

The Rebel Alliance

Memorandum

To: Leia Organa

From: Cameron Snider

Introduction

As the leader of our new Cyber Squadron, I have extensively searched and modified our computer network, and have found many major security concerns. From unauthorized users, to files with incorrect permissions, and even sensitive Rebellion data in the hands of Darth Kate herself. It is imperative that we hastily secure our network, and start using new security protocols to ensure this doesn't happen again.

First Key Point

The first issue I noticed when searching our network, was that there are a lot of unauthorized users. I discovered that Darth Kate had already infiltrated our system. This is obviously a major security concern, as she would have access to all of our sensitive Rebellion files. She actually already had access to a file that showed the location of the Rebel Base. Fortunately, I was able to take the file back, and reassigned ownership of the file to Admiral Ackbar. I was then able to remove Darth Kate from our system, and she is no longer a user that can look at our files. I also set up a simple UFW Firewall to help keep out Empire spies in the future. On top of this, I made sure that other critical services like SSH and apache2 were updated and running properly.

There were also authorized users that were not using our network properly. Han Solo was using the network to broadcast a message about the Rebellion every two minutes. This was not only extremely annoying, but was also entirely unnecessary, as any legitimate users on the Rebellion's personal computer network are already fighting the Empire. Perhaps this message might be better served being broadcast to other

computer networks. I was able to remove Han Solo's ability to broadcast this message, which helped keep our network cleaner and reduced unnecessary traffic.

Second Key Point

The second issue that I noticed was that there were certain sensitive Rebellion files that had incorrect permissions. This meant that they could be seen and even changed by users that we didn't want to see or modify. There were three in particular, including:

rebel-fleet-locations.jpeg

echo-base.webp

death-star-plans.jpeg

It could potentially be very bad if the wrong people were to have access to the files above. I made sure to give the right people the permissions that they needed in order to ensure their safety and proper use.

Etc.

In the future, I would recommend using some new security protocols to ensure this does not happen again. First, any new users need to be created and authorized by me. This will ensure that the only users in the system are the ones that are meant to be there. On top of this, I will also be checking the list of authorized users every day to make sure that there aren't any new unauthorized users that have made their way into the network. Our new UFW Firewall should help out, but it will still be good to manually check to ensure absolute safety.

Also, any new sensitive Rebellion files or documents should be cleared with me before they are uploaded to the network. This will allow me to manually assign the specific permissions that each file needs to allow the right people to see and modify them. This will ensure that our secret files don't end up in the hands of Darth Vader again.

Finally, nobody will be allowed to broadcast messages on a set schedule. This will help make sure our network stays clean, and will make sure that people don't just tune out the important broadcasts.

Closing

Although there were many major security problems, I was able to secure our network and keep Darth Kate out. If we all make sure to follow the new security protocols I have set up, this will not happen again, and our important Rebellion files will not end up in the hands of Darth Kate again. If you have any questions about the process, or what you should do to ensure total Cyber Security in the future, please reach out to me and I will be more than happy to walk you through everything.

(Here is a screenshot of my Qualtrics Survey)

We thank you for your time spent taking this survey.
Your response has been recorded.