ISU 1 CDC 2022

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
ISU1 2022

Table of Contents

Page Intentionally Left Blank

ISU 1 2022

Hello our fellow banking experts!

For over 2 months now, we at the Community Direct Credit Union have been trusted with our loyal customer's money to help them save, spend, and, most importantly, keep their money safe!

Due to a large boom in customers over the past week, we at the CDC have been working tirelessly on upgrades to our banking software, creating a new website, and finally creating a better and more secure customer database. Expanding, however, always comes with its downsides. We've been worried about potential cyber attacks on our software and machines. Because of that, we're looking to have a complete security analysis on all of our code. Taking a look at our infrastructure has been long overdue, especially for a business as popular as ours.

With your help, we can keep our customer's assets safe, and hopefully create more money for our customers (and of course… ourselves.) Everyone, employees and customers alike, will be extremely grateful for your help in a security analysis and upgrade!

We're counting on you!

Community Direct Credit Union

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 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. The specified boxes should be joined to the domain to allow domain users to login via LDAP/S.

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
    - Administrators must be able to perform administrative actions on the virtual machine
- 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
    - C:\Users\Administrator
- Blue
    - C:\Windows\System32

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

Default Username: root
Default Password: cdc

Operating System: Ubuntu Server

This is the database server for Community Direct Credit Union. This is where the information needed for the Banking App is stored.

This server must be domain joined to the Active Directory server. Failure to do so can result in point penalty or disqualification from placement.

Required Access

- Administrative SSH Access on port 22
    - Administrators must be able to perform administrative actions on the virtual machine.
    - Must be accessible from the Competition Network.
- It must be accessible to the Banking App on port 5432.

Flags

- Red
    - Add a Postgres user with the name being the flag.
- Blue
    - /etc/

Banking App (app.team{num}.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu 16.04

The banking app is the primary way for customers of the bank to access their accounts online. With the banking application still being in early development the application experiences crashes every now and then. The development of the application was outsourced in the name of money but in return updates come out at random. Once an update comes out teams need to do an upgrade in a timely manner to avoid upset customers and an upset management. If at any point a security issue is found while using the application a bug ticket can be submitted at cdc_support@iastate.edu but a fix is not guaranteed and could take days to implement.

This server must be domain joined to the Active Directory server. Failure to do so can result in point penalty or disqualification from placement.

This server's banking application must be upgraded when an upgrade comes out. Failure to do so can result in usability check point penalties and service scanner check point penalties.

Notes

- The application binary can be found in /usr/local/bin/app
- The systemd service file can be found at lib/systemd/system/app.service
- This will need to be able to contact the API and the Active Directory server for authentication and CRUD actions.

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.
    - Admins must be able to upgrade the application binary
- User HTTP/S access to the website on port 80 or 443 respectively
    - Users (green team / red team) must be able to access from the Competition Network

Flags

- Red
    - Add an http server on port 666
- Blue
    - /etc/app/flag.txt

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

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu 14.04

This static website serves to explain to customers who we are as a company and why they should trust us with their money. Made by the company owner personally!

Notes

- The code for the website is located at /home/cdc/www.
- The current website build is stored in /home/cdc/app-deploy.

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 to the website on port 80 or 443 respectively
    - All users must be able to view the website.
    - Must be accessible from the Competition Network

Flags

- Red
    - Site defacement
- Blue
    - /etc/

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:

- Bank President
- Bank Board Members
- Tellers
- Security Administrator

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.