Credentials Rotation

Last Modified: August 29, 2022, by Carlos Hermosilla

Use Cases

- The credentials used for the production environment are too old
- Someone who had credentials for any server has left the company
- The current credentials have been compromised for one of several reasons. For example, the laptop of an employee got stolen

Description

Credentials should be changed at least once a year to minimize the chances of someone external having access to them. If there is an extraordinary event, like someone leaving the company, or something that could compromise at least one of the credentials used for production/test/development, it is advisable to perform this process as soon as possible.

Steps

1. Check MFA is enabled at least on the root accounts of any cloud platform you use. Ideally, MFA should be enabled on all users.
2. Delete and/or reset the password on any proprietary instance (Lesli, Deutsche-Leibrenten, etc.) of the users who are leaving or had their credentials compromised. This must be done for all servers that they had access to.
    a. Change the password of other users if necessary
3. Delete or change the user's password on AWS, Google Cloud, or any other platform that the company uses for their cloud infrastructure
4. Inside each platform, you need to generate new credentials for each environment. That will depend on the cloud platform you are using, but here is an example of steps you need to take in AWS:
    a. Generate a new SSH key/pair for the servers. Since the servers are linux instances, you can use the same ***ssh-keygen*** command you would use on any normal linux machine.
    b. Generate new credentials for any programmatic user using IAM.
    c. Generate new credentials for any user on the system (this should not be necessary, but if the user that is leaving/was compromised created those credentials, it is possible they may have them.
    d. Generate new API keys that you may be using on your system