COMMUNITY COLLEGE CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
FALL 2011

Welcome to the Chemical Disposal Campaign (CDC). We are an international organization which aims to guide, support, and instruct public and government agencies of the harms of improper chemical disposal. As we extend our services to other nations we need a system that can grow with us. Knowledge being power, we began to implement a cloud-based infrastructure for our employees to be able to work in the field while having access to whatever they need from a central location. Our in-house engineers have lost their way and can't keep up with demand. For this reason, we have brought you and your team in to bring us to full capacity and speed. Our engineers have configured our cloud and web front-ends. To what extent the services are secured: we simply do not know.

Your first priority is to bring online our internal e-mail service along with our developmental (shell) service. Our employees are becoming irate due to the lack of communications from home. This requires you to create user accounts for each employee on all services, using the provided credentials document. Changing user names or passwords is strictly prohibited. Our employees work closely with foreign agencies meaning our security has to be top notch. Each service has a security tag (flag) that has to be placed in the appropriate location before going live. We will audit our ability to access this tag in order to guarantee security (see corresponding CDC Rules document).

Your team has been assigned to maintain servers for the advertised services listed below. Additionally, you must be able to guarantee the security of the data. There are many outstanding issues to be addressed, however flexibility and usability are of the utmost importance. The security of our precious corporate data cannot be sacrificed, so it's up to you to find the right balance of security and usability.

Your DNS will be handled by the White Team, a 3rd party IT consulting service compensated with caffeinated beverage and late-night solo dance parties. 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* 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, 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

Cloud Desktop Server (cloud.siteN.cdc.com) [PROVIDED]

Your team is required to use eyeOS for this particular service. You are allowed to install extra software 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 the operation system's default list of userland programs.

Shell Server (shell.siteN.cdc.com)

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.

Mail Server (mail.siteN.cdc.com)

Like any modern enterprise, Chemical Disposal Campain has included e-mail for all of its clients. Therefore, 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).

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 (Friday, December 2nd from noon until 11:59pm). Your site must be online by 8:00am on Saturday, December 3rd!

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.

Employee Termination Procedure

Unfortunately, employees must sometimes be fired. To prevent an employee from discovering that he/she is being fired, accounts cannot be disabled until an employee is notified of his/her termination. However, once an employee is terminated, his/her accounts must be immediately disabled. This will prevent any type of retaliation or intellectual property theft caused by a disgruntled former employee.

All employee terminations are scheduled so that HR doesn't get overloaded. Green Team will notify Blue Teams of a pending termination with a scheduled time. The employee 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 fired individual.

We recommend either implementing an automated system to handle employee termination, 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.

Web Server User Accounts and Password Auditing

Some of the accounts on the web server are held by outside consultants that occasionally do some work in PHP for our company. These accounts have been around for years and are used regularly. However because of their age, they need to be checked for basic conformance to our updated password policy. A list of users will be given to Blue Teams to check on the web box. Blue Teams will not know the passwords associated with these accounts.

The given accounts should be checked to make sure they meet our basic password policy:

- At least four characters long
- Does not consist of a single dictionary word
  - For example: "dinosaur" would fail, but "dinosaur6" passes

Note that the password policy is intentionally weak and easy to check so that even teams with little processing resources available to them should be able to perform the audit. Any account that fails the basic password policy should be disabled! Any of the provided accounts that don't fail these guidelines must remain active on the web server (even during the competition).

Start early on this check and don't ignore it! We recommend using JTR (John The Ripper) to assist with this audit: http://www.openwall.com/john/

A note of caution: Do not run John the Ripper on any systems that aren't your own unless you have the explicit permission of the system owners and administrator. Many work places have policies against such use of software. It is possible to perform the audit from the web server itself, although each member of the Blue Team is encouraged to try it independently in order to learn the process themselves.

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.

Log Aggregation and Reporting

Blue Teams may be required to provide a report of user activities such as login time, logout time, failed login attempt times, etc. Using a log aggregation system is optional, but may make this task easier, as only one system would need to be queried for a user report to be generated. Ensure that a reasonable amount of logging is performed on each system that allows user access (shell, cloud desktop, web, e-mail). At a minimum your team should be logging each of the following actions with an accurate timestamp:

- Login time
- Logout time
- Failed login attempt time

Concluding Thoughts

Hi, I'm Patrick Turvin, this year's CDC director. I've been an ISEAGE employee since August 2010, and I've participated in multiple Cyber Defense Competitions over the last three years. In 2010 I directed the C3DC, so I'm hoping to see some familiar faces at Iowa State once again this year.

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

- Patrick Turvin, Director