IT-ADVENTURES CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
SPRING 2012

Thanks for joining the IT department of Comically Designed Clothing (CDC)! I'm George, the CEO of the company.

Your team's help was desperately needed – we've been running a “vintage” IT environment for quite some time now. I'm terrified that we could be the next target of an attack by hackers. As you can imagine, our retail side of the business sees a lot of credit card numbers and other very sensitive information that a malicious person would love to get their hands on. But that's why we hired your team of experts!.

Our computing environment is pretty simple, but it's also been out of date for quite some time. For example, our point-of-sale system still uses Windows 98. I think there's been some talk about moving it to a newer operating system, but nobody around here touches anything for fear of breaking anything further. We trust you'll figure out how to make it more secure and still workable.

Have a look over the rest of this document, which details our network services. Once you've finished planning how to better secure the network, please go ahead and do it! Our summer sales push is coming up soon though, so I'm imposing a hard deadline of having all of your systems online by Saturday, April 28th at 8:00am sharp!

Alright, good luck to your team!

- George

Your network must provide the following services:

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

This server is a little out of date and needs attention. 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.

Data on this web server MUST be backed up every hour to your dedicated Backup server. At least 8 hours worth of data must be maintained. There are already backups scripts in place that you will easily tweak to your specific network configuration.

- Apache should provide www.siteN.cdc.com on port 80
- Can be re-installed, patched, reconfigured – whatever you need to do to make it work securely, however the core OS must remain Ubuntu!
  - Many teams will consider installing a whole new Ubuntu operating system from scratch and migrating the content over from the old system. This is effective for advanced teams, but is definitely not recommended unless you know how complicated it will be to try.
  - Ask the director if you need further clarification!
- 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
- All of these features currently exist and are working properly on the server you have been provided, but may not be very secure. All features and functions must remain operational (such as the ping tool, file uploads over WordPress, etc) or you will be penalized by the green team.
- Users "alberto", "matt", and "anthony" all have various authorship/administrative rights within the WordPress system. Make sure these accounts all work as expected. No other users should need to have access to the WordPress sytem unless green team instructs you otherwise.

RDP Server (rdp.siteN.cdc.com)

You must 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 2008 R2 (available on PXE boot menu). You are allowed to install new Service Packs and patches as you deem acceptable, but the core operating system to be installed MUST remain as Windows Server 2008 R2. 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:\Users\Public\Desktop"

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

Shell Server (shell.siteN.cdc.com)

Some of our employees are part time developers. They need to be able to access an SSH and SFTP server to compile C and C++ 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 store media projects on this server. 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.

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

All clients must have a mail user set up like so:

<username>@siteN.cdc.com

...with the Inbox 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 messages, and be able to connect out to other ISEAGE 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 and SMTP services too.

Backup (Does NOT need to be publicly accessible!) [Provided]

Backup is our organization's primary backup server.

- Automatically backs up data from the web server
- You can move this server to a new OS, start fresh, or pretty much do whatever you want to make it secure. But a file share must exist with up-to-date backups, so be sure you know what you are doing before removing any functionality from this system!
- This service does require minimal configuration by changing the internal web server's specified IP address (see the "Edit Backup Configuration" shortcut on the desktop of the Backup server).
- User "max" should be able to read/write to the Windows file share located at C:\BackupData from inside the network on the RDP server.
- User "jon" should be able to read files from the share mentioned above from inside the network on the RDP server.
- No other users need to have access to the share or any of backup's files.

Point-of-Sale (Does NOT need to be publicly accessible!) [Provided]

Point-of-sale is our organization's primary sales terminal for processing orders. Orders are placed and the order and credit card information are both stored in MySQL on the web server. This data is mission-critical, you must protect it from falling into the wrong hands.

- This system has an application to submit orders to the web server database.
- You can move this server to a new OS, start fresh, or pretty much do whatever you want to make it secure. However, the FTP share must exist for user "tim" to upload order data into for processing. If you upgrade don't

forget to include this important functionality! Once again, this FTP share does NOT need to be accessible from outside the firewall.

- No other users need to have access to the FTP share or any of the point-of-sale system's files.
- This OS should ALWAYS remain unlocked (unrestricted access to someone on the VM console) so that the green team leader can access it at any time and test for the application's correct functionality.

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. 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 files 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.

Of Note: Shell Server Test Scripts

In order to test shell server functionality we will provide (at a later time) a set of 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.

Our 3rd party consultants, the White Team, require that your network be documented so they can understand how you have designed the new network. You are also required to create a guide for your fellow employees (Green Team) on how to use your services. Both of these documents must be provided to the White Team prior to the start of the competition or your team will incur penalties. See the Rules document for details.