IT-ADVENTURES: CYBER DEFENSE COMPETITION

Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
SPRING 2011

The Cereal Deliciousness Corporation (CDC) is a small breakfast cereal producer in Ames, Iowa. CDC has been in business for many, many years, and was a very early adopter of computers and IT in the 1990s. Sadly, the company's IT infrastructure has fallen into complete disrepair in recent years. Because of their poor performance, CDC's CEO 'Captain' Ned Crunch has fired all of the former IT staff and has hired your team to replace them. CDC knows that a lot of it's current IT system needs a little attention, some of it is pretty outdated!

To make matters even worse, Captain Crunch's high-school nemesis, Ray S. N. Bran, has opened a competing breakfast cereal company based in Antarctica. Ray will stop at nothing to break into your systems to get to your company's secret recipes for your best-selling cereal, *Chucky Larms* ('flags', see Rules document); ***you must prevent his minions from stealing our secret recipes!***

Your team has been assigned to maintain servers for the advertised services listed below, and be able to guarantee the security of the data. There are many issues to be addressed. Flexibility and usability are of the utmost importance, but the security of our precious corporate data cannot be sacrificed.

Your DNS will be handled by the White Team, a 3rd party IT consulting service. Because of this, you'll need to make sure you let the White Team know what IP you have assigned for each service shown below. You will be given a list of user names and passwords that must be implemented on every advertised service. You cannot change these passwords unless you are told to do so by our user experience team leader (we call him 'Green Team Leader' because of his love of green t-shirts).

Your network must provide the following services:

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

This server is a little out of date and needs a little attention. You *may not* alter 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, ModSecurity, etc) that will protect your web server from any malicious or badly-written client code, and making sure all of the software is up-to-date. This server must be in your subnet, but you can choose the IP address it uses. For example if your subnet is 5.5.5.0/24, this machine should be 5.5.5.N

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

Your team is required to use Windows Server 2003 this particular service. You are allowed to install extra software, Service Packs, and patches as you deem acceptable. This server must be in your subnet, but you can choose the IP address it uses. Every user should be able to access and run the following programs, and icons to these programs should be placed in the "C:\Documents and Settings\All Users\Desktop" folder:

- FileZilla FTP Client
- Firefox 3.0
- PuTTY SSH Client
- WinSCP
- LibreOffice
- Adobe Acrobat Reader

Shell Server (file.siteN.cdc.com) [PROVIDED]

Clients need to be able to access an SSH and SFTP server to compile C and C++ code (using the GCC compiler). 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. This server must be in your subnet, but you can choose the IP address it uses.

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.

All setup will be done remotely. Hardware has been provided to meet the requirements of a basic network design, and you have been given no budget by CDC corporate for upgrades. The day before your site goes online, you will have a twelve hour window to put the finishing touches on your network before your services go live for the world to access.

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 non-technical employees 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.