NATIONAL CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
SPRING 2013

Thank you for coming on board at Cyclone Development Company! We are a fast-growing development company which excels in software consulting for businesses around the world. My name is Glen, and I am the Director of Information Technology at Cyclone Development Company. As the Director of IT, it is my top priority to ensure our developers and other staff have all the resources and services they need, and not a moment after they need them.

We are very excited for you to start here. Our lead network administrator, Jim, got fired last week after a large attack on our systems and we are in need of help to get everything back online as soon as possible. During the attack, many of our systems were compromised; some of them beyond repair (the RDP server, for example). The remaining systems will need to be fully inspected for any lingering security risks or back doors planted by the attacks. We have already wiped the systems that could not be recovered, so you will be responsible for bringing those systems back online.

Jim has setup many of the systems himself, including the payroll system on the web server. He used an open source payroll application built on Python using the Flask framework. He mentioned using this solution because of how it integrates with our API server. That's about all I know about the payroll application, but I'm sure there is good documentation about all of that on the Internet.

We tried to secure some of the attacked boxes after the attack. However, we could not be sure about the web server so it was blown away replaced with a fresh Debian box. We then reinstalled the payroll app from the source at https://github.com/mpdavis/ncdc-web. The machine itself should be fully secure, but we may want to run the payroll application though a security review at some point. Unfortunately we forgot to save the user database, so you will need to input all of the users from the Users and Password list document yourself.

Our mail server was salvaged and is running an older version of both Windows Server and Microsoft Exchange. It's been on my list of things to upgrade for a while, but I'll leave that decision to you. It is currently attached to our Domain Controller, which was also salvaged. I'll let you decide if you would like those to remain on separate installations of Windows Server. One quick note about these servers: they are currently running on an outdated domain. You will need to migrate them to a different domain as well after upgrading them. I'll leave the details down below.

There is a shell server on the network too that some of our remote developers and in house infrastructure developers use to compile code on. They occasionally like to try running scripts and such on it to be sure it works in linux (most of them develop on OS X). This was salvaged after the attack and its current condition is unknown. Please make sure it still satisfies the developers' needs.

You'll notice that Jim still has accounts on many of the systems. Since he no longer works here his access should be revoked as soon as you can get to it. We don't need another attacking episode to occur due to harsh feelings.

The rest of the details for each of our systems is detailed below. Please read it thoroughly so that there are no surprises when you get into the systems. I hope everything makes sense. If you have any questions along the way please be sure to ask! There are plenty of resources available to help in your success.

Thank you again for your commitment to Cyclone Development Company! Good luck!

- Glen Goodman, Director of Information Technology

Your network must provide the following services:

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

This server is on a current version of Debian, so the OS should be secure. 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 social security numbers!), and other web security measures to protect our sensitive data from being leaked. This server connects to the API server to generate payroll reports.

- 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.
- Content must be backed up (including any databases).
- Ask the competition director if you need further clarification.

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

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. In the past they have used this shell server. They just need a place where they can login and run the following things.

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 also be able to run python files and use a python interpreter. 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
- Administrators (dave and susie) must have sudo access
- **User files must be backed up**

Exchange/Email Server (mail.siteN.cdc.com) [PROVIDED]

The corporate email runs Microsoft Exchange 2003 on a Windows Server 2003 box. It is very out-of-date, but in working condition. Your team is welcome to migrate to any mail provider of your choice, or keep the current server. If you choose to switch, you must migrate the existing mailboxes. Many employees prefer to check their mail using a web browser, so your mail server must provide web access over self-signed SSL/TLS.

- SMTP should be running on standard port 25
- IMAP should be running on standard port 143
- POP3 should be running on standard port 110
- Web mail should be accessible over https on port 443
- All mail currently on the server must continue to be available

Domain Controller/Active Directory (dc1.siteN.cdc.com) [PROVIDED]

Your team must provide Domain Controller services to the network. This Domain Controller must be available to the entire network for remote users to connect to and authenticate against. You are not required to keep the provided DC, but if you re-create one yourself it must work correctly on Active Directory's default ports of 389 and 88.

Currently this system is setup on the “cydevcompany.com” domain. This is the old company domain, and it needs to be migrated to the new domain at “siteN.cdc.com” where N is your team number. Please be sure to do this soon so users do not lose any mail.

API Service (api.siteN.cdc.com) [PROVIDED]

This server exists to generate Microsoft Excel documents. It was built on Windows because that was the easiest way at the time to generate .xls files. The payroll system uses this when a report needs to be generated for a user. This system is optional, but the reporting functionality is not. The service currently resides on the Domain Controller.

- Accessing api.siteN.cdc.com on port 80 should return the recent report generation page.
- Reporting functionality on the payroll application must remain intact, but is not required to utilize this server explicitly, as long as the above requirements are satisfied.

RDP Server (rdp.siteN.cdc.com)

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. 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 host Windows Terminal Services on the OS/version of your choosing. Every user should be able to access and run the following programs, and icons to these programs should be shown on all users' desktops:

- FileZilla FTP Client
- Notepad++
- Mozilla Firefox
- PuTTY SSH Client
- LibreOffice
- Adobe Acrobat Reader
- Google Chrome
- Eclipse IDE

Backups (does NOT need to be publicly accessible)

Our backup system got corrupted and lost after the attack. We need to get a backup server online ASAP and have it backup all critical data from other servers.

- Must backup emails, shell server contents, RDP user documents, and web server databases
- Must keep a minimum of 8 backups at 1 hour intervals.
- Backups will be checked during the competition.

DNS

Your team is required to host DNS for your network. All required subdomains are listed next to the accompanying required service. ISEAGE, our ISP, will forward all DNS requests in our zone to the .1 IP address of our range. (If your range is 64.9.53.0/24, DNS should respond on 64.9.53.1)

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, March 1st from noon until 11:59pm). The site must be online by 8:00am on Saturday, March 2nd!

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

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 six years. In 2012 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, there's a lot going on in this scenario. 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 as well as suggestions for the future.

I am very excited to be working with our sponsor for this event, WebFilings. They will be providing food and drink for the event as well as some sweet prizes. Their marketing team has also designed the new NCDC logo for us! If you are interested in potentially pursuing a career or internship with them, I would like to suggest bringing a resume. WebFilings managers and team members will be on site the day of the competition.

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

- Max Peterson, NCDC 2013 Director