NCDC 2022

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Spring 2022

Table of Contents

Page Intentionally Left Blank

NCDC 2022

Hello, Cyber Security and Grid Engineers!

We would like to extend our most sincere thanks to you for assisting us with our power grid. Truthfully, it has become quite difficult to maintain and keep secure from bad actors and nefarious types, so your addition to the team was a great choice on all fronts!

With it being the coldest part of the year, we want to ensure that our systems are locked down and stable to provide power to all of our customers at a reliable, sustainable rate, and we need your help to do it. Our software contractors have been on call around the clock to assist in your efforts as well, and will issue patches upon request, so be sure to security test their software! Not that we don't trust them, because we do, but sometimes, and this is certainly not common, their software has some very slight zero days that affect a small number of our machines, anywhere from 10% to 90% at worst, and, again, we do trust them, but we would love an external audit and some blue team help.

We expect some bad actors to be attacking the systems in the not-so-distant future, so audits, upgrades, patches, and documentation need to get done as soon as possible! We thank you, and our customers thank you.

Corporation for the Distribution of Current

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.

Controller GUI/Frontend (www.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu 16.04 LTS

NOTE: OS Migrations are allowed, but ONLY to the 18.04 LTS version of Ubuntu Server. This is also only to be done via the tools provided, and a reinstall of the operating system from scratch will not be allowed.

This is the interface that will be used to interact with the controller and substation. It is a simple Spring application located at /srv/gui/controllerGUI.jar and is being served with nginx. This is the application that engineers and billing employees use to monitor the health of the system and track billing as well as do maintenance and addition of new devices.

The source code has been provided in the same directory so that you may mitigate any vulnerabilities you find or for you to do quality of life improvements. **Rewrites will not be allowed. If you are unsure of a code change that may constitute a rewrite, consult the White Team at cdc_support@iastate.edu.**

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 Access to the Controller Application on port 80 or 443 respectively
    - Must be accessible from the Competition Network
    - Technicians, Accounting, and Administrative users must be able to log in to and interact with the UI.
    - See below for more specific access requirements.

Flags

- Red
    - Defacement of the main site
    - /root/
- Blue
    - /etc/
    - /home/

Controller Server (con.team{num}.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: Ubuntu 14.04 LTS

NOTE: OS Migrations are allowed, but ONLY to the 18.04 LTS version of Ubuntu Server. This is also only to be done via the tools provided, and a reinstall of the operating system from scratch will not be allowed.

This is the main controller for the system, and is the proxy between the Web GUI and the Substation. The binary is located at /srv/controller/con with a config file at /srv/controller/config.txt. It is a program that was contracted out and, as per the agreement, the source code is not available. However, should you find any vulnerabilities, you are able to submit a bug report and have a patched binary issued for that specific vulnerability.

Notes on Bug Reports and Patches:

- Please allow up to 5 business days for a patch to be issued. This is a worst-case though, and patches will usually be issued by the end of the next business day.
- You MUST submit the bug report with some specific pieces of information.
    - Specifics of the bug, such as steps to reproduce and what behavior you noticed
    - Screenshots and images as proof of the bug
    - Reasoning as to why the bug or vulnerability is a vulnerability. Simply saying "there might be a buffer overflow" will not be sufficient. Saying "this *could* lead to X, Y, or Z" may lead to a patch, but that will be determined by the developer. Stating potential fixes will result in a greater chance of receiving a patch.
    - Reports must be sent to cdc_support@iastate.edu with your team name and number clearly stated.
- Should you receive a patch, this will only be issued to the requesting team. This gives teams that do their due diligence an advantage when the competition comes.

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.
- Power Device Communication Protocol on port 8089
    - Must be accessible from the Competition Network
    - The GUI must be able to reach out to this box. If unable to, the GUI will not function properly.

Flags

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

SUBSTATION (sub.team{num}.isucdc.com)

Operating System: Modern Embedded Linux

This is a critical component of the power delivery system. It is the central hub of the whole system. It is used by the controller to monitor the health of the system, and it is responsible for distributing the load to the generator. It is an embedded device, and as such, a shell is not available on the console, instead a configuration menu is provided. However, if maintenance mode or a fault is triggered, a SSH server will be spawned so Technicians can connect and perform maintenance. It accepts connections from the general public and also connects to all the generators, and as such, must be able to reach both. The source is not available for this service, however you may submit patches for any vulnerabilities or issues you may encounter.

Notes on Bug Reports and Patches:

- Please allow up to 3 business days for a patch to be issued. This is a worst-case though, and patches will usually be issued sooner than that.
- To expedite the patching process, please submit the patch request with some specific pieces of information:
    - Specifics of the bug or issue, such as steps to reproduce and what behavior you noticed
    - Screenshots or images as proof of the bug or issue
    - Reasoning as to why the issue is a problem. Simply saying “there might be a buffer overflow” will not be sufficient. Saying “this *could* lead to X, Y, or Z” may lead to a patch, but that will be determined by the developer. Stating potential fixes will result in a greater chance of receiving a patch.
    - Reports must be sent to cdc_support@iastate.edu with your team name and number clearly stated.
- Should you receive a patch confirmation, it will only be installed on the requesting team’s systems. This gives teams that do their due diligence an advantage when the competition comes.

Required Access

- Power Device Communication Protocol on port 8085
    - Must be accessible from the Competition Network
    - Must be accessible to the Controller box. If the controller is not able to reach this service, it will not function properly.
- Administrative Technician SSH on port 1622
    - This will not be enabled by default. Only fault or maintenance conditions will trigger it to open. However, it must remain always accessible.
    - Must be accessible from the Competition Network

- Technicians and External Contractors will be logging in to perform maintenance and patching. If they are unable to do so, your machines may not be able to be patched.

Flags

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

GENERATORS (gen{N}.team{num}.isucdc.com)

Operating System: Modern Embedded Linux

This is a main component of the power delivery system. It is the powerhouse of the whole system. The substation connects to this device to configure it and monitor it. It consumes fuel proportional to the current wattage every thirty seconds. It is an embedded device, and as such, a shell is not available on the console, instead a configuration menu is provided. However, if maintenance mode or a fault is triggered, a SSH server will be spawned so Technicians can connect and perform maintenance. It accepts connections from the substation, and as such, must be able to be reached by it. The source is not available for this service, however you may submit patches for any vulnerabilities or issues you may encounter.

Notes on Bug Reports and Patches:

- Please allow up to 3 business days for a patch to be issued. This is a worst-case though, and patches will usually be issued sooner than that.
- To expedite the patching process, please submit the patch request with some specific pieces of information:
    - Specifics of the bug or issue, such as steps to reproduce and what behavior you noticed
    - Screenshots or images as proof of the bug or issue
    - Reasoning as to why the issue is a problem. Simply saying “there might be a buffer overflow” will not be sufficient. Saying “this *could* lead to X, Y, or Z” may lead to a patch, but that will be determined by the developer. Stating potential fixes will result in a greater chance of receiving a patch.
    - Reports must be sent to cdc_support@iastate.edu with your team name and number clearly stated.
- Should you receive a patch confirmation, it will only be installed on the requesting team’s systems. This gives teams that do their due diligence an advantage when the competition comes.

Required Access

- Power Delivery Communication Protocol on port 8087
    - Must be accessible to the Substation box. If the controller is not able to reach this service, it will not function properly.
    - Does **NOT** need to be publicly accessible.
- Administrative Technician SSH on port 1622
    - This will not be enabled by default. Only fault or maintenance conditions will trigger it to open. However, it must remain always accessible.
    - Must be accessible to the Substation box.
    - Does **NOT** need to be publicly accessible.

- Technicians and External Contractors will be logging in to perform maintenance and patching. If they are unable to do so, your machines may not be able to be patched.

Flags

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

Billing (billing.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2012 R2

This server is meant for accounting folks to be able to collaborate with each other on billing and financial documents related to power consumption and billing the customers. Employees will remote in and share spreadsheets with each other.

Required Access

- RDP Access on port 3389
    - Must be accessible from the Competition Network
    - Accounting users must be able to RDP in and create, update, and delete spreadsheets and share them with other accounting employees.
    - Administrators must be able to perform administrative actions on the virtual machine.

Flags

- Red
    - Creating spreadsheet in C:\Windows\System32
- Blue
    - C:\Users\Administrator\

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
  - This user role must have Administrator or root access on all machines possible
- Senior Technician
  - This user role must have Administrator or root on the devices and controller server to perform maintenance. They should also have login and full access to the GUI and have SSH access to the GUI server, although root is not required.
- Technician
  - This user must have SSH access to the substation and login on the device servers, as well as login and interaction with the GUI
- Software Developer
  - This user must have SSH access on the controller server and the gui server in order to perform application maintenance and patches. They do not need root, but must be able to update and move the applications, the application configurations, and restart the services.
- Power Grid Operator
  - This user must be able to log in to the GUI application to add new devices and view the system health.
- Accounting Chair
  - This user must be able to log in to the GUI application and view the current draw percentage to get billing information. This user must be able to RDP into the Billing server in order to create, update, and delete billing spreadsheets.
- Accountant
  - This user is expected to have the same permissions as the above role.

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.