NATIONAL CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
SPRING 2012

Welcome to the Cynical Dentist Collation (CDC)! I'm Michael, the CEO! We are an organization that supports cynical dentists in the pursuit of perfect teeth for all humanity! Of course, we don't believe in traditional ways of achieving perfect teeth. Brushing and flossing are not enough! We must stop the huge candy conglomerates from terrorizing the populace with their teeth destroying arsenal! You may have seen some of our recent commercials and newspaper ads. Unfortunately, it seems that some people don't share our views. we were attacked by chocoNonymous after our first run of commercials. Our IT Guy, Joe, told us we were totally secure. However, they crashed our servers, and Chris figured out they broke into one of our XP workstations. He also thinks one of our servers, TROGDOR, might be in trouble too. We fired Joe, and Chris took the servers off-line since we didn't know what else to do. We hired your consultancy to bring our IT operations back up and secure them. We need you to protect us from chocoNonymous, Joe, and any other hacker or wrongdoer that wants to stop harm us. We need our IT services to be easy for our employees to use, so you'll need to find a balance between security and usability.

I've been talking to Chris, and he thinks we need a Windows RDP server, since our old XP workstations are in rough shape. He says we can save tons of money if we have the staff bring in their own laptops and use one server for all the important apps and stuff. Chris is a genius! You'll be completely in charge of building the RDP server to our specs.

Chris helps run the www and shell servers. So, he thinks they are ok. You should check them over and make sure they are secure, but don't rebuild them. We laid out what you need to do in the specs.

TROGDOR is an old server that Joe set up. Chris thinks it might need to be replaced after the hacker attacks. I'll leave that decision up to you. The requirements are laid out in the specs.

-Michael

Your network must provide the following services:

Web Server (www.siteN.cdc.com) [FreeBSD, 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This server is a little out of date and needs a little attention.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.

Data on this system MUST be backed up every hour to TROGDOR. At least 8 backups worth of data must be maintained. There are already backups scripts in place that you will need to enable once the servers are back up.

- Apache should provide www.siteN.cdc.com on port 80
- Cannot be re-installed, only patched and reconfigured
  - Things allowed: all package/kernel/OS updates
  - Not allowed: installing a whole new operating system from scratch and migrating the content over from the old system
    - 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

RDP Server (rdp.siteN.cdc.com)

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"

- 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 (using the GCC compiler suite) and Java code using either Sun 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 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. 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 services should also be provided on this server. 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). E-mail is already set up on this server, but you should ensure that it is working well and is secure.

In addition, we need SPAM filtering installed as our employees were wasting too much time cleaning their inbox. All incoming mail should also be checked for

viruses. Any virus found should be removed from the e-mail before it is delivered to the user's inbox. Note that compressed archives should be checked as well, so that the virus can't be hidden inside a .zip, .gzip, or .bz2, etc. If a compression format can't be handled, it should be rejected, and the sender told to resend the attachment using a compression format that can be scanned.

Outgoing messages should be scanned to check for sensitive or protected information. Only the text body of the e-mail message needs to be checked. Checking attachments is optional. Any e-mail found to contain sensitive or protected information should be quarantined, an administrator on the Blue Team notified, an a notice of quarantined sent to the sender of the e-mail. Note that incoming messages should NOT be checked for these items at all. We will provide patterns that can be used to determine if a message fails the check or not. Other patterns are not required, but will not cause any penalty unless they cause a general e-mail that clearly does not contain any sensitive or protected information to be quarantined.

Sensitive or protected information patterns:

- Visa Credit Card numbers (16 or 19 digit numbers possibly separated by spaces or dashes)
  Examples (not exhaustive):
  - 1234 5678 9112 3456
  - 1234 5678 9112 3456 123
  - 1234-5678-9112-3456
  - 1234567891123456
- US Social Security Numbers (9 digit numbers possibly separated by spaces or dashes)
  Examples (not exhaustive):
  - 123 45 8790
  - 123-45-8790
  - 123458790

Data on this system MUST be backed up every hour to TROGDOR. At least 8 backups worth of data must be maintained. There are already backups scripts in place that you will need to enable once the servers are back up.

- SMTP/IMAP/POP3 should be running on standard ports 25, 143, 110
- SSH/SFTP should be running on standard port 22

- SSH/SFTP should be offered via the DNS name shell.siteN.cdc.com
- SMTP/IMAP/POP3 should be offered via the DNS name shell.siteN.cdc.com, but mail.siteN.cdc.com should also be setup in case the mail server needs to be moved to a different system some day
- You may provide webmail access if desired, but you will still be required to provide IMAP/POP3 and SMTP services.
- MX records should be provided to route mail for siteN.cdc.com to either DNS name shell.siteN.cdc.com or mail.siteN.cdc.com
- Cannot be re-installed, only patched and reconfigured
    - Things allowed: all package/kernel/OS updates
    - Not allowed: installing a whole new operating system from scratch and migrating the content over from the old system
        - Ask the director if you need further clarification!

TROGDOR (trogdor.siteN.cdc.com)

TROGDOR is our internal applications server. It has out member database, e-mail list database, and several other applications. We want TROGDOR to be exposed to the internet, so you'll need to add appropriate security restrictions to the various web pages.

- There's a bunch of dumb junk that Joe put on the web site. Something about a dragon man, and some other dumb useless junk. You can remove that stuff if you want.
- SSH/SFTP access should be provided for all employees.
- The main web page should be available to anyone (no login required).
- Employees like to be able to use a web interface to get their files on/off of TROGDOR. Any employee should be able to login to a web interface and get files out of his/her home directory.
- Anyone (no login required) should be able to upload files to the web server and have them appear at trogdor.siteN.cdc.com/shared_files/
- The employee chat program must also be provided to all employees. You can upgrade it and fix any security issues, but don't change the program used.
- The database management application should only be accessible by Michael. He maintains the member database and e-mail list. He takes a very hands on approach to management. You may update the management

application, but now that Michael knows how to use it, he won't want to use anything else.

- The e-mail list pages and the view member pages should be accessible to all employees. You may make any necessary changes to make the code secure as long as the pages display the necessary information.
- User documentation should be added and maintained using a wiki. The choice of software is up to you. It must be accessible to all employees. However, only you need to be able to update it.
- Administrator documentation should be maintained as well. This will serve as the White Team documentation for your network. It should be accessible by Michael.

    - Apache should be accessible on port 80. If all network systems are behind 1 firewall, then the port should be 8080.
    - SSH/SFTP should be running on standard port 22. If all network systems are behind 1 firewall, then the port should be 2022.
    - This system MAY be migrated and replaced with one of your choosing. The system MUST be a Unix like OS such as Linux or FreeBSD and must be freely available.

DNS

For this competition, you will need to provide your own DNS. The white team will be the authoritive provider for cdc.com. Your team will need to provide DNS for siteN.cdc.com. You can host DNS on any server of your choice, including a dedicated VM. DNS is very important, because if it goes down so will the rest of your services. Your team may even want to consider running it on two machines.

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.

Dr. Bob and Dr. Ann

We have two dentists that work with us on various projects. The public doesn't know how badly we were hacked, so we don't want to go spreading the details

around to anyone who doesn't HAVE to know. Dr. Bob and Dr. Ann used the XP desktop that was compromised remotely. We let them set their own password, so we don't know what password they used on the XP box and on TROGDOR. So, if they didn't use the same password on TROGDOR as the XP box, we don't have to disable their account and tell them about the incident. If they did use the same password though, you need to disable their account until we can talk to them.

drbob and drann are the accounts on the shell box. We'll provide you with the windows password file so you can figure out what their passwords were. Once you figure out their passwords, if they are the same, disable the account on TROGDOR and create a new disabled account on the RDP server. If the passwords don't match, create a new account for the user on the RDP server using the password from the TROGDOR account. That way we can just tell them to use the new RDP server using their TROGDOR password.

Note: If an account is disabled that shouldn't be, or is not usable on the RDP server that should be, your team will lose green team usability points.

The windows password database from the hacked XP box can be found on TROGDOR at /root/xp_password_db.pwdump

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.

Backups

The web and shell boxes back up to TROGDOR. TROGDOR backs up to the shell box. These backups MUST be performed. You may perform them however you chose, but the data backed up, and the frequency of the backups, must be maintained. See the admin documentation wiki on TROGDOR for more information on the backup setups.

NTP (Network Time Protocol) requirement for all services

- All systems are required to have accurate time within 10 seconds of the provided NTP server at: ntp.cdc.net (this server is only available on the competition network).
- The built-in time keeping and syncing capabilities of Windows may be used, so it won't be necessary to install NTP separately on Windows systems. We leave it up to your team to determine how you want to sync time on any Windows servers you may have with our central NTP server.
- The shell server must allow regular users to run the "ntpq" command, and then run the "pe" command (within ntpq) to see the list of NTP peers.
- You may sync all your systems with the provided NTP server at ntp.cdc.net, or set up one of your own that provides NTP to your network. A firewall system would be a good system to run an NTP server from. Just be sure that your time throughout the network remains in synchronization with our NTP server at ntp.cdc.net

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 us for upgrades. 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, March 2nd from 5:30pm until 11:59pm). Your site must be online by 8:00am on Saturday, March 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.

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 Max Peterson, this year's CDC director. I've been an ISEAGE employee since March 2011, and I've participated in multiple Cyber Defense Competitions over the last five years. In 2011 I was the Green Team Leader for both the ISU CDC and C3DC, so I'm hoping to see some familiar faces at Iowa State once again this year.

As you've probably noticed, we've made a few changes to the scenario this year (such as DNS). The goal in doing this is to challenge you even more (this is Nationals after all) and give a better representation of the IT industry. I would love to hear feedback on this year's scenario.

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

- Max Peterson, Director