COMMUNITY COLLEGE CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY INFORMATION ASSURANCE CENTER
Fall 2010

Welcome to our company!

On behalf of all employees, welcome to the Coalition of Digital Comrades (CDC)! We've had a lot of issues with our past IT personnel, and sadly had to finally let them go. Your group will be creating a new IT infrastructure for our company from the ground up (with few small exceptions). We demand great performance, consistent service availability, and above all else, unwavering security. Our company needs to run many different services, all of which are below.

You will be given a list of user names and passwords that must be implemented on each service. You cannot change these passwords nor delete any user, unless instructed by the personnel manager (Green Team Leader). You will also be given 'flags' that must be present on each required service at a later time. Failure to include these flags will result in a penalty. (See the Rules document for details).

Due to remodeling, the IT facility will be closed until the day before you must go live (weird coincidence, eh?). Therefore the coalition has demanded that all work be done remotely until that time. Your team will be allowed to begin work shortly, and your on-site setup will open on December 3rd. You MUST be live by 8am on December 4th! We'll send directions regarding remote setup when the date approaches.

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 your 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], 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 has e-mail for all of its employees. Therefore all employees 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)
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. As such, you will be using the coalition existing remote desktop server and adapting it to the new network. 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 (or equivalent web browser)
- PuTTY SSH Client
- OpenOffice.org
- An e-mail client (* 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) (provided to your team)
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). 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.

Directory Server (directory.siteN.cdc.com)
Stressing unwavering security you need to provide authentication for each employee. Keeping each employee responsible for their actions on your network is a must! Where ever an employee is required to login, they need to provide creditable credentials. This is required for Mail, RDP, and Shell Servers. Each employee knows the policies and need to abide by them. Your team has the option to use any authentication you see fit. Directory must reply to requests for information and authentication from both outside and inside your fireall.

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

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, whom hosts these competitions, 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 for understanding and patience; do remember that ISEAGE staff are also students like yourselves. Everyone on the ISEAGE staff is committed to providing a successful CDC, with your support I am confident it will happen.

Participating in two ISU CDCs, IT Adventures and being an ISEAGE employee, I have seen the competition from multiple perspectives and opted to put a personal spin on this fall's competition. This will be my first competition as director. That being said I am overwhelmed, anxious, but most of all, excited. I want to see how everyone enjoys these changes. I believe a change now and again is nice to keep everyone engaged and allow them to broaden their horizons.

- Patrick Turvin, Competition Director