Final Log Analysis(Objective 6)

Lengthy Logs: Attack Analysis

> Tyler Higgins | 12-19-2020

System Affected

`Prod-Web Server`

Service Affected

`MySQL`

In an attempt to find out what happened, I first started by looking for all the log files I would need to review. I was unable to find any log files for the WordPress install, and it was confirmed in the WordPress config file that while debugging is enabled, logging of the errors is not. This made it impossible to find the WordPress user that was used to compromise the system. In an attempt to still figure it out I tried a few different users, playerone, root, NONE, MySQL, and admin. None seemed to be the correct user to complete the challenge.

Moving on to examine the logs I was able to find, which was the log file for the MySQL database instance, I was able to observe that on 09-12-2017 @ 10:59:57 a command was issued to delete all entries in the user table named wp-users `query DELETE * FROM wp_users`. This completely wiped out the list of users in our database. The location of the log file is `/var/log/mysql/mysql.log`

While looking over the log it looked like the playerone user was first selected, during the attack to gain more information, which is what lead me to think that was the user that was compromised, especially with the weak password.

I believe this attack could have been prevented with a better password policy in place for all users, especially admins. Having weak passwords for high ranking accounts is never a good idea for reasons like this one, a break-in that wiped out our entire database of users.

The fix for this attack is luckily simple, the password for playerone needs to be changed and the security of the password needs to be upgraded and a backup of the WordPress database needs to be used to restore access to the system. We should also enable all logs in the WordPress config file so we can get a more detailed look in case this happens again.