IT-OLYMPICS CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
SPRING 2013

Thank you for coming on board at Can Do Company! We are a growing IT contracting company based in Ames, Iowa. We contract out various IT work for any size of client; from setting up a new server to designing and implementing corporate networks, we "Can Do" it! My name is Roger, and I am the Director of Information Technology at Can Do Company. As the Director of IT, it is my top priority to ensure our consultants and other staff have all the resources and services they need, and not a moment after they need them.

We recently went through some financial hardships due to the recession and had to file for Chapter 11 bankruptcy. During this time we had to lay off most of our IT staff and consequently lost the ability to run some important production machines. We are very excited to get our feet under us again in all respects, and hiring your team to rebuild IT is a big step in that direction.

As part of the rebuild, we will need to stand up a remote desktop server, email server, and backup solution. All of these systems were lost during the transition period and will need to be re-done from scratch. I'm leaving this up to your team; specifics are detailed below.

The remaining systems, our web and shell servers, are still online and working. However, they have not been updated since our layoffs and may be vulnerable to some newer attacks. I am concerned that there may have been some intrusions because of this, so please make sure to give the servers a good look-through and plug any holes that the intruders may have placed.

The rest of this document outlines the requirements for each of our services and policies. Please read it carefully, as we need everything to work according to these specific requirements!

Good luck!

Roger

Your network must provide the following services:

Web Server (www.siteN.cdc.com) [Provided]

This server runs our corporate website. You may not delete 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, safe implementation of CGI, etc) that will protect your web server from any malicious or badly-written client code. It will also benefit you to make sure all of the software on your server is up-to-date.

All existing features are working properly on the server you have been provided, but may not be very secure. All features and functions must remain operational or you will be penalized by the green team.

- Apache should provide www.siteN.cdc.com on port 80
- Must provide FTP access for all users to their home directories on port 21
- Users must be allowed to create home pages in /home/user/public_html that are accessible from http://www.siteN.cdc.com/~username (this is already configured for currently existing users).
- Administrators (ben and nolan) must have access to the Quarterly Financials on the wiki (reminder: this is a flag). No other users require access to the Quarterly Financials.
- Data on this web server MUST be backed up every hour (during the attack phase) to your dedicated Backup server. At least 8 hours worth of data must be maintained.
- Can be re-installed, patched, reconfigured – whatever you need to do to make it work securely, however the core OS must remain some flavor of Linux!
- Many teams will consider installing a whole new Linux operating system from scratch and migrating the content over from the old system. This may be effective for advanced teams, but is not recommended unless you know how complicated it will be to try. If your team chooses to migrate, the data on the wiki must be preserved.

Shell Server (shell.siteN.cdc.com) [Provided]

Some of our employees are part time developers. They need to be able to access an SSH and SFTP server to compile code. 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 users need to store large amounts of data on this system. Users should be able to have at least 25 processes. This server must be in your subnet, but you can choose the IP address it uses (just like all your other services). In order to test to make sure that compilation works properly on the shell box, we will provide (at a later time) a set of files and test scripts that Blue Teams can use to verify their boxes are properly configured. During the Green Team usability checks, these scripts and files or slightly modified ones will be used.

- SSH/SFTP should be running on standard port 22
- SSH/SFTP should be offered via the DNS name shell.siteN.cdc.com
- Users must be able to compile and execute C, C++, Java, and Python code
- Administrators (ben and nolan) must be able to use sudo to run commands as root
- User files must be backed up

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

You will need to provide a full desktop experience on an RDP server for our employees. They will be using their own computers to access it, and we don't know how powerful they will be. You'll need to make sure that users can do everyday tasks such as browse the internet, write documents, check e-mail, etc.

Your team is required to use Windows Server (available in the ISO Datastore). Any version is allowed. Every user should be able to access and run the following programs, and icons to these programs should be included on all users' desktops:

(Note: ISEAGE staff recommend you use the website http://ninite.com to automate the installation of several of these programs.)

- FileZilla FTP Client
- Mozilla Firefox
- PuTTY SSH Client
- LibreOffice
- Adobe Acrobat Reader
- Internet Explorer
- An e-mail client that works with your mail server (a web based solution is also acceptable, but you must note this in your green team documentation)
- Must be compatible with rdesktop running on Linux

E-mail Server (mail.siteN.cdc.com)

Our team needs to be able to send emails and attachments to each other, as well as to users of other teams. You'll need to provide an email server to serve IMAP, POP3, and STMP traffic. You may use any operating system and email server you like.

- All clients must have a mail user set up like so: <username>@siteN.cdc.com
- The inbox password should set to the respective user login password.
- Users need to be able to access their email via IMAP and POP3. This server must also accept incoming SMTP messages, and be able to connect out to other CDC sites via SMTP (for example, bob@site1.cdc.com should be able to send to dan@site2.cdc.com).
- You may provide webmail access if desired for ease-of-use (which will likely benefit your green team score), but you will still be required to provide IMAP, POP3, and SMTP services too.

A Backup Solution (Does NOT need to be publicly accessible!)

This will be your team's primary backup. The following data must be backed up:

- Website content and data, including anything in users' home directories and MySQL databases.
- User data on the shell server.
- User data on the RDP server.
- Emails and attachments from the email server.

DNS [Provided]

For this competition ISEAGE will handle the hosting of all DNS services. **It is your responsibility to inform us what IP addresses your servers will be using before the competition using the IScorE system (more information on IScorE will be provided at a later date).** For example, 64.5.53.200 → www.site9.cdc.com.

Firewall [Optional]

Your team may decide to use a firewall to protect your servers. White Team recommends pfSense (www.pfsense.org) for this task because we are familiar with it and can provide you with basic assistance if needed. However, other solutions are acceptable as well if you would prefer to use them. If this is your first time at a CDC we would encourage you to instead use a software-based firewall on your boxes until you get on your feet (that is, not have a dedicated firewall box). Software-based firewalls are included for free in Linux and Windows, and are very easy to set up and use. If you think you're up for the challenge of a dedicated firewall we'll gladly help you make that leap, but we just want to be sure you start on solid ground.

Remote Setup

All setup will be done remotely (see the Remote Setup document). Hardware has been provided to meet the requirements of a basic network design, and our budget is currently limited, so you will need to ensure you distribute your limited computing resources (see the CDC Rules document). The day before we go online, you will have setup time to put the finishing touches on the network before the services go live for the world to access (Friday, April 26th). The site must be online and ready for the attack phase by 8:00am on Saturday, April 27th!

Member Expulsion Procedure

Unfortunately, we occasionally have unruly members. To prevent a member from discovering that he/she is being ejected, accounts cannot be disabled until a member is notified of his/her expulsion. However, once a member is expelled, his/her accounts must be immediately disabled. This will prevent any type of retaliation or intellectual property theft caused by a disgruntled former employee.

The Green Team Leader will notify your team (Blue Team) of a pending termination with a scheduled time (via an Anomaly). The member accounts must be terminated within 5 minutes of the scheduled time, but NO SOONER. For example, if you are told at 2:00pm to disable an account at 3:15pm you are required to have that account totally disabled on all services by 3:20pm, but not even a minute before 3:15pm, lest you tip off the expelled individual.

We recommend either implementing an automated system to handle member expulsion, or a well documented process of ensuring that an account can be disabled on all systems within 5 minutes. Please be sure to detail how you are approaching this problem in your White Team Documentation.

Shell Server Test Scripts

In order to test to make sure that code compilation (C, C++, Java) works properly on the shell server we will provide (at a later time) a set of files and test scripts that Blue Teams can use to verify their boxes are properly configured. During the Green Team usability checks these scripts and files (or slightly modified ones) will be used to verify that your services are operating as expected.

Concluding Thoughts

Hi, I'm Max Peterson, this year's CDC director. I've been an ISEAGE employee since March 2011, and I've participated in multiple Cyber Defense Competitions over the last six years. I have helped with many IT-Olympics competitions, but this will be my first time as director. I hope you are excited for the competition as I am!

I hope to bring another successful event for students, advisers, and volunteers alike this April. Please don't hesitate to contact me with any questions or concerns you may have about the competition. Have fun, and we wish everyone the best of luck!

- Max Peterson, IT-Olympics 2013 Director