COMMUNITY COLLEGE CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
FALL 2012

Computer Discount Center (CDC) welcomes you and your team! My name is Oscar, assistant to President. Our goal is to provide the best custom-assembled computers to each and every customer. The President wants to grow the company by way of eCommerce. In preparation for the influx of orders we have recently virtualized our existing systems. This will allow us to grow in to the future. However, we have learned our IT staff of one is not enough to complete the next step in the allotted time. I have brought your team aboard to move our company on to the final stretch. I do warn you our IT staff was not able to do anything outside of just virtualizing our systems. We still do incorporate legacy systems that should be brought up to standards.

We have two standing system as of now: An out of date Windows Server that is the entry to our intranet and more, and a Linux web server that has been setup by a previous IT employee (Matt) who is no longer with us. I would like to see the new virtualization software used fully. Feel free to split off services from existing systems on to their own VMs, if you feel you can do it securely and without breaking their functionality. The current IT staff have knowledge of Windows, Linux, and Unix, but their strength is in Linux. Do remember that after your stay is done, the current IT will be in charge of management and maintenance.

Being understanding of increased security concerns we would like to increase our current security audits. To make sure key information is being secured, we would like for you to place “flags” at designated locations with in the systems. This will allow our audits to confirm the strength of your security implementations.

These new security implementations you are enabling should be strong enough to withstand attacks from even the most skilled internet “hackers” along with any internal would-be “spy”. We like to refer to them as the “Red Team”. While security should be at the forefront of your agenda, do not forget we have employees who do work from home or from the road. You should not put to much extra burden on them, in the name of security.

Our DNS is provided by our ISP, ISEAGE, we refer to them as the “White Team” due to that they are the most trust worth people we know, and they handle all back end work so we don't have too. You will have to contact the White Team with the IPs you have assigned to each service.

To assure that we have not left any employee out the transition we will provide a list of users. These users need access to all systems. It is the middle of the fiscal year and we do not want to make users re-create their passwords. We will include their passwords along side their user names. Passwords may NOT be changed without authorization from the HR manager (We call him the “Green Team Leader”, since everything in his office and his attire is green).

On behalf of everyone at Computer Discount Center (CDC), I thank you! With your help we are able to grow our company to new horizons.

- Oscar Rodriguez

Your network must provide the following services:

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

This server is on a new version of Fedora, so the OS should be secure. Matt wrote the website himself, and says it should be "totally secure", but you should verify that. It is important that our eCommerce system isn't be hacked. No web content or functionality may be removed from this machine. Doing so is equivalent to taking the web server offline. Your team should focus on implementing common security measures. Focus on areas such as user authentication, protecting the confidential information (especially credit card numbers!), 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.
- Content must be backed up (including any databases).
- FTP uploads should be kept in the users' public_html directories and accessible from siteN.cdc.com/~<username>
- Ask the competition director if you need further clarification.

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

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. One employee 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 is the wiki and backup system listed below.

Corporate Wiki (wiki.siteN.cdc.com)

The corporate wiki is currently on our RDP server, I would look in to moving it to a new server.

- HTTP 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.
- The wiki we have provided is run on MediaWiki, but it can be run on any wiki software of your choice.
- 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) to the backup server during the competition.
- 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 new/existing coding projects for the web server or general systems 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.

Employees 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. Look in to the notion of moving 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 ISP, 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 they 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 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, Nov. 30th from noon until 11:59pm). The site must be online by 8:00am on Saturday, Dec. 1st!

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 employee.

The Green Team Leader will notify your team (Blue Team) 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

Hello, everyone! This year I am the CDC director, Patrick Turvin. I welcome back all returning participants. For new participants, I have been the Community College CDC director for the past two years, this will be my third. I have been a part of 11 CDCs in total. I am currently an employee of the ISEAGE research group here at ISU. I also graduated from Kirkwood Community College, so I know what it's like be a participant on that level.

I strive to bring another successful competition to each of the students, advisers, and volunteers. If you have and questions or concerns don't hesitate to contact me. Enjoy yourself, and have fun. Good look to everyone!

- Patrick Turvin, Director