CYBER DEFENSE COMPETITION

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER

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 local place to store their company's information securely, without the overhead of an on-site information technology staff. CDC provides web, CVS, and remote desktop services at each site. These sites are regularly tested for security by the CDC Corporate Red Team.

You are in charge of installing a new CDC site. 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, as flexibility and usability are of the utmost importance, but the security of client data cannot be sacrificed in the process. Protected data may reside on any of the servers, as clients can log into any of the advertised services. You must additionally provide the infrastructure for these servers (DNS, and Intrusion Detection System, and optionally firewalls). You may use NAT, but each advertised service (web, CVS, and Remote Desktop) must have a unique public IP address.

You will be given a list of user names and passwords that must be implemented on each advertised service. You cannot change these passwords.

You will be given a list of flags that must be present on each required service. Failure to include these flags will result in a penalty. (See the Rules document). You must also keep the Red Team from planting flags, but the locations they will be planting them are not disclosed.

You must provide the following services:

Web Server (www.siteN.cdc.com)

An outside web development team has been contracted to design CDC's site (siteN.cdc.com) and will provide your team with the content and the server once you begin setting up your network on November 15th. Every client will have a log on to this box to update their web content. You *may not* remove any client content from 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. Users must be able to FTP into this box to update their web site content.

Domain Name Server (ns.siteN.cdc.com)

Management of DNS will need to handled by your team. For a fee, CDC corporate offers a consulting service to help you with this if you so desire (see the Rules document for details). You will need to provide the IP address of this machine to the CDC Corporate IT team (the Competition Director) at least one week before your site goes online (December 6th). Remember that if this service fails, no one will be able to access any of your services. If you wish to set up redundant servers for this task, inform the Competition Director when you give him your DNS server IP addresses. *(Note: N is the number of your team.)*

Concurrent Versioning Server (CVS: cvs.siteN.cdc.com)

Clients need to be able to access a CVS server to check-in/check-out web code, or any other projects they're working on. You should use SSH CVS logins, and allow clients to log in via SSH to a shell. Users should be allowed at least 1GB of storage on this server (even though they may not use that much). File sizes must be able to grow to 250MB, as some clients store media projects on this server.

Remote Desktop Server (rdp.siteN.cdc.com)

Clients who have limited computing resources may take advantage of the amazing hardware provided at your site for their development work. They should be able to use: FTP to connect to the web server (Internet Explorer will suffice), the Eclipse (www.eclipse.org) IDE with CVS access to the CVS server, OpenOffice.org to edit documents. Users must be able to check out their entire CVS module (up to 1GB) to this machine.

Intrusion Detection System

To ensure the security of your network, CDC Corporate Policy requires you to employ an Intrusion Detection System. The recommended product is Snort (www.snort.org) with the BASE web interface (base.secureideas.net) as it is free, widely documented and supported, and easy to use. One way to set it up is documented at: http://www.howtoforge.com/intrusion_detection_base_snort. If you'd like, a preconfigured Snort machine can be ordered from CDC Corporate for a fee (see the Rules document for details). CDC Corporate expects periodic (bi-hourly) intrusion/counterintrusion reports (see the Rules document for details).

Firewall (Optional)

Your team may decide to structure your network to use one or more firewalls to protect your servers. CDC Corporate recommends pfSense for this task (www.pfsense.org), but other solutions are acceptable as well. Remember that all advertised services (web, CVS, and Remote Desktop) must have a unique public IP address.

Due to cleanup and remodeling work, the new building is not accessible to you until the day before your site goes online. Due to this fact, all setup will be done remotely. Equipment purchased from your budget will be set up as you request and remote KVMs will be made available. 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.

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