# IT-ADVENTURES: CYBER DEFENSE COMPETITION

## Scenario

**IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER**

SPRING 2010

The CDC Data Corporation (CDC) is a small dot-com startup in Metropolitan, Iowa. It is a hosting company with small sites across the country. This way, clients can have a way to store their company's information securely “in the cloud”. CDC provides web, mail, and file services to clients. These sites are regularly tested for security by the CDC corporate red team.

You are in charge of setting up an environment for a new CDC client. As such, your team has been assigned the task of designing a secure network that will hold up to attack and keep client information secure. You must maintain servers for the advertised services (more detail below), and be able to guarantee the security of the data. There are many issues to be addressed. Flexibility and usability are of the utmost importance, but the security of client data cannot be sacrificed.

Your DNS will be handled by CDC corporate. As such, you must use the IP addresses assigned for each service, shown below. You will be given a list of user names and passwords that must be implemented on every advertised service. You cannot change these passwords unless approval is given by CDC corporate.

Your network must provide the following services:

### Web Server (www.siteN.cdc.com - 50)

An outside team was contracted to compile your client's web data into a single server and will provide your team with this server once you begin setting up your network. You *may not* alter any web content or applications on this machine. Doing so is equivalent to taking the web server offline. Your team should instead focus on implementing global security measures (Apache configuration, PHP configuration, ModSecurity, etc) that will protect your web server from any malicious or badly-written client code, and making sure all of the software is up-to-date. This server is running encrypted HTTP (HTTPS), with a certificate signed by CDC corporate. You may assume your clients have been provided the necessary information to trust this certificate. This server must be in your subnet, number 50. For example if your subnet is 5.5.5.0/24, this machine should be 5.5.5.50.

### Mail Server (mail.siteN.cdc.com - 100)

Clients need to be able to access their email via encrypted IMAP (IMAP/S), with a certificate signed by CDC corporate. You may assume your clients have been provided the necessary information to trust this certificate. This server must also accept incoming SMTP, and be able to connect out to the internet with SMTP (for incoming and outgoing email). This server must be in your subnet, number 100.

### File Server (file.siteN.cdc.com - 150)

You must make a server accessible to your clients to store sensitive data. They should be able to SSH into this server to manage their files, or use SCP to do so remotely. SCP is simply a file transfer, similar to FTP, that uses SSH as its transport protocol (similar to how HTTPS is just HTTP encrypted with SSL). This server must be in your subnet, number 150.

### Firewall

Your team has been provided with a pfSense firewall appliance that already has the rules required to forward traffic to the web server. However, it is not set up with the correct external IP address. You will need to verify that this is set up securely, and add the necessary rules for the mail and file servers. Remember that your firewall must properly map each of the IP addresses above to the correct server, so it will need IP address aliases on its external interface. Requests for DNS zone changes will not be honored.

All setup will be done remotely. Hardware has been provided to meet the requirements of the client and you have been given no budget by CDC corporate for upgrades. The day before your site goes online, you will have a twelve hour window to put the finishing touches on your network before clients begin using your services, and the corporate Red Team is allowed to begin testing.

Corporate, for auditing purposes, requires that your network be documented; and for public relations, that you have a guide available for your client on how to use your services. Both of these documents must be provided to CDC Corporate [the White Team] prior to your site coming online. See the Rules document for details.