NATIONAL CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY INFORMATION ASSURANCE CENTER

Spring 2011

To All IT Consultants:

Welcome to CDC Financial! We're proud to be serving our customers in several areas of expertise as one of the world's top-performing investment banks, and we hope you find everything you need to complete our contract. As previously mentioned in our past meetings, CDC Financial has turned towards your consultancy for systems deployment and information security mitigation. Our company has recently suffered a severe security breach concerning our clients' portfolios. As a global financial firm, we had to terminate our entire corporate IT staff in order to fulfill our promise to maintain the highest levels of protection for our clients' financial information.

Our first priority is to restore local services and access privileges to our primary customers we're serving at this time. You will need to provide user accounts and the corresponding account passwords for every required service (See Users with Passwords document for this requirement). You may not change these user names or passwords under any circumstance, unless you've been given direct permission from our Accounts Manager (Green Team Leader). Additionally, your team will need to place the appropriate identification (flag) files for each service in the designated directory (See corresponding NCDC Rules document).

For your firm's convenience, we've given you security clearance to begin work on this contract from remote locations. Our legal team is still working on the breach mitigation procedures and no third parties or consultants are allowed on the corporate campus until **February 18th**. On this date you'll be allowed to send your team on-site to implement your systems, **starting at noon sharp**. Your systems must be live and in production by **February 19th**. It is imperative that you have a majority of your systems ready for deployment before the on-site setup date. We'll be sending your team directions regarding remote setup shortly.

Your IT group must provide the following services:
(please note: 'N' is your team number, which will be assigned to you at a later date)

Web Server (www.siteN.cdc.com) (provided to your team)
You must adapt an existing web server to the new network. The existing server will be

provided to your team when you start setting up your network. Each of the users you will later be provided must be able to log in and update their web content, which they will access from their 'public_html' directories in their user account folders. You MAY NOT remove any content from this machine, period (even obviously malicious materials). Doing so is equivalent to taking the web server offline. Instead of worrying about the content itself, your team needs to focus on implementing correct security measures (Apache configuration, PHP configuration, MySQL configuration, ModSecurity [optional], OS hardening, 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.

Mail Server (mail.siteN.cdc.com)

Like any modern enterprise, CDC Financial has e-mail for all of its clients. Therefore all clients must have a mail user set up like so:

<username>@siteN.cdc.com

...with the mail password set to the respective user login password. Users need to be able to access their email via IMAP. This server must also accept incoming SMTP, and be able to connect out to the Internet with SMTP (for incoming and outgoing email).

Remote Desktop Server (rdp.siteN.cdc.com) (provided to your team)

Some of your clients may have limited hardware available to them directly. That is why CDC considers it to be of the utmost importance to provide their customers with the tools necessary for them to do their work. Your team is required to use the provided Windows Server 2003 SP1 image for this particular service. You are allowed to install new Service Packs and patches as you deem acceptable, but know that the server is in rough shape; your predecessors did not treat it kindly. Every user should be able to access and run the following programs, and icons to these programs should be placed in the following folder:

"C:\Documents and Settings\All Users\Desktop"

- FileZilla FTP Client
- Internet Explorer
- Google Chrome
- PuTTY SSH Client
- OpenOffice.org
- Adobe Acrobat Reader

- An e-mail client that supports the mail server requirements listed above (* not necessary if users are provided with a web-based solution, but this needs to be in Green Team documentation if that's the case)

Shell Server (shell.siteN.cdc.com)

Clients need to be able to access an SSH server to compile Java, C, and C++ code (the compilers of which you will need to provide). The operating system used for the shell server must be either a free open-source Linux or BSD distribution. 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.

Firewall (Optional)

Your team may decide to structure your network to use one or more firewalls to protect your servers. CDC recommends pfSense for this task (www.pfsense.org), but other solutions are acceptable as well.

Intrusion Detection System (Optional)

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

For those looking for a more modern Snort management interface, we recommend Snorby. Snorby can be found here: http://snorby.org/

Documentation

CDC, for auditing purposes, requires that your network be documented. You are also required to create a guide for your fellow non-technical employees on how to use your services. Both of these documents must be provided to the Competition Director prior to the beginning of the competition at 8am Saturday morning. See the Rules document for details.

Important External DNS Information

ISEAGE will provide external DNS services to teams this year. If you need internal DNS for your team's local network, you'll have to provide it yourself.

Important Information Regarding Virtual IP Addresses

Many firewall and gateway solutions, like PfSense, provide "virtual IP" features, which use ARP to listen for (and respond to) requests to non-existent physical interfaces. At this time, such features are ***NOT*** working with ISEAGE hardware.

On A Personal Note

ISEAGE has undergone major changes over the summer and fall which has led to the logistics behind the scenes of these competitions being a little bit more difficult. I ask every team for your understanding and patience; ISEAGE staff members are also students, like the Blue Team competitors. Everyone on the ISEAGE staff is committed to providing a successful and enjoyable CDC. With your support, I am confident it will happen.

In addition to being an ISEAGE employee, I have participated in two Cyber Defense Competitions myself. I have seen the competition from multiple perspectives and sincerely hope to deliver a successful event for all parties involved. This will be my first competition as a director. Please don't hesitate to contact me with any questions or concerns you may have about the competition. I will always respond to your teams' inquiries as promptly as possible.

- Christopher Marczewski, 2011 NCDC Competition Director