The Rebel Alliance

Memorandum

To: Leia Organa
From: Lucas Hsu

Introduction

Searching for ways to secure our server led to a long journey of research and test implementation. After trial and error, I found and listed the problems I could fix. Securing the server is a work in progress, but here are my findings.

Organization

The initial setup of the server lacked organization. Some of the people allowed to access the server were empire droids and Darth Kate herself. I removed access from them so they could no longer enter the server. With them removed, I added the rest of the officers and members to the server. Now Leia Organa, Bail Organa, General Draven, and others can log in and see the files needed for the death star attack. I am unsure why some officers lacked access, but I fixed it. In the future, I recommend setting up who has access to the server early and ensuring they have access.

Files

For some odd reason, only I could see the files critical to the success of our mission. The death star plans, the echo base layout, and the rebellion fleet locations were all under my control when they should not. I gave those files to the right people to ensure each had the necessary information. Now, the correct officers can see the files and are ready to go. If you add new files or other officers upload files, ensure that the files are with the right people.

Banner of the Day

When you first log in, you receive a message that radiates empire. Being greeted with an empire message was offsetting, so I changed it into a greeting for officers and officials to make them feel more welcome. If this happens again, ask IT to change the banner.

Passwords

The passwords used were simple, at best, and stored in an insecure file. I changed the passwords and notified each person of their new password so they could access the server. I tested other ways of making the passwords secure, and I landed on one that was reliable. If the empire gets your passwords, I would be surprised. I recommend sending a message to everyone about password etiquette to prevent hacks.

SSH

To make these changes, I had to log in remotely so I could work. The only problem with logging in outside our network is that it makes the server prone to attacks. I first tried to secure the server by adjusting some settings to make it harder to hack. I encountered a problem when something happened to the whole server, and I was locked out. The technicians rebooted it, and I was able to fix the problem. I updated SSH to make it more secure and left it at that. In short, I recommend finding a safe way to secure SSH better and limiting users who try to log in.

Updates

The server was way out of date. With a few commands, I installed what was necessary to protect the server the easiest. That meant installing a firewall and Apache to help utilize resources. I also updated some services that helped make my job easier. Whenever an update is released, update your server. It will help protect it as well as optimize the system.

Random Message

I do not know who gave Han Solo all privileges, but it ended up backfiring. The empire hid a message that would broadcast at random intervals to everyone. Even after deleting the message, the broadcast was just there. I tried my best, but that message will still appear now and then. If you have complaints, take them up with Han Solo. In short, ensure the people who have access to everything are allowed to have access to everything.

Firewall

With a critical server like the rebellions, having a fire is key. The only problem is the server did not have one. To address this, I installed and enabled the firewall to ensure outside intruders would not enter. I succeeded in putting up the firewall. When another server is added to the rebellion network, activate the firewall to limit access to protect the server.

Other

I poked around a bit and found many files and connections that surprised me. The fact that over 80 countries connected to the server concerned me. I also discovered a Voldemort file that looked fishy and out of place. Since I did not know what it did, I left it alone. I recommend checking the system for suspicious files and looking through them to determine if they are necessary.

Closing

The server needed serious help, and I provided what I could. Even with what I did, the server is still vulnerable. I learned loads of commands and even tried to hack back in to continue my work but to no avail. My computer can only run so fast and cracking passwords takes a lot of time and power, which are things I do not have. So, I hope the empire does not hack your server, and I also hope others can double-check my work. I wish I knew how, but I'm just a cybersecurity vigilante from Jakku. With the current precedent, I'd recommend hiring another cybersecurity professional cleared as a rebellion supporter.

Screenshot of survey: