HSCDC 2019

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
2019

Table of Contents

PAGE INTENTIONALLY LEFT BLANK

2019 HSCDC Scenario

Dear Community Department of Care,

Recently we have we have heard of various groups of hackers looking to try and scrape our patient medical records from our systems. While nothing so far has managed to break our secure systems, we are not sure things will remain this way.

We need your knowledge and know how to make sure our servers are in tip top shape for the next wave of attacks. You are tasked with locking down our public facing website, our postgreSQL database, our active directory authentication and lastly our RDP, which allows for our physicians to work and chart from home.

Most of our original IT members have been long gone, and as such we rely on your expertise to audit and secure our various diverse set of systems. Our business partners, DocView, have been kind enough to make their source code open to the public.

We are expecting a full lock down of our system while still allowing our various skilled staff continue their work for the community.

Thank you,

Community Department of Care Board of Directors

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.

WWW Box (www.teamN.isucdc.com)

Default Username: cdc
Default Password: cdc

Operating System: Ubuntu Server 18.04
Application Source: /root/www

It is a Django application running the site for patients to view their personal information. Each patient can login to the site and view all medical information about themselves. Admins have the ability to add new patients and modify old, existing patient data. It should be publicly accessible over the competition network through a web browser

Required Access

- HTTP on port 80 on the Competition Network
- SSH for Admins in port 22 on the Competition Network
- Admins should be able to modify and interact with the django code
- Admins, Dean of Medicine, Department Head, Surgeon, and Doctors should be able to log in to the django admin page and change, remove, and add Patient Objects, Link Objects, Users, and Groups
- Patients should be able to login through the web console to view their own data

Flags

- Blue Flags
    - Django settings
        - FLAG = 'FLAG_DATA_HERE'
    - /root/
- Red Flag
    - /etc/

DB Box (db.teamN.isucdc.com)

Default Username: root
Default Password: cdc

Operating System: CentOS 7

This is a PostgreSQL database machine that holds all information regarding patients as well as patient login credentials and doctor login credentials.

Required Access

- SSH for Admins in port 22 on the Competition Network
- PSQL over port 5432 on the Competition Network

Flags

- Blue flag: /etc/
- Red flag: /root/

RDP Box (rdp.teamN.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2008
Application Source: C:\DocView

The RDP box hosts a Windows Terminal Services instance on Window Server 2008. It has an application on it, DocView, that doctors and nurses use to enter patient data. It is an older and fragile system, tampering with it too much is pain.

While migrations are allowed for this box, it is not recommended, due to its ***very*** fragile nature.

Required Access

- RDP Access for all except for Patients on PORT 3389

Flags

- Blue Flag: C:\
- Red Flag: C:\back.png

Active Directory Box (ad.teamN.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2008 R2

The AD (Active Directory) box hosts Microsoft's Active Directory Services on Windows 2008. Your other boxes must authenticate user logins against this box's Active Directory.

Required Access

- RDP Access for IT Administrators on port 3389 for the Competition Network
- LDAP on port 389 on the Competition Network

Flags

- Blue Flag: C:\
- Red Flag: 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 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 specified otherwise. 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. Modifications are allowed as long as the core functionality remains present and is functional as expected.

User Roles

Role Type	Definition
IT Admin	The IT Admins are remote support for the hospital. They are the hospital’s administrators and handle the technical work for the hospital’s computers. They have full access over everything. To be clear: this account is synonymous with the “Administrator Account” role. Anytime our documentation refers to “Admin” or “Administrator”, this also means “IT Admin” or “IT Consultant.” See Administrator Accounts below for more.
Department Head	As much as we tell him that he doesn’t need Admin, he still insists upon it ‘Just in case’. They require the same access as an IT Manager.

Dean of Medicine	Access to DocView over RDP, and administrator access to our website through our Django app. To clarify, they require Django 'Super User' access as well as RDP login for access to DocView.
Surgeon	Required access to the DocView program over RDP through the RDP server.
Doctor	Required access to the DocView program over RDP through the RDP server.
Nurse	Required access to the DocView program over RDP through the RDP server.

User information can be found in the "Users" document. Team specific passwords are available on your dashboard on IScorE.

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 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".

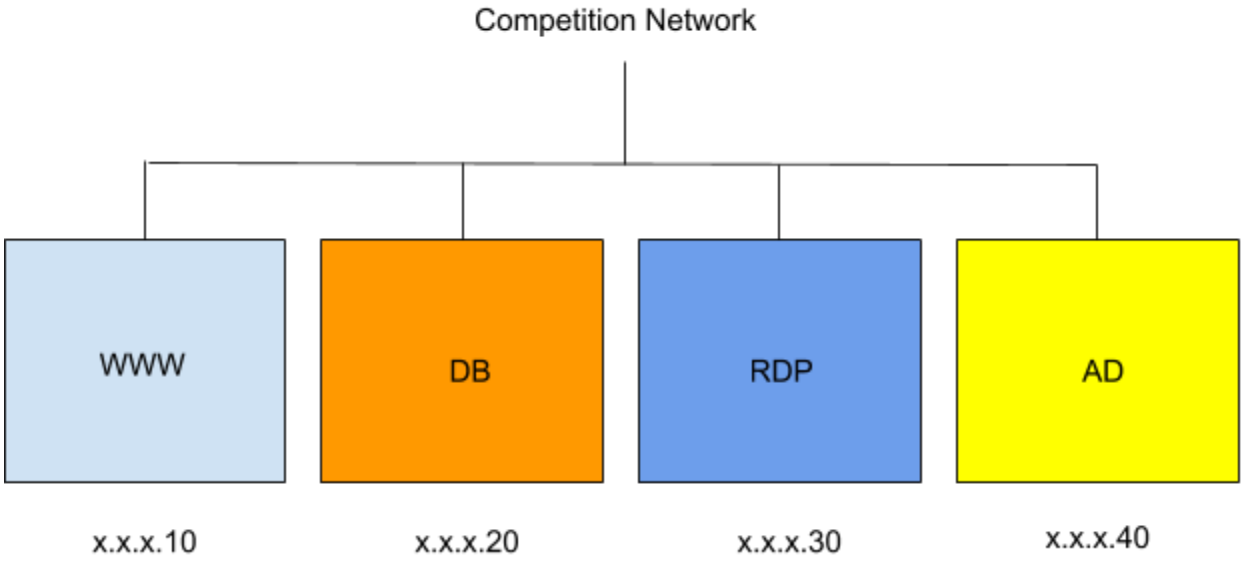
ISEPhone

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 4.1 of the competition rules will be used for this competition.

Network Diagram and Overview



Please review the competition rules, and specifically the “Requirements for Services” section for additional details on what is expected from your services.

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 setup 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 the VPN, and how to create a VM.