The Rebel Alliance

Memorandum

To: Leia Organa
From: Conrad Bradford

Senator Organa,

This memo was created to inform and educate you about the recent security breach in our systems by the Galactic Empire. We have confirmed that this attack was orchestrated by the Sith Lord, Darth Kate. Our team of agents has done their best to recover, but we are still unsure of the depth of this breach. Our findings and attempts of recovery are reported below.

Vulnerabilities and Problems Found

In our server we found several unauthorized users who could remotely login (ssh) with their own passwords. The users were Obi1, Darth Kate, Jar, and ysanneisard. We also discovered that the message displayed upon a user login (message of the day) was altered to display Darth Kate with intent to intimidate the whoever just logged in. We also discovered that several user accounts had been deleted and that several incorrect accounts had administrative privileges (root access). The accounts missing were Leia Organa, Bail Organa, Mon Mothma, Admiral Raddus, and Admiral Ackbar. The accounts with unauthorized admin privileges (meaning they can do whatever they want on the server) were Han Solo and Darth Kate. The Empire used Han Solo's account to broadcast a rebel message every two minutes using an automated process executor on our server known as crontab. The Empire also snuck several password stealing files and processes in multiple locations throughout the sever. There was a password cracking cronjob (a repetitive command that logs the password to another server periodically which bypasses password updates). There was a password directory that also kept track of all user passwords and put them onto another server. Under the root directory we

Commented [A1]: As part of the assignment, you will write a report on any of the modifications and remediation that you have performed on the systems. The report will be in the form of a memo to the leader of the Rebel Alliance, and should detail the following:

1. What did you find?
2. What you did do to fix it?
3. Suggestions for new policies and practices to safeguard their computer systems

Using the provided template write a 500 to 1000-word memo. The leader is a politician and not a tech person at all. All technical terminology used needs to be understood by a non-technical audience. The report should be uploaded to GitHub as a PDF, no other file format, and the link submitted to Learning Suite. If you consented to be a research subject, you must also include a screenshot showing you completed the Qualtrics survey. The report should be logical, flow well and have good spelling, grammar, and punctuation.

found a reverse shell file. This file allows another computer to connect to any IP address (any device) through any port (route). In the server was also planted numerous Empire propaganda The Empire changed all of our passwords to “1234” and made all of our top secret files accessible to anyone. It is a shame how they have exploited us.

Solutions and Patches

In order to resecure our server and regain control we deleted all the suspicious files and password stealing methods. We then changed each user password to something unique for that user. We added the missing users and, we also updated the administrative group to have only the authorized admins. We moved all of our top-secret files to the correct directories with the correct users. We changed the permissions of those files to only allow those we want to read, edit, and move the file. We also removed all unauthorized users: Darth Kate, Jar, Obi1, and yisanneisard. To further secure and improve our system we updated our server. We disabled anyone from logging in through the root (all powerful) user unless they are already logged in with their account, and have administrative access. We installed UFW which is a firewall. We made sure the firewall only allows access to our server through a specific set of IP addresses. IP addresses are the locations of the devices trying to login. We also installed apache2 which will improve our servers ability to read and access web servers. Finally, we deleted Han Solos cronjob that was constantly displaying and interrupting the server, and we changed the message of the day (login message) to the Rebel Alliance default. We are unsure of all the weaknesses in our server, but this is what we found and fixed.

Safe Practices and Policies for the Future

We recommend keeping your password private, and unique. Don’t use simple passwords like “1234” or “password” or “mynameis____”. Those can easily be guessed by someone trying to break into the system. Using a longer passphrase only you would know is much more secure. We also recommend checking who is logged in whenever you are on. This can be done by typing the command “who” into the server and hitting enter. If you find suspicious users logged in, you can then take action to remove them and find out how they accessed the server. We also recommend not disclosing your IP address to anyone as that would allow them to get past our firewall security system. Don’t click on any suspicious links that people email you, or from someone you don’t know because that could allow them access to your computer or to get your IP address.

In effect, the Rebel Alliance is still intact, and we are constantly learning how to use and improve our server so we can one day defeat the evil Galactic Empire.