ITO 2022

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
ITO 2022

Table of Contents

Setting Up a Server
Remote Setup Guide

Page Intentionally Left Blank

ITO 2022

Dear Security Team,

We are in desperate need of securing our pharmacy! For decades we have been serving our customers medication needs, but not so must our security needs. We heard that you were the best and brightest, and would be able to assist us in our security venture.

Our systems include a point of sale system that every customer interacts with. It is our main revenue source, if it goes down we go down. The other main service is the doctor system. Doctors use this system daily to input prescriptions into our system. Without this system working it will be a long slow death of the company.

All of our information is stored in a database system which we contracted out years ago and did not pay for support. This system is critical to our organization because it holds all of our patient records. Without it working customers and doctors can not interact with our systems.

With our pharmacy being the largest in the world we have to handle many requests each day. We use a queue to speed up this process. Our amazing software engineers know everything about software but not much about security. We desperately need help here.

Anything you and your team can do to help our security posture would be great! Our customers expect their information to be safe with us and the government expects

hippa to be followed. Anything you can do to help us here will greatly convince more customers to use us and that means more money!

Sincerely,

Corporate Doctor Center

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.

Pharmacy Point of Sale (sale.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows 10 IOT Enterprise

This is the main operating application of the hospital pharmacy. It connects to the database and pulls the prescriptions for the patients and medications that are available. It then allows the user to purchase their prescriptions and other medications. It also has a menu for the pharmacy workers, which allows them to manage prescriptions for patients and allow the pharmacist to check out patients.

It operates in two parts, a background HTTP server that interacts with the database and queue, and the GUI, which calls the HTTP server to perform the actual work.

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 source code and the compiled applications are located in C:\PointOfSale
- This will need to be able to contact the DB, Queue, and the Active Directory server for authentication and management operations.

Required Access

- RDP Access on port 3389
    - Must be accessible from the Competition Network
    - Patients must be able to connect via the “Guest” windows user
        - Patients **do not require** access to a desktop, **if** the Point of Sale application launches automatically when they login.
    - The pharmacist must be able to launch the application and login via their account **and** have access to a desktop for general user actions.
    - Administrators must be able to perform administrative actions on the virtual machine.

Flags

- Red
    - Add a new medication with the manufacturer being the flag
- Blue
    - C:\Windows\System32

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

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

This is the server that holds all of the patients, prescriptions, and medications. It is using MSSQL 2017 with three seperate tables with the previously mentioned items. The patient table will consist of the name, weight, height, date of birth, patient history, and prescriptions belonging to the patient. The prescription table will consist of the name of the prescription, who it's prescribed to, amount, and dosage. Finally, the medication table consists of the name and manufacturer.

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 point of sale will create any tables that are missing when the application starts

Required Access

- Administrative RDP Access on port 3389
    - Must be accessible from the Competition Network
    - IT Administrators must have full system access
- MSSQL access on port 1433
    - Must be accessible from the Competition Network

Flags

- Red
    - Creation of a new table
- Blue
    - C:\Windows\System32

Doctor System (doctor.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

This is the server hosting an application that the Doctors will be using to view, create, and modify patients and their data such as basic data, patient history, and prescriptions. The server will have the application sitting in C:\ProgramFiles(x86)\DoctorApplication and a configuration file in the same directory which should contain the addresses for the Queue and the Database. The app is dependent on the other two and will not function properly until they are configured. Additionally, the login is via AD credentials, and thus AD must also be configured to log into the 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 application needs networking access to correctly function

Required Access

- Administrative RDP Access on port 3389
    - Must be accessible from the Competition Network
    - IT admins, Head Doctor, and Doctors must be able to make new prescriptions and patients
    - Other user groups cannot login to the application or the users
    - Administrators must be able to perform administrative actions on the virtual machine.

Flags

- Red
    - Add a new patient “Flag” into the database with the patient history being the flag
- Blue
    - C:\Windows\System32

Queue (queue.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2012 R2

To avoid what are potential race-conditions in the database, we are utilizing a Queue for any database writes. Namely, adding new patients, medications, and prescriptions. The program will batch process items in the Queue and write them to the database as it receives them one-by-one and in order to ensure data integrity.

The Queue is a hosted RabbitMQ instance and the consumer is a custom application at C:\Program Files\QueueConsumer\QueueConsumer.exe. A database config file can be found in the same directory, called Config.txt. It contains only the IP address or domain name of the desired database.

The process is monitored by nssm, an executable for which can be found on the desktop.

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

- A binary can be found in C:\Program Files\Queue Consumer\
- This must be able to access the database. It will not work otherwise. It must also be able to access RabbitMQ on localhost.

Required Access

- Administrative RDP Access on port 3389
    - Must be accessible from the Competition Network
    - IT Administrators must have full system access
- RabbitMQ Web Interface on port 15672
    - Must be accessible from the Competition Network
    - IT Administrators and Department Heads must have full access to the RabbitMQ Interface
- RabbitMQ amqp on port 5672
    - Must be accessible from the Competition Network

Flags

- Red

    - Creation of a new Queue
- Blue
    - C:\Windows\System32

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

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2016

Our systems should use Active Directory for centralized authentication. The AD has been promoted to a domain controller and set with the respective team domain. All the boxes should be joined to this server to allow users to authenticate and login.

Notes

- **Any instances of the servers or services not joined to AD are subject to a point penalty at the discretion of the White team.**

Required Access

- Administrative RDP Access on port 3389
    - Must be accessible from the Competition Network
    - IT Administrators must have full system access
- LDAP/S on port 389 or 636 respectively
    - Must be accessible from the Competition Network
    - All users must be able to run LDAP queries with appropriate permissions

Flags

- Red
    - Add a new user
- Blue
    - C:\Windows\System32

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 must have root or Administrator privileges on all provided systems
- Department Head
  - This user must have full access to each application. This includes the Point of Sale, the Doctor Application, and RabbitMQ.
- Doctor
  - This user must be able to add new patients, modify existing patients, and create new prescriptions in the Doctor application. They must also be able to create new prescriptions for patients.
- Pharmacist
  - The pharmacist must be able to login to the Point of Sale system to manage medications, view all patient prescriptions, and purchase medications for patients.
- Patient
  - The patient must be able to connect to the Point of Sale system and purchase their assigned prescriptions and other medications. They do not need to have a desktop shell on the Point of Sale system, if the application starts as they login.

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.