# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The security analysts from the IT team of this social media organizations looked up some of the vulnerabilities that threat actors could exploit in the future: the organizations’s employees’ share passwords, the admin password for the data base is set to the default, firewalls are outruled and they are not able to filter traffic and multifactor authentication is not used.  So, as security analysts, we chose some hardening tools and methods you could use to prevent a data breach. The first one is to ensure a multifactor authentication (MFA) that currently doesn’t exist. The second one is to add password policies due to the high risk it involves about the current condition of the passwords. The last one is about to configure firewall maintenance that hasn’t been done. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| We selected the multifactor authentication (MFA) to help protect against brute force attacks and similar security events, is a hardening tool that is set up once and then maintained. The organization doesn’t have anything like this tool so it’s a very useful step into becoming more secure as a organization. Adding password policies will fill up two of the four vulnerabilities of the organization, they are used to prevent attackers from easily guessing user password, manually or using a script to attempt thousands of stolen passwords, it’s a method that is set up once and reviewed. Lastly, the firewall has to be configured correctly in order to filter traffic coming in and out of the network, otherwise the organization is open wide to data breaches and threat actors, it’s a tool set up once and then maintained. |