# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| After inspecting the organization’s network, we discovered four major vulnerabilities. The four vulnerabilities are as follows:   1. The organization’s employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multifactor authentication (MFA) is not used.   We can suggest:   1. Setting and enforcing strong password policies, addressing the NIST latest recommendations for password policies. 2. Implementing multi-factor authentication (MFA). 3. Performing firewall maintenance regularly, Configuring port filtering on the firewall.   Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts.  MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords.  Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack). Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. The rules that are included in the password policy will need to be enforced regularly within the organization to help increase user security.  Multi-factor Authentication es security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. Can help protect against brute force attacks and similar security events. MFA can be implemented at any time and is mostly a technique that is set up once then maintained.  Firewall maintenance should happen regularly. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication. Port filtering is used to control network traffic and can prevent potential attackers from entering a private network. |