FALL 2006: CYBER DEFENSE COMPETITION SCENARIO

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 Unix (Linux, BSD, et cetera) in your design. This said, any implementation is acceptable as long as it provides the following items:

Web Server

An outside web development team has been contracted to design CDC's site (www.cdcN.com) and will provide your team with the content and the server once the business opens on November 3rd. Proper management of DNS will need to handled by your team. Your name servers are already registered with a registrar as ns-1.cdcN.com and ns-2.cdcN.com. You will need to provide the IP address(es) of this(these) machine(s) to the registrar (White Team). Note: N is the number of your team.

Email Server

This service will provide accounts for the staff with spam filtering and virus protection. A list of users will be provided. Additionally, configuration of cdcN.com is needed so that mail is directed to the appropriate server. Users should be able to check email from both inside and outside the corporate network using IMAP and web mail (POP is not required, but may ease things down the road). The IMAP and web mail connections can be secure (i.e., SSL), but this is not a requirement. The IMAP server should be accessible via imap.cdcN.com and web mail should be webmail.cdcN.com. If POP is used, it should be pop.cdcN.com. User accounts should be of the format USER@cdcN.com.

File Server

Each user should have a home directory and there should be a common "scratch space" for any user to temporarily upload data to for sharing purposes. Users should be able to access files from both inside and outside of the local network. Users should be able to log in to this service with the same credentials that they use to access their email.

Remotely Accessible 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 with the same credentials that they use for the email server and file server and compile C/C++ programs using GCC.

The use of a firewall is strongly encouraged, but it must be able to come down (allow all traffic) with fifteen minutes notice to allow testing of the internal network by an external security certification authority. To allow for this, no Network Address Translation will be allowed. All machines must be addressed with a publicly routable IP from the set provided by the Internet Service Provider (White Team).

On Wednesday, November 1st at noon, two days prior to the CDC's grand opening, the facility will be closed to employees until the evening of Friday, November 3rd. No local or remote access will be allowed.