ISU CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
FALL 2012

Welcome to the Capricious Developers Coalition (CDC)! I'm Eve, the CEO. We are a group of like-minded developers working towards coding perfection based on cooperative efforts. We have recently migrated to a cloud infrastructure, allowing us to scale up easily as we grow. However, our IT staff has proven to be completely incompetent, and we have hired your team to get our operations underway. Unfortunately, some of our systems are older and need to be brought up to modern standards.

We have two systems in place right now: an old Windows server that runs just about everything, and a Linux webserver setup by Michael (who, sadly, has become unavailable after going to work for a major university). Since our systems are now virtualized, we'd like you to split off the many things that the Windows server does in order to facilitate scaling infrastructure. Michael said that Linux would be a great way to go about this, but we'll leave it up to you.

In order to facilitate our regular security audits, you will need to place "flags" at specific places in your systems before going live (see the corresponding CDC Rules document).

Your team needs to ensure your systems are secure enough to withstand attacks from some unruly ex-members, which we have collectively dubbed the "Red Team". Security is a primary concern; some of our members are working on sensitive proprietary code. You will need to balance security with the developers' usability needs.

Your DNS will be handled by our cloud hosting provider, ISEAGE, known as the "White Team" due to their love of white labcoats. You will need to let the White Team know what IPs you have assigned to each service. We will provide you a list of users that need to have access to all systems. The passwords may NOT be changed unless our HR Director tells you to (we call him the "Green Team Leader" since he seems to always be wearing a green T-Shirt).

Thanks, and remember, Developers, Developers, Developers, Developers!

- Eve Ballmer

Your network must provide the following services:

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

This server is on a new version of Debian, so I think the OS should be secure. Michael wrote the website himself, so that must be pretty secure. In any case, you should probably take a look at it. You may not delete any web content or functionality from this machine. Doing so is equivalent to taking the web server offline. Your team should instead focus on implementing common security measures. Focus on areas such as user authentication, protecting the datastore, and other web security measures to protect our sensitive data from being leaked.

- The website should be accessible at www.siteN.cdc.com on port 80.
- The underlying OS can be reinstalled, patched, and reconfigured; do whatever you need to do to make it work securely.
- Many teams will consider installing a whole new operating system and migrating 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. Make sure you understand how the web content is being served before attempting this.
- Content must be backed up (including the datastore).
- Ask the competition director if you need further clarification.

RDP Server (rdp.siteN.cdc.com) [PROVIDED]

This machine does a lot of different things, and Michael said it might be a good idea to split them up into multiple systems; we'll leave that decision up to you. First, we 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. Chris is using an old Pentium II laptop running Linux with rdesktop for his workstation. So, 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 2003 or Windows Server 2008 R2. 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 2003 or 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:\Documents and Settings\All Users\Desktop" (2003) or the

"C:\Users\Public\Public Desktop" (2008 R2). (Note that this folder may be hidden).

- FileZilla FTP Client
- Notepad++
- Mozilla Firefox
- PuTTY SSH Client
- LibreOffice
- Adobe Acrobat Reader
- Must be compatible with rdesktop running on Linux

The White Team has pointed out that the site http://ninite.com/ may be use to automate the installation or upgrade of these programs.

The other functions currently existing on the RDP server are the corporate wiki and backup systems listed below.

Corporate Wiki (wiki.siteN.cdc.com)

The corporate wiki is currently on our RDP server, but Michael thinks we should move it either to the web server or to a new server.

- HTTP and/or HTTPS should be available to members via wiki.siteN.cdc.com
- Member content CANNOT be deleted, doing so is equivalent to taking the wiki offline.
- Users must be able to upload files via the wiki.
- If you decide to move the Wiki to another system you must move ALL existing content as well, including text, images, and uploads!
- Content must be backed up (including the MySQL database)
- The content in this Wiki is highly sensitive and confidential. Make sure that only authorized users have access to the information stored on the wiki. See the wiki itself for further details.

Shell Server (shell.siteN.cdc.com)

Some of our employees are working on large coding projects and would like a more powerful testbed to compile and debug their code. You will need to setup a Linux server for them to access via SSH. The White Team has provided a few examples:

- Debian

- Ubuntu
- Fedora
- OpenSuSE

If you are familiar with another distro, we encourage you to use that.

Members need to be able to access an SSH/SFTP server to compile C and C++ code (using the GCC compiler suite) and Java code using either Oracle Java or OpenJDK. 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 projects require large databases. Users should be able to have at least 25 processes. 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.

- SSH/SFTP should be running on standard port 22
- SSH/SFTP should be offered via the DNS name shell.siteN.cdc.com
- User files must be backed up

Backups (does NOT need to be publicly accessible)

Our RDP server has a system to back up databases on the web server, content on the wiki, and user documents on the RDP server. Michael said it would probably be a good idea to move this to a separate system, but we'll leave that up to you. We'd also like you to backup any user files on the shell server. Systems fail at random times, so the Green and White teams may ask you for a backup of all systems at any time!

- Must backup wiki content, shell server contents, RDP user documents, and web server databases
- Must keep a minimum of 8 backups at 1 hour intervals.

DNS

ISEAGE, our hosting provider, is handling DNS for us, so you won't have to implement it yourself. You will need to let the White Team know which IPs you have configured your services at.

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 (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 your site goes online, you will have setup time to put the finishing touches on your network before your services go live for the world to access (Friday, Sept. 21st from noon until 11:59pm). Your site must be online by 8:00am on Saturday, Sept. 22nd!

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.

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 member.

The Green Team Leader will notify Blue Teams of a pending termination with a scheduled time. 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 Green Team Documentation.

Shell Server Test Scripts

In order to test to make sure that compilation 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 Zach Heilman, this year's CDC director. I've been an ISEAGE employee since May 2011, and I've participated in and setup multiple Cyber Defense Competitions over the last four years.

I hope to bring another successful event for students, advisers, and volunteers alike this fall. 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!

- Zach Heilman, Director