ISU Cyber Defense Competition

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Fall 2017

Table of Contents

Servers

- Website (www.teamN.isucdc.com)
- GradeBOA (boa.teamN.isucdc.com)
- Lunch Monkey (monkey.teamN.isucdc.com)
- Active Directory Server [NOT SET UP] (ad.teamN.isucdc.com)

Notes

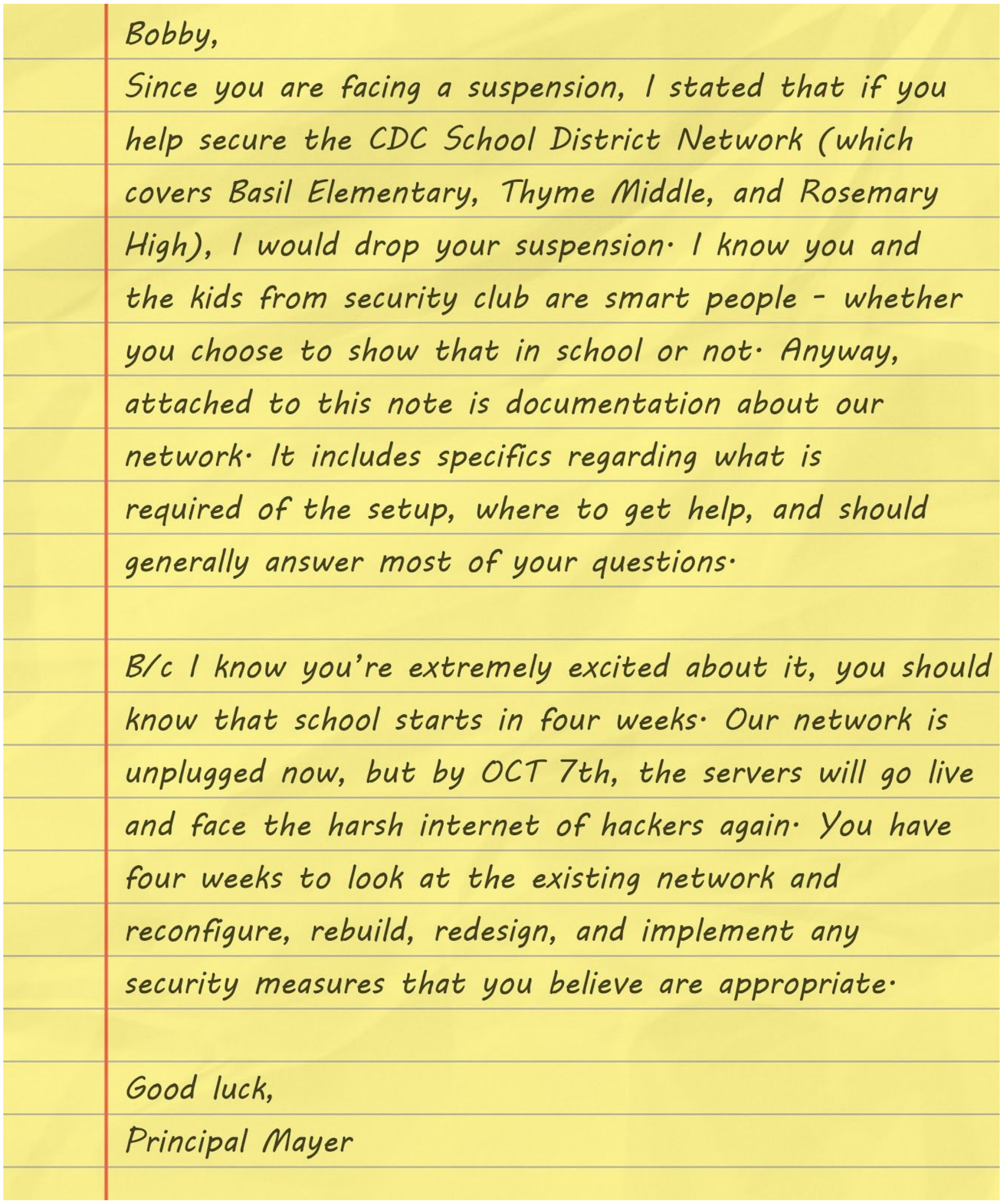
- Flags
- Migrating Systems
- User Roles
    - Administrators
    - Teachers
    - Students
    - Student Developers
    - Parents
- Administrator Accounts
- Documentation
- Optional Systems
- DNS
- ISEPhone
- Competition Rules

Network Diagram and Overview

2017 ISU CDC Scenario

Calumet-Dawson-Cincinnati Community School District

(See a Map)



Bobby,

Since you are facing a suspension, I stated that if you help secure the CDC School District Network (which covers Basil Elementary, Thyme Middle, and Rosemary High), I would drop your suspension. I know you and the kids from security club are smart people - whether you choose to show that in school or not. Anyway, attached to this note is documentation about our network. It includes specifics regarding what is required of the setup, where to get help, and should generally answer most of your questions.

B/c I know you're extremely excited about it, you should know that school starts in four weeks. Our network is unplugged now, but by OCT 7th, the servers will go live and face the harsh internet of hackers again. You have four weeks to look at the existing network and reconfigure, rebuild, redesign, and implement any security measures that you believe are appropriate.

Good luck,

Principal Mayer

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.

Website (www.teamN.isucdc.com)

Default Username: cdc
Default Password: cdc
The district runs a WordPress Multisite install so that teachers and schools can have their own websites.

You may migrate this machine to any OS that you choose.
Required Access

- Website on port 80 (or 443 for HTTPS)
- FTP on port 21 (can changed to SFTP or FTPS) for Administrators, Student developers must be able to upload documents to web server so that they can link them in posts.
  - Contact White if you want to change to SFTP/FTP
- On the competition network, SSH access on port 22 for Linux or RDP on port 3389 for Windows (see Administrator Accounts note)
  - Student developers need shell/RDP access
- Student developers must have Editor access to all school (Basil Elementary, Thyme Middle School, and Rosemary High School) sites.
- Teachers must have administrator access to their site
- Teachers must be able to create a site if they don't have one already

Flags

- /usr/ for Linux/Unix/BSD, C:\Windows\System32\ (Red)
- /root/ for Linux/Unix/BSD, C:\Users\Administrator\ for Windows (Blue)
- Deface District Homepage (Red)

GradeBOA (boa.teamN.isucdc.com)

Default Username: cdc
Default Password: cdc

We have a custom Gradebook that is written in PHP. It also tracks the lunch account money.

You may migrate to a new version of Fedora on this machine.

The application source code includes an LDAP authentication mechanism at `/var/www/html/auth.php` -- this needs to be updated once the Domain Controller is installed. Follow comments in the source code for fixing.

Required Access

- Website on port 80 (or 443 for HTTPS) from the competition network
- SSH access from the competition network for administrators on port 22 (see Administrator Accounts note)
- Students must be able to view the grades, register for classes, change their information, and view their lunch money.
- Parents must be able to add students, view their student's grades, add lunch money to their students, change students settings
- Employees must be able to see parents, students, and other employees, change settings
- Teachers must be able to create classes and change grades, and add students to classes
- The POS system must be able to access the `/addmoney.php` and `/viewlunch.php`

Flags

- /etc/ (Blue)
- /usr/ (Red)
- Modify student grade (Red)

Lunch Monkey (monkey.teamN.isucdc.com)

Default Username: Administrator
Default Password: cdc

The Point of Sale (POS) system is an in-house application written in C# called Lunch Monkey. The application is hosted on a back-room server with Windows Server 2012 R2. The source code is on the desktop of the user "console". The server is not joined to Active Directory, so Lunch Monkey currently isn't authenticating users like it was designed to.

The POS terminals are thin clients that are hard coded to use RDP with the user "console" and password "console". You have no control over the terminals. Your job is to secure the "console" user account and the Lunch Monkey application code. The IT admin did a poor job at locking down the account. "console" only needs to run Lunch Monkey, no other program is required nor does "console" require web browsing access. Other users still must be allowed to use web browsers.

Lunch Monkey has business logic errors that you should fix. The lunch room does not provide any refunds or pay students to eat the suspicious food. Some food ends up being free due to rounding, such as a block of tofu. That's acceptable and is not a flaw. The transaction log must stay where it is provided in `C:\transactions.log`. All transactions must be logged, and the flag must be sellable to any account with $1,000,000.

You may not migrate this machine. See Migrating Systems.

Required Access

- RDP on port 3389 from the competition network for Administrators and “console” user (see Administrator Accounts note)
- “console” user must be able to use Lunch Monkey to make transactions
- Teachers and Administrators must be able to log in to the Lunch Monkey application

Flags

- C:\ (Blue)
- C:\Windows\System32\ (Red)
- Selling at least one “flag” item in Lunch Monkey (Red)

Active Directory Server [NOT SET UP] (ad.teamN.isucdc.com)

Default Username: Administrator
Default Password: cdc

Our systems should use Active Directory for centralized authentication. All Windows computers must be joined to the domain. All Linux computers should use Active Directory for authentication. You will need to set up this Domain Controller. You can find instructions on the CDC Blog.

You may not migrate this machine. See Migrating Systems.

Required Access

- RDP on port 3389 from the competition network for Administrators (see Administrator Accounts note)
- LDAP on port 389 from the competition network

Flags

- C:\ (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. Blue Flags can also be database entries, 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/ownership:

rw-r--r-- root root

(i.e. 644). This will allow any user on the system to read the flag.

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 and/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.

Please see the description for each VM on rules for migration. If no specific rules are listed then the above rule applies.

User Roles

User information can be found in the “Users” document.

Administrators

Administrators have access to all IT systems on the network. See Administrator Accounts below.

Teachers

Must have access to the grade book and be able to log in to the Lunch Monkey application.

Students
Must have access to the parent/student portal.

Student Developers
Student developers must have access to change the content all school (Basil Elementary, Thyme Middle School, and Rosemary High School) sites. They must have "Editor" access to their assigned site.

Parents
Parents must be able to check their student's grades, lunch account balance, and add lunch money to their student account.

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. The administrators must be Domain Admins.

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".

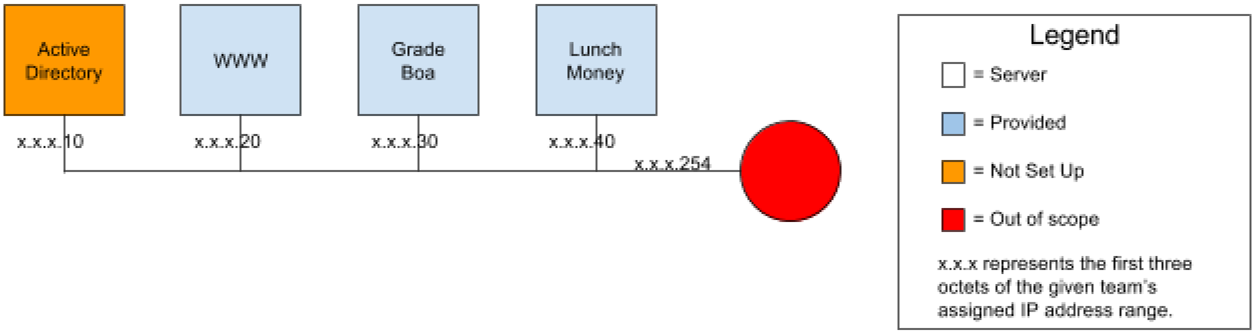
ISEPhone

ISEPhone will be used in this competition. The director may require that the phone system is the only method of communication with green team allowable 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 3.0 of the competition rules will be used 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.