# Security risk assessment report

**Scenario**



Review the following scenario. Then complete the step-by-step instructions.

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers’ personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization’s network, you discover 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.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three hardening tools and methods to implement for addressing the vulnerabilities found:   1. Perform firewall maintenance regularly. 2. Implement multi-factor authentication (MFA). 3. Setting and enforcing strong password policies. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. Perform firewall maintenance regularly.   Firewall maintenance should happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.   1. Implement multi-factor authentication (MFA).   Multi-factor authentication (MFA) can help protect against brute force attacks and similar security events. MFA will also make it more difficult for people within the organization to share passwords. Identifying and verifying credentials is especially critical among employees with administrator level privileges on the network. MFA can be implemented at any time and is mostly a technique that is set up once then maintained.   1. Setting and enforcing strong password policies.   Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script. 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. |