# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| After discovering the major vulnerabilities in the organization’s network, the security analyst recommended hardening tools and methods to implement. First, setting up Strong password policies. After inspecting, the organization’s employees’ share the same password together and the admin password for their database is set to default. The organization is likely to be breached again by an attacker using a brute force attack. To prevent this from happening, the security analyst recommended implementing strong password policies to prevent attackers from easily guessing user passwords and enforcing frequent changes to passwords. Include rules regarding password length, a list of acceptable characters and a symbol. Also the user losing access to the network after a certain number of unsuccessful attempts. Second, the organization’s firewalls do not have rules in place to filter traffic coming in and out of the network. The security analyst recommended implementing a firewall maintenance which will be set up once and updates from time to time. It entails checking and updating security configurations regularly to stay ahead of potential threats. Lastly, the organization does not use Multifactor Authentication (MFA). The security analyst recommended implementing a Multifactor Authentication on top of a strong security password. It is an added security measure that requires a user to verify their identity in two or more ways to access a system or network. Such as pin number, biometrics, one-time password (OTP) and more. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Enforcing Strong password policies within the organization instead of employees’ sharing the same password and admin password is set to default for a better and add more security layer in the organization. It will discourage and find difficult for malicious actors from using brute force attacks and will not likely to access organization’s networks and data. This security hardening method should be enforced regularly within the organization.  Setting up firewall maintenance and should be updated before an incident occurs proactively and after an incident occurs to stay ahead of potential threats. This method also protects the organization from various DOS attacks such as a smurf attack combining both IP spoofing and DOS attack.  Enforcing Multifactor Authentication (MFA) since the organization is not currently using this method. This can be set up once then maintained regularly. Combines this with strong password policies and on top of that, it requires users to verify two or more ways to access the system like a biometrics, ID, pin number etc. will discourage the malicious actors from setting up an attack. It is effective against brute force attacks and similar security events. |