

## IOWA STATE UNIVERSITY, INFORMATION ASSURANCE STUDENT GROUP ASSOCIATION HIGH SCHOOL CYBER DEFENSE COMPETITION SCENARIO, SUMMER 2007

The CDC Data Corporation (CDC) is a small dot-com startup in Metropolitan, Iowa. A building has just been leased and twenty-five employees are ready to go to work on their mission of creating organized databases out of old written records or mismanaged data files for their clients. The actual database work will be delegated to the employees working on the projects (on their personal machines), but a secure network that will be able to meet regulations regarding the security of CDC's client data must be designed.

As the Information Assurance team for CDC, your team has been assigned the task of designing a secure network that will hold up to attack and keep client information secure. Your team is only responsible for the servers and a “kiosk” machine available to all employees in the break room. Therefore you are not responsible for the database servers. Employees will be responsible for the setup of their own machines as most are tech savvy (given the nature of CDC). There are many issues to be addressed with this setup as flexibility and usability are of the utmost importance but the security of client data cannot be sacrificed in the process. This data may be in the form of data files on a central file server, emails to or from CDC employees, or it may be available for review on CDC's web server.

No specific software requirements have been outlined for your team but it is expected that whatever software is used does not violate any copyright law or licensing agreement. Two of the executives cannot agree on an Operating System for CDC, so as a compromise, you will be required to use both Windows and a Unix (i.e., a Linux or a BSD) in your design. This said, any implementation is acceptable as long as it provides the following:

### Web Server

An outside web development team has been contracted to design CDC's site ([www.cdcN.com](http://www.cdcN.com)) and will provide your team with the content and the server once the business opens on **START DATE**. Management of DNS will need to be handled by your team. Your name server is already registered with a registrar as **ns.cdcN.com**, but you will need to provide the IP address of this machine to the registrar (White Team) at least a week before CDC opens for business. (*Note: N is the number of your team.*)

### Email Server

You will provide accounts for CDC employees. You should protect against spam and viruses. A list of users will be provided. Additionally, DNS MX configuration of [cdcN.com](http://cdcN.com) is needed so that mail is directed to the mail server. Users should be able to check email from both inside and outside the corporate network using IMAP and webmail. The IMAP connection must be unencrypted so email traffic can be monitored for data leaks. You may implement a secure login method to protect the password, if you wish. The IMAP server should be accessible at **mail.cdcN.com** and webmail should be at **www.cdcN.com/webmail**. User accounts should be of the format **USERNAME@cdcN.com**.

### File Server

Each user should have a home directory and there should be a common “scratch space” for any user to upload data to share with other CDC employees. There should also be a public FTP server for clients to download their data once its processed and uploaded by CDC engineers. Users should be able to log in to their home directories with the same credentials that they use to access their email. CDC users must be able to upload data to the FTP folder (maybe not via FTP), but clients must have access to download their data from outside of your network using FTP.

### Programming Environment

Users have requested to have a remotely accessible programming environment accessible to them for testing. Users should be able to log in to this service via SSH to **ssh.cdcN.com**, with the same credentials used for the email server and compile C/C++ programs using GCC.

The new building is not accessible to you until the CDC is open for business. Due to this fact, all setup will be done remotely. Equipment will be set up as you request and remote KVMs and power relays will be made available.