from the station, and the HTTP video stream.

This server must be domain joined to the Active Directory server. Failure to do so will result in your team being unable to place in the Top 3. This server is joined to the AD by default.

Notes

- All of the code for the website's frontend and backend are found in /home/cdc. There are several READMEs to help you understand the application.
- This box contains the news station website in /home/cdc/news-website. This is a Nuxt application (a Vue framework) that contains the frontend code in news-wesbite/app and some backend code in news-website/server. You will need to modify the Environment variables in /etc/systemd/system/news-website.service to the correct address of the NEWS box and your team's provided flag.
- There is additionally a standalone backend server written in Go in /home/cdc/weather-backend. There is a GET endpoint for getting the latest weather data in this app, and it must check that the incoming request has x-api-key-flag set to the flag. This is already coded, you will just need to change the variable in backend.go and rebuild it (instructions in /home/cdc/README).
- The web application also uses MySQL and is hosted behind an Apache reverse proxy

Required Access

- Administrative SSH Access on port 22
    - IT Administrators MUST be able to access this machine via SSH for system administration purposes. They MUST have Administrator access.
- HTTP Access on 80
    - Any user MUST be able to access the website to watch the news, read articles, and view the weather. This MUST be available from the competition network.

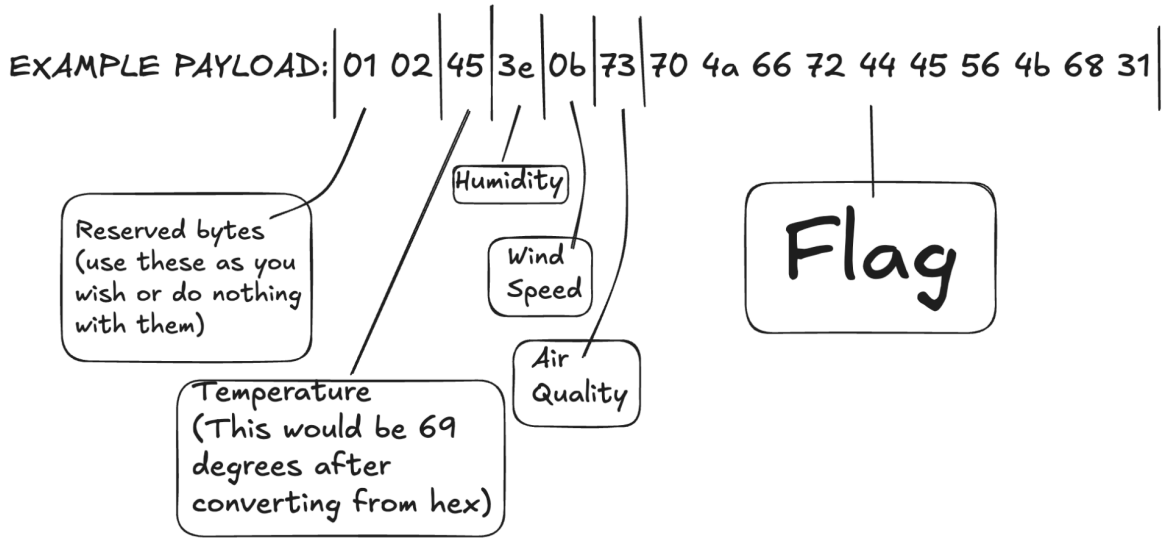
Flags

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

Arduino Firmware

As described above, this is not a box but rather a device that will be physically transmitting weather data and a flag for your team over radio. By default it will transmit data over plaintext. Due to a recent partnership with a secretive geo-engineering company, the data that the weather balloon collects must be kept secret. Here's how it works:

Since LoRa can only send small payloads of data and we want to send everything in one payload, we must be efficient with how weather data is formatted.



The very first byte (not pictured) will be your team number which is out of your control/cannot be manipulated so that the data gets posted to the correct TEAM_X/weather-data topic i.e. TEAM_40/weather_data.

The firmware can be attained here:
https://github.com/Januszski/ISU_1_2025_Weather_Balloon_Firmware
Keep in mind you are ONLY to modify the contents of manipulateOutgoingPayloadData(), nothing else.

You may use TRANSMITTAL_ITERATION. This will be manually adjusted by ISEAGE for each iteration, for example if its the first time we broadcast data for your team it will be set to 1, second time it will be set to 2 and so on.

On top of providing confidentiality to the data being transmitted by the weather balloon, think of other things you may be worried about as a security engineer. What if attackers capture a broadcast and later do a replay attack, causing your systems to display outdated weather data? This is why reserved bytes are provided.

Note that since attackers will not be able to physically get ahold of the balloon, in this scenario it is ok to hardcode secrets into the firmware/function.

To get started we recommend either using the Arduino IDE or a C IDE and copying over the pieces of code you may need, such as the manipulateOutgoingPayloadData() and the generatePayloadBytes() function. Print out the output of your function to make sure things look how you expect. The size of the payload must remain constant. Remember, whatever you encrypt must eventually be decrypted, so you can create a test payload with your custom program, copy the output, replace the RAW_HEX variable in publish_mqtt_test.py on the weather station box, run publish_mqtt_test.py to simulate receiving that payload from the ISEAGE MQTT broker, then make sure the data is decrypted somewhere along the way so that the website displays the up to date weather information.

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:

- IT Administrator
- HR Staff
- Meteorologist
- Journalist
- Subscriber

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.