High School CDC 2021

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Spring 2021

Table of Contents

Setting Up a Server
Remote Setup Guide

Page Intentionally Left Blank

High School CDC 2021

WOOP! WOOP! That's the sound of the ambulance! Welcome to the Critical Dysfunction Centre! This Emergency Room is always bustling with new arrivals from ambulances, along with other goobers who get injured and arrive, needing to see a doctor or receive critical care.

Here at the Critical Dysfunction Centre, we try our best to care for all patients and their needs. We have a wide variety of services for our patrons, from urgent care to emergency visits to pharmacy, all in house! And you have been tasked with the most important job of them all: securing our services!

We would hate to get a violation for losing patient data, so please, do your best to secure the services as best you can from the evil hackers who would want to steal the data! We're counting on your team to do a great job.

Thanks,

Critical Dysfunction Centre

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.

Ambulance (ambl.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2012 R2

This is the simulated Ambulance for the hospital. Ambulance drivers and EMTs should be able to log into this box and run the application in order to register patients with the hospital.

Notes

- A binary can be found in C:\Program Files (x86)\Ambulance\Ambulance.application and the source code can be found in the same directory as Ambulance, called Source.zip
- This will need to be able to contact the API server for authentication and CRUD actions.

Required Access

- Administrative RDP Access on port 3389
    - Must be accessible from the Competition Network
    - All EMTs, Ambulance Drivers, and IT Administrators must be able to run and interact with the ambulance application.
    - Administrators must be able to perform administrative actions on the machine.

Flags

- Red
    - Add a new patient into the database with the FirstName being the flag
- Blue
    - C:\Windows\System32

DocView DX (docview.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc2021

Operating System: Windows Server 2019

This is the main software that doctors and nurses use to view and edit patient details and statuses. It is a fairly complex piece of software. It was created by an external software contractor, called Northwind Software. It has a background service and a client component that communicates over WCF. The main client is using WPF for the application UI rendering. The software will save credentials in the Windows Credential Manager after the first login. The service component must run with elevated credentials as it reads from a protected section of the Windows Registry. The background service is the piece that communicates with the API, so the API must be reachable by it. An installer has been created to aid installation.

Notes

- The source of the application is available in the Administrator accounts desktop folder, in a file called, Source.zip
- The program reads from the HKLM:\SOFTWARE\WOW6432Node\NorthwindSoftware\ registry key in order to load it's configuration. In particular, the BaseAddress REG_SZ value is the address of the API machine.

Required Access

- Administrative RDP Access on port 3389
    - Must be accessible from the Competition Network
    - All Doctors, and Nurses must be able to run and interact with the DocView application.
    - Administrators must be able to perform administrative actions on the machine.

Flags

- Red
    - HKLM:\SOFTWARE\WOW6432Node\NorthwindSoftware\Flag
- Blue
    - C:\Windows\System32\

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

Default Username: root
Default Password: root

Operating System: Ubuntu Server 18.04.5

Notes

- It holds medical and patient information and interacts directly with the API.
- Data can be accessed via a PostgreSQL console.

Required Access

- PostgresSQL Access on port 5432
    - Must be accessible from the Competition Network
    - Administrators must be able to perform administrative actions on the machine
- Administrative SSH Access on port 22
    - Must be accessible by administrators on the Competition Network
    - Administrators must be able to perform administrative actions on the machine

Flags

- Red
    - /etc/groff/
- Blue
    - /etc/ssh/

API (api.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 20.04

Notes

- The binary is located at /usr/local/bin
- The configuration file is located at /etc/itoapi
- The service file is located at /etc/systemd/system/itoapi.service
- Nginx is serving as a proxy to add cors headers

Required Access

- Administrative ssh access must be available on port 22
    - Must be accessible from the Competition Network
    - Administrators must be able to perform admin tasks
- All EMTs, Ambulance Drivers, Doctors, Patients, and IT Administrators must be able to access the api on port 80 and interact with the ambulance application, docview, and the patient portal using the api.
    - Must be accessible from the Competition Network

Flags

- Red
    - Add a proxy header in nginx api service with the proxy header being the flag
- Blue
    - /root

Patient Portal (portal.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 20.04

This acts as the patient portal that hospital patients can use to schedule appointments and check in for those appointments. Patients will need to login before being able to use the portal.

Notes

- The patient portal will require access to the API to verify credentials.

Required Access

- Administrative SSH access on port 22.
    - Must be accessible in the Competition Network.
    - Administrators must be able to perform administrative actions on the virtual machine.
- HTTP/S Access to the Patient Portal on port 80 or 443 respectively
    - Must be accessible on the Competition Network
    - Must be accessible by all users, including unauthenticated users

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 the 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:

- CFO
  - As the CFO, this role has unfettered access to all things because they say so. Treat this role as an IT Administrator.
- IT Administrator
  - This role will need Administrator level permissions on all boxes to perform administrative actions.
- Department Head (Head of Oncology, Immunology, Surgery)
  - This role should have administrator access to all applications lined out in the scenario, but not necessarily the system. They should be able to make changes and interact with the applications, but do not need to have Administrator access on the systems themselves.
- Doctor
  - This role must have full access to the DocView application as well as some other abilities outlined in the scenario above. Does not need Administrator.
- Nurse
  - This role must have the same permissions as the Doctor role and should be treated as effectively the same.
- EMT
  - This role will need full access to the Ambulance application to add patients, but not necessarily Administrator access on the system.
- Ambulance Driver
  - This role must have the same access as the EMT, and should be treated as effectively the same.

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.