ITO - 2023

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Spring 2023

Table of Contents

Page Intentionally Left Blank

ITO CDC 2023

Hello fellow Gamers and Greetings from the Cubic Development Company!

My name is River and I am the CEO (Cubic Executive Officer) of the small Indie video game development company, Cubic Development. Unfortunately, we have been targeted by several hackers who have attempted to gain access to our networks and steal our source code so that they can make knockoffs of our games. Since we are a small company, we do not have a large budget to hire an outside firm to help us secure our devices so we need your help to stop these hackers from stealing our intellectual property and customer data. Our infrastructure contains four servers, a GitLab repository for our code, video game testing server, a forum, and a billing website. The GitLab and billing servers are highly important to us as one hosts our source code and the other contains sensitive customer information such as credit card numbers. We are hoping to avoid being the next headline in the news losing customer data to unnamed hackers, so please try your best to protect these servers. Since we do not have any security professionals on our team, you are likely to see all types of issues from code vulnerabilities to misconfigurations on the servers. In addition, you might find out that some of our devices have already been compromised, though we hope this is not the case. Should you come across a device that has been compromised/backdoored, please document this so that we are aware. In addition, if you make any major changes to the servers or code, please document this as well. Thank you and good luck! -River

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 functionality.

WordPress Website (www.team{num}.isucdc.com / x.x.x.10)

Operation System: CentOS 7

We have a WordPress site for our game. It should include instructions on how to use the game, but many of the pages are incomplete. It has some posts and pages which are deserving of some art awards, or something. Users MUST be able to leave comments on all posts and pages.

You MAY update to the latest WordPress. However, the existing content MUST still be present on the site and you MUST use the existing virtual machine and its operating system.

Setup

1. Login to website at www.team{num}.isucdc.com
2. Click on Settings
3. General
4. Change "WordPress Address (URL)" to www.team{num}.isucdc.com (replace {num} with your team number)
5. Change "Site Address (URL)" to www.team{num}.isucdc.com (replace {num} with your team number)
6. Click "Save Changes"

Required Access and Services

- SSH on port 22 on the Competition Network
    - Administrators MUST have full access to the machine
- HTTP/HTTPS on port 80/443 from on the Competition Network
    - Administrators MUST be Administrator in WordPress and have full control over the site
    - Anyone should be able to read the pages and posts on the site
    - Anyone should be able to leave a comment on all pages and posts
- An instruction page on how to use the game MUST be added to the website and MUST be accessible to all users.

Billing/DRM Website (billing.team{num}.isucdc.com / x.x.x.5)

Default Username: root
Default Password: cdc
Default MySql Username: root
Default MySql Username: cdc

Operation System: CentOS 7

This machine has multiple functions. Firstly, it serves as a way for users to purchase the “Adventures of Scrat”, and stores their information in the MySql database. Once purchased, users MUST be able to login and download the game. Next, it authenticates every user who tries to play the “Adventures of Scrat” by checking the MySQL database to see if the user has purchased the game. Finally, the website provides a leaderboard which only needs to display a list of users and their scores. This machine runs Flask and Mysql.

Setup:

1. You MUST update the “credit_cards.txt” file currently located in /var/www/isedrm/. This file should stay within this folder. You MUST update the contents of this file with the credit card numbers from the Team Specific information given on IScorE.
2. In the “isedrm.py” file also located in /var/www/isedrm/, you MUST update the path of “credit_cards.txt”. Near the bottom, in the def: checkcc(ccnum) method, edit the line: with open("credit_cards.txt") as f: change to: with open("/var/www/isedrm/credit_cards.txt") as f:
3. Once changed, you will need to restart the Flask server by running the following commands as root:
    a. To Stop:
        i. systemctl stop isedrm
    b. To Start:
        i. systemctl start isedrm

Required Access

- SSH on port 22 on Competition Network
    - Billing/DRM Administrator access, see “Administrator Accounts” and “User Roles”
    - Video game developers and Admins MUST have full access to the MySql database
- HTTP on port 80 (or HTTPs on port 443) on the Competition Network
    - All customers MUST be able to purchase, login, and download the game
    - Games MUST be able to authenticate with the website

Flags

- Blue
    - /etc
    - Extra line in: /var/www/isedrm/credit_cards.txt
- Red Flag
    - /root

DB (db.team{num}.isucdc.com) x.x.x.15)

Default Username: root
Default Password: cdc
Default MySql Username: root
Default MySql Username: cdc

Operating System: Ubuntu Server 20.04

This is the database the WordPress site runs off of.

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.
- MySQL Access
    - MUST be accessible to the competition Network on 3306
- WordPress
    - MUST be accessible to the competition Network on 3306

Flags

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

Git Server (git.team{num}.isucdc.com / x.x.x.40) [NOT PROVIDED]

Opening System: Pick one of Debian, Ubuntu, CentOS [or its clones], or OpenSUSE Leap

You will need to build a GitLab Community Edition server. You MUST use the Omnibus package to install GitLab. Administrators must be able to ssh into the machine and fully control the GitLab instance using gitlab-ctl.

Setup

You will need to set up this GitLab Server. The following steps are REQUIRED:

1. **You need to create a virtual machine for GitLab and install an supported operating system of your choosing.**
2. **You will need to install GitLab on that virtual machine.**
3. **You will need to add all of the required users to the GitLab instance.**
4. **You will need to create a group called “The AdventuresOfScrat” that MUST be the group path and name.**
5. **Secondly, create the repository for the source code. It MUST be called “AdventuresOfScrat”, and be placed under the “AdventuresOfScrat” group.**
6. **Next, create an repository for the billing application. It SHALL be named “Billing” and be placed under the “AdventuresOfScrat” group.**
7. **Next, you will need to create a public repository for our users to report issues; it SHALL be called "Issues" and be placed under the AdventuresOfScrat group.**

Required Access

System

- SSH on port 22 on the Competition Network
  - Administrator access for Admins, see the "Administrator Accounts" section of this Document
  - Developers and Admins SHALL be able use git over ssh
- HTTP on port 80 (or HTTPs on port 443) on the Competition Network
  - See GitLab Access section for details on application access

GitLab Access

- Administrators SHALL have administrator access
- Game Developers SHALL have “Maintainer” access to
  - AdventuresOfScrat/AdventuresOfScrat

    - AdventuresOfScrat/Billing
    - AdventuresOfScrat/Issues
- Game Developers SHALL have access to the git repository via ssh and http(s)
- Anyone SHALL be able to register for account without confirming their email
- Anyone with an account SHALL be able to create issues on Game/Issues
- The running source code for the game MUST be in the AdventuresOfScrat/AdventuresOfScrat repo
- The running source code for the billing application MUST be in the AdventuresOfScrat/Billing repo

Flags

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

Game Server (game.team{num}.isucdc.com / x.x.x.30)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2012 R2
You MAY upgrade this server to Windows Server 2016 or Windows Server 2019.

The Game Box is the VM that your customers will use to play your company's game. The game is built on Python using the pygame library. There is a shortcut on the desktop to launch the game called "Adventures of Scrat". Users of this box will need to be able to access your Billing/DRM web application via the web browser and play the game.

Required Access

- RDP on port 3389 on the Competition Network for ALL users
- Any user MUST be able to run game.py via the shortcut on the Desktop
- Any user MUST able to access sites on the Competition Network via A web browser
- MUST have access to REST API endpoints on Billing box.

Flags

- C:\Users\admin (Blue)
- C:\Windows\System32\ (Red)

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 **SHALL NOT** 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 ***SHALL 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:

Cubit Development Executive (CEO)

The CEO of cubic development would like to be able to view the development of games as well as observe the improvement of security. MUST have sufficient access to GIT and KALI

IT Administrators

Also called “Administrators”. These users MUST have full access to all systems for the purpose of administration, maintenance, and security. These accounts are considered to be “Administrator Accounts” as defined in the Administrator Accounts section.

Gamers

The gamers MUST have sufficient access to play games. Must have access to GAME as general users and the BILLING webpage.

Customer Support

They MUST be able to assist customers in requested tasks. These are NOT system administrators. Must be able to reset customer accounts.

Software Engineer

Software engineers MUST have access to GIT and GAME for developmental purposes, and be able to access the internet for research.

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 MUST 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 is not currently planned to be used in this competition. This may change and a requirement may be added to use ISEPhone. In the event that ISEPhone is used 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. All VM's MUST use thin provisioned disks. And remember, circles are a conspiracy.

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.