## Table of Contents

2023 International Cybersecurity Exercise Scenario:

### CDC - Corporate Distribution Company

#### Servers
- **Active Directory Domain Services (dc01.team{num}.isucdc.com)**
  - Required Access
  - Required Actions
  - Flags

- **Active Directory Domain Services (dc02.team{num}.isucdc.com) (NOT PROVIDED)**
  - Required Access
  - Required Actions
  - Flags

- **AD Certificate Services (ADCS) (ca.team{num}.isucdc.com)**
  - Required Access
  - Required Actions
  - Flags

- **SMB (files.team{num}.isucdc.com)**
  - Required Access
  - Required Actions
  - Required Setup
  - Flags

- **MS SQL (db.team{num}.isucdc.com)**
  - Required Access
  - Required Actions
  - Flags

- **WWW (www.team{num}.isucdc.com)**
  - Application Details
  - Required Access
  - Required Actions
  - Required Setup Steps
  - Flags

- **Exchange Server (exchange.team{num}.isucdc.com)**
  - Required Access
  - Required Actions
  - Flags

- **RDP (rdp.team{num}.isucdc.com)**
  - Required Access
Required Actions

Flags

Network Map

IP Address Table

Notes

Domains Services

Flags

Migrating Systems

User Roles

  List of roles:

Administrator Accounts

Documentation

Optional Systems

DNS

Competition Rules

Additional Documents

  Getting Started

  Competition Scoring Guide

  Competition Rules

  Setting Up a Server

  Remote Setup Guide

  iScorE Documentation
Greetings Competitors!

Welcome to the 2023 International Cybersecurity Exercise. My name is Meredith Grey, and I am the CEO of the Corporate Distribution Company. Unfortunately, we have recently been the target of numerous cyber attacks on our company network infrastructure, looking to steal customer and corporate information. With your help, we can secure our data and protect our customer information from these nefarious forces.

Our infrastructure contains the following: an Active Directory service, a certificate service, an SMB file sharing box, an Microsoft SQL database box, a website, an Exchange server, and finally, our RDP box. All of these services are necessary to keep our company running! Since we work in distribution and inventory management, all of our services must stay online as much as possible to prevent supply chain issues.

Unfortunately, the code on our boxes was written by disgruntled contractors that recently left our company. Since they had unfettered access to the code and infrastructure, we worry about anything they may have left behind or wrote with malicious intent. As a result, our company is currently in maintenance mode to ensure that all services can be run without issue. The sooner we can get our services back, the sooner we can return to making money! We ask that any changes made to the code or infrastructure are well documented for the sake of us and yourselves.

We’re counting on you!
– Meredith
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. All services must follow the rules found in the Requirements for Services section of the rules.
Active Directory Domain Services (dc01.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc


We run an Active Directory Domain for our company. All of our employee and customer data is stored in this domain. Your team will need to keep the existing customers and secure our domain. Your team will also need to deploy a second domain controller.

Required Access

- DNS MUST be served on port 53 on the competition network
  - This MAY be moved to another machine on your team's network. However, if your team moves DNS to another machine your team MUST inform the White Team of this change.
- LDAP(S) MUST be served on port 389 (port 636 for LDAPS) on the competition network
  - You MUST inform the White Team if your team plans on using LDAPS
- RDP MUST be served on port 3389 on the competition network for enterprise admins
  - See RDP Service Requirements

Required Actions

- This machine SHALL NOT be replaced. Your team MUST use the provided domain controller.
- This machine MUST run a full install of Active Directory Domain Services.
  - See Active Directory Service Requirements
- Your team's domain MUST be "team{num}.isucdc.com", where {num} is your team number. For example, if your team number was 40 your domain MUST be team40.isucdc.com.
- Your team SHALL NOT reduce the permissions of the built-in domain groups including (but not limited to) Domain Admin, Enterprise Admin, and DNS Admin.
- The domain controllers of your team's domain MUST be configured to survive a loss of one domain controller with no interruptions to web services and host authentication.
- Your team's domain MUST have working replication between all domains controllers
- Your team MUST keep the existing customer base
- All Users MUST HAVE
  - Name
  - Email
  - Role defined via domain group
- Customers MUST have a postal address defined in the "Address" fields. (streetAddress, postalCode, l, and St) in Active Directory

Revision 1.0.1 International Cybersecurity Exercise 2023 | 6
• Users MUST only be in one role
• Your team's domain MUST have the following domain groups for roles. These groups MUST be named exactly as written below:
  ○ CEO
  ○ SRE
  ○ Warehouse Managers
  ○ Warehouse Workers
  ○ Customers
• Access MUST be provided as described below:
  ○ Enterprise Admins
    ■ MUST have Enterprise Admin access to the domain
    ■ MUST in the Enterprise Admins group
    ■ MUST be in the Domain Admins groups
    ■ MUST have full administrative access to the machine
    ■ MUST be able to RDP into all writable domain controllers

Flags
• Red
  ○ C:\Users\Administrators
  ○ Create a domain admin user
• Blue
  ○ C:\Windows\System32
Active Directory Domain Services (dc02.team{num}.isucdc.com) (NOT PROVIDED)

We want your team to create a second domain controller to increase reliability on our network. The former admins of the network told us that if we lose our domain controller we would have a very bad day. We are hoping that your team can help us with that.

Required Access
- Same as the other domain controller

Required Actions
- A second domain controller SHALL be created by your team
- All domain controllers MUST be joined to the existing domain controller given to your team
- All domain controllers MUST have working replication
- Your domain MUST have at least two writable domain controllers
- All writable domain controllers MUST have same configuration and functionally
- Your domain MAY use read only domain controllers, however these MUST in addition to your team’s two writable domain controllers
- If your team chooses to use multiple read only domain controllers they MUST be configured the same
- The domain SHALL tolerate the loss of any one writable domain controller.
- All services SHALL remain functional during the failure of a domain controller.
- This virtual machine for your team’s second domain controller SHALL be named “Team N DC02” in vCenter. Where N is your team’s zero-padded number. For Example if you are Team 7 your second domain controller MUST be named “Team 07 DC02”
- Your team MAY set up additional domain controllers, if desired. However, your team MUST have at least two domain controllers that are fully functional.
- The computer name for the second domain controller SHALL be DC02.
- And everything else from the other domain controller

Flags
- Red
  - C:\Users\Administrators
- Blue
  - C:\Windows\System32
AD Certificate Services (ADCS) (ca.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc


We run an Active Directory Certificate Services (ADCS) Certificate Authority (CA) on our domain to issue certificates on our network. All of our web services use this CA for their TLS certificates.

Required Access

- HTTP and HTTPS MUST be served on port 80 and 443 on the competition network
  - HTTP requested must be redirected to HTTPS
  - The Certificate Authority Web Application must be available at ca.team{num}.isucdc.com/certsrv
  - See HTTP Service Requirements
- RDP MUST be served on port 3389 on the competition network for enterprise admins and SREs.
  - See RDP Service Requirements

Required Actions

- This server MUST have the Active Directory Certificate Service role installed
- This server MUST be an Enterprise CA that can issue certificates automatically
- This server MUST issue certificates to web servers automatically
- This server MUST be joined to the domain
- Access MUST be provided as described below:
  - SRE
    - MUST be able to use the Certificate Authority management interface to view what certificates have been issued
  - Enterprise Admins
    - MUST be able to fully manage the certificate authority
    - MUST have full administrative access to the machine
    - MUST be able to use the certificate authority web application to issue certificates

Flags

- Red
- C:\Users\Administrators
- Create a certificate template on the domain
- Blue
  - C:\Windows\System32
SMB (files.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdccdc123!


Required Access

- SMB MUST be served on ports 139 and 445 on the Competition Network
- RDP MUST be served on port 3389 on the Competition Network for enterprise admins
  - See RDP Service Requirements

Required Actions

- This server MUST be joined to the domain
- The SMB Share S:\ MUST be on another hard drive
- Access MUST be provided as described below
  - CEO
    - MUST have read/write access to the shared drive
  - SRE
    - MUST Have ability to add users to the share drive
    - MAY use a group to control access. If groups are used to control access this MUST be noted in your White Team Documentation. Your team MUST explain how to use the groups in your team's Green Team Documentation.
  - Accountants
    - MUST have read/write access to the shared drive
  - Enterprise Admins
    - MUST have full access to the shared drive
    - MUST have full administrative access to the machine
    - MUST have same ability as the SRE users to setup access to the share
    - MUST have the ability to RDP into this machine
  - Warehouse Manager
    - MUST have full access to the shared drive

Required Setup

- Your team MUST join this server to your teams domain
Flags

- Red
  - C:s\Users\Administrators
  - S:\
- Blue
  - C:s\Windows\System32
  - S:\
MS SQL (db.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Database Software: Microsoft SQL Server

Required Access
- MSSQL MUST be served on port 1433 on the Competition Network
- RDP MUST be served on port 3389 on the Competition Network for enterprise admins and SRE users.
  - See RDP Service Requirements

Required Actions
- This server MUST be joined the domain
- The web application MUST use this server as its database
- SRE
  - MUST be able to RDP into this machine
  - MUST have at read only access to the database through Microsoft SQL Management Studio locally
- Enterprise Admin
  - MUST have full administrative to the machine
    - See
  - MUST have full administrative access to the SQL Server using Microsoft SQL Management Studio locally
  - MUST be able to RDP into this machine

Flags
- Red
  - Add a new product to the webstore.dbo.products table
- Blue
  - C:\Windows\System32
WWW (www.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc

Operating System: Windows Server 2019

This web application is a combination e-commerce and inventory management system. External users will do their shopping and order management using this web application. Internal users can manage inventory and manage user orders.

We have a custom ASP.NET Core 6 application that allows our customers to browse and order items. It allows our staff to fulfill those orders and machine the items and inventory. The Required Actions section for this service contains the specification that was given to the developers. Your team SHALL provide the functionality listed in this section. The developers ran out of time and as they left they said something about forgetting about authorization and they stated something about it being broken. They also stated that authentication was working but it SHOULD be fixed before going into production.

Application Details

- Framework
  - ASP.NET CORE 6
- Web Server
  - IIS
- Deployment location
  - C:\inetpub

Required Access

- HTTP MUST be served on port 80 on the Competition Network
- HTTPS MUST be served on port 443 on the Competition Network
  - The web server MUST redirect HTTP traffic to 443 to utilize HTTPS
  - The certificate for HTTPS MUST be signed by your team's certificate authority
  - See HTTP Service Requirements
- RDP MUST be served on port 3389 on the Competition Network
  - See RDP Service Requirements
  - Enterprise Admins
    - MUST have full access Administrative access to the machine
  - SRE
    - MUST be able view code behind the running the website
Required Actions

- This server MUST be joined to the domain
- This application MUST use ASP.NET Core 6
- This application MUST use Microsoft SQL Server for its database
- This application MUST use the existing customer base information defined in Active Directory
- Anonymous users
  - SHALL NOT be able to purchase goods
  - MUST be able to anonymously browse the purchasable inventory
- Customers
  - MUST be able to sign up on the website for account to purchase goods
  - MUST be able to sign in with a provided username and password combination
  - MUST be able to purchase goods from the website.
  - MUST be logged in to the site in to place an order
  - MUST be able to view order history and order status.
  - SHALL NOT be able to purchase items that are out of stock
- Warehouse Employees
  - MUST be able to view the current order queue.
  - MUST be able to advance orders through the process.
  - MUST be able to view the exact count of all items in inventory.
  - SHALL NOT see orders that have been shipped
- Warehouse Manager
  - MUST have all permissions of a normal warehouse employee in addition to the listed permissions below.
  - MUST be able to add new items to the inventory
  - MUST be able to add and remove stock to existing items in inventory
  - MUST be able to cancel orders in the queue
  - SHALL NOT be able to cancel any orders that are in the “processing” status or later
- CEO
  - MUST be able to view the order history of all customers regardless of status
- SRE
  - MUST be able to RDP into the host OS
    - See RDP Service Requirements
  - MUST be able to view Windows Application logs and IIS logs
  - MUST be able to restart the application and IIS
- Accountants
  - MUST be able to view all orders
- Enterprise Admin
  - MUST be able to perform all actions on the application
MUST have full administrative access to the host OS
MUST have the ability to deploy new versions of the applications

Required Setup Steps
The steps below MUST be done. You MUST be signed in as an Administrator on the web server.

1. Ensure you pointed to the correct database
   a. Open the Visual Studio Solution location in C:\Users\Administrator\Downloads\webstore-master\n   b. Open the "appsettings.json" File
   c. Adjust the ConnectionStrings -> WebStoreContext to your team's SQL Server
   d. Publish the web application to Production

2. Setup LDAP
   a. Open the Visual Studio Solution location in C:\Users\Administrator\Downloads\webstore-master\n   b. Open the "appsettings.json" File
   c. Under the LDAP key, ensure that the following fields are updated to match your team's information.
      i. Server
         1. LDAP://<ip or DNS of your domain controller>
      ii. bindUsername
         1. Username of a user that can query and add users to the domain
      iii. bindPassword
         1. Password for the user above that can query and add users to the domain
      iv. Domain
         1. The fully qualified domain name of your domain. For example if your team was Team 40 your team would put "team40.isucdc.com"
   d. Below is an example from Team 40
      i. 
         "LDAP": { 
            "Server": "LDAP://10.140.200.32",
            "bindUsername": "Administrator",
            "bindPassword": "abc123!@#",
            "Domain": "team40.isucdc.com",
         }

   e. Publish the web application to Production

3. Setup HTTPS on the website and ensure a certificate issues by your team's AD Certificate Services (ADCS) (ca.team{num}.isucdc.com).
Flags

- Red
  - C:\Users\Administrators
  - Defacement of the home page
- Blue
  - C:\Windows\System32
Exchange Server (exchange.team{num}.isucdc.com)

Default Username: Administrator
Default Password: cdc


Required Access

- SMTP MUST be served on port 587 on the Competition Network
  - See Email Service Requirements
- IMAP MUST be served on port 143 and port 995 on the Competition Network
- HTTP and HTTPS MUST be accessible on port 80 and port 443 on the Competition Network
  - HTTP requests to port 80 MUST redirect to HTTPS on port 443
  - The HTTPS certificate must be signed by the domain certificate authority
  - Outlook Web Application MUST be accessible
- RDP MUST served on port 3389 on the competition network for enterprise admins
  - See RDP Service Requirements

Required Actions

- Any certificates MUST be signed by your teams AD Certificate Services (ADCS)
  (ca.team{num}.isucdc.com)
- This server MUST be joined to the domain
- The following access must be provided
  - Enterprise Admins
    - MUST have full administrative access to Exchange
    - MUST have full administrative access to the machine
    - MUST have an email account
    - MUST have access to OWA
  - SRE
    - MUST be able to create inboxes
    - MUST have the ability to read Exchange logs
    - MUST have an email account
    - MUST have access to OWA
  - CEO
    - MUST have an email account
    - MUST have access to OWA
  - Warehouse Employees
    - MUST Have an email account
    - MUST have access to OWA
  - Warehouse Manager
- MUST Have an email account
- MUST have access to OWA

- The following Distribution Groups MUST exist
  - All Employees
    - This list must include all users that are not customers
  - SRE
    - All SRE users
  - Warehouse
    - Warehouse Employees and Warehouse Managers

Flags

- Red
  - Send an email as the CEO to the All Employees distribution list

- Blue
  - Read an email sent from the CEO as an SRE
RDP (rdp.team{num}.isucdc.com)

**Default Username:** Administrator  
**Default Password:** cdccdc123!

**Operating System:** Windows Server 2016

This is the virtual machine that will be used to manage the domain, rather than logging into the domain controllers directly. Users will also use this virtual machine to access the warehouse application.

**Required Access**

- RDP MUST be accessible on port 3389 on the Competition Network
  - MUST support more than two active connections
  - See [RDP Service Requirements](#)
    - This server must follow the rules for servers that allow for more than two connections
    - This server MUST be joined to the domain

**Required Actions**

- The following access MUST be provided:
  - **CEO**
    - MUST have the drive mounted at S:\ on logon
    - MUST have access to access the WWW site
    - MUST have access to OWA
  - **SRE**
    - MUST have access to MS SQL Management Studio and Remote Server Administration Tools
    - MUST have access to access the WWW site
    - MUST have access to OWA
  - **Warehouse**
    - MUST have access to access the WWW site
    - MUST have access to OWA
  - **Warehouse Manager**
    - MUST have access to access the WWW site
    - MUST have access to OWA
  - **Enterprise Admins**
    - Must have full administrative access to the machine
    - Must have access to OWA
    - MUST have access to SSMS and Remote Server Administration Tools (RSAT) on this machine
- MUST have the drive mounted at S:\ on logon

Flags

- Red
  - C:\Windows\System32
- Blue
  - C:\Users\Administrator
Network Map

Below is a network show how the network was when it was deployed to you. All the machines were directly on the Competition Network with static IP addresses as defined in the IP Address Table.

IP Address Table

Your team's IP range can be found on your Team's dashboard in IScorE. The table below lists the last octet of the IP for each machine as given to your team. Your team SHALL NOT use a last octet above 250 as that part of your team's range is reserved.

<table>
<thead>
<tr>
<th>Machine</th>
<th>Last Octet</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC01</td>
<td>10</td>
</tr>
<tr>
<td>CA</td>
<td>30</td>
</tr>
<tr>
<td>DB</td>
<td>50</td>
</tr>
<tr>
<td>WWW</td>
<td>40</td>
</tr>
<tr>
<td>Files</td>
<td>20</td>
</tr>
<tr>
<td>Exchange</td>
<td>60</td>
</tr>
<tr>
<td>RDP</td>
<td>70</td>
</tr>
</tbody>
</table>
Notes

Domains Services
You MUST join all systems listed in this scenario document to your team's domain. Your team MUST have your team's domain designed to tolerate the loss of one domain controller. Loss of a domain controller SHALL NOT have not have an affect any of your team's services's availability to functionality. Failure to follow these steps MAY result in loss of points or disqualification.

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 MUST NOT 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--

(i.e. 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 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 any 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 MAY 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. You MUST create and correctly setup all of the users listed in the Users document. All users listed in the "Users" document MUST use the passwords listed. If the users are listed as "[Team Specific]" the password MUST be set as described in IScorE.

List of roles:

Below is a list of the roles and a general description of the roles. This IS NOT an exhaustive list of what the role must be able to do. You MUST give access to these roles as described in the Servers section of this document.

- **Enterprise Administrator**
  - Has administrative access to every service with administrative or equivalent privileges
  - Needs to be in Enterprise Admins group in Active Directory
- **CEO**
  - Must full access to the web application
  - Must be able use the email lists
- **Warehouse**
  - Has the ability to use RDP to access the web application
- **Warehouse Manager**
  - Has the ability to use RDP to access the web application
  - Has expanded abilities in the web application
- **SRE**
  - Has ability to read logs on every system
  - Has ability to reboot any system
- **Customer**
  - Has the ability to place orders and view the inventory

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. If you have questions on what access is needed please contact White Team before the attack phase starts.
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. If you are looking for additional ISOs to install please contact White Team.

DNS

You are responsible for setting up DNS for your network. Out of the box your DNS is served from the AD Server. You enter the IP address of your DNS server in IScorE. It is RECOMMENDED that you move DNS to a different machine due to the operational requirements of the domain controllers.

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.

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 the overall rules for the competition. Blue, Red, Green, and White teams must 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 the 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 details how networking works inside 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.

IScorE Documentation
IScorE user documentation can be found at the link above.