Iowa State University

OF SCIENCE AND TECHNOLOGY

ISERink

Student L10A1

In the following activity, an organization will be described. Try to imagine what the potential risks could be in such an organization. To begin, simply read over the following organization (adapted from a previous CDC) carefully.

Welcome!

I am Robert Commit of Cache, Daemon, & Commit, Attorneys at Law. We are pleased to welcome you to the Information Technology division of one of the premier law firms of Iowa since 1912. You will be a valuable addition to the long line of dedicated men and women who have helped thousands of people with legal affairs over the past century.

You are joining the company in our new information technology team to provide the services that our lawyers and clients need to be productive and efficient. Your duties will include maintaining our existing servers and adding desired capabilities. We have a long tradition in providing the very best and hope you will take our value of excellence to heart.

An integral part of our company is protecting and safeguarding our clients' privacy. We have many cases that are not known publicly and we must protect client confidentiality. At the same time, we must maintain excellent records for auditing purposes. These two goals drive our need for safe, secure, and comprehensive systems.

Below I have attached a list of our servers and systems and what services they must provide. It includes your duties as a member of the Information Technology team of Cache, Daemon, & Commit. Make sure to read it carefully and understand everything that you need to provide. One key thing to note will be that Cache Daemon Commit has funds for up to three new servers, one of which will be the new RDP server. There is a strict 6 server limit, however.

We hope you enjoy your time at Cache, Daemon, & Commit!

Robert Commit

Partner, Cache, Daemon & Commit, Attorneys at Law

By entering into employment at Cache, Daemon, & Commit you hereby release and discharge forever Cache, Daemon, & Commit, its clients, partners and employees from all liability including but not limited to loss of life, bankruptcy, defamation of character, destruction or damage of property, and psychological harm.

Corporate Webserver (www.teamN.isucdc.com)

Default Username: root
Default Password: cdc

Our CentOS webserver hosts our corporate website. The website was created with a front-end of Angular JS and a backend of PHP and MySQL. There are three main features of the website. The first is the company and lawyer profiles which are open to the public. Lawyers and other company employees have access to the second section which is the cases list. The last section is the information about each case including a portal to upload and download files. The files will be stored on the file server located at ftp.teamN.isucdc.com. Each lawyer should only be able to view the files relating to the cases on which he is working (listed above). Unfortunately, we do not have the resources to rebuild the server from scratch and have no desire to leave CentOS.

Required Access

- All employees should be able to upload and download files

Required Services

- Website on port 80
- SSH on port 22 for administrator

FTP Server (ftp.teamN.isucdc.com)

Default Username: root
Default Password: cdc

We have an FTP file server that employees that can use to upload and download case related files. Each case will have a separate folder. Inside each case folder, there will be a folder labelled "evidence". All files on this folder must be available through the web based interface on http://www.teamN.isucdc.com. Our sensitive case files must be accessible through the web based interface and FTP to the lawyers working on the case. We are very happy with our current server and do not have the resources to rebuild it from scratch.

Required Services

- FTP access over port 21 (or other port with permission)
- SSH on port 22 for administrator
- Must be available via web interface on corporate web site

Help Desk Server (help.teamN.isucdc.com)

We have hired a reputable tech company to make a chat server. This chat server will be used by our employees and clients for tech support with our services. This chat server is available at https://download.iseage.org/chatbundle.tar.gz. You are free to use this chat server or create your own but you must provide a realtime chat service for our employees and clients. It can be hosted on any server but must be accessible to the public at help.teamN.isucdc.com. If you use the provided chat bundle, nginx and Java are required.

Required Services

- Chat over port 80

Question to Discuss:

1. What jumps out to you as an obvious place for an attacker to start if their goal is to compromise your confidential information?
2. How could an attacker use the Held Desk Server to obtain sensitive information?
3. You are inheriting these servers “as-is” from employees that worked here previously, and do not have the funding to start from scratch. What issues can you imagine coming out of this?
4. Multiple ports will need to be open running various services including port 21 (FTP), port 22 (SSH), and port 80 (HTTP). What are some ways you can secure these services while still allowing them to function properly?