# 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

The social media organization suffered a major data breach, resulting in the release of names and addresses, this is Personally Identifiable Information (PII). As a result of the data, a security risk assessment has been conducted. Upon inspection of the network, the four major vulnerabilities are:

1. **Employee's share passwords**
2. **Admin password for the database is set to default**
3. **Firewalls do not have rules in place to filter ingress and egress traffic**
4. **Multifactor authentication (MFA) is not used.**

Hardening tools and methods to implement for these vulnerabilities are the following:

- **The organization's employees' share passwords**.

    1. Password policies,
    2. MFA,
    3. Network access privileges

- **The admin password for the database is set to the default.**

    1. Password policies,
    2. Baseline configurations,
    3. Configuration checks

- **The firewalls do not have rules in place to filter traffic coming in and out of the network.**

    1. Port filtering,
    2. Disabling unused ports,
    3. Network log analysis
    4. Firewall maintenance

- **Multifactor authentication (MFA) is not used.**

    1. MFA
    2. Password policies
    3. Network access privileges

## Part 2: Explain your recommendations

1. The organization’s employees' share passwords.
    - **Password policies:** Implement strong password policies that require employees to create complex passwords, regularly change them, and prohibit the sharing of passwords.
    - **Multifactor authentication (MFA):** Enforce the use of MFA, requiring users to provide multiple forms of authentication to access sensitive systems or data.
    - **Network access privileges:** Implement proper access controls and restrict user privileges based on the principle of least privilege, ensuring that employees only have access to the resources they need.
2. The admin password for the database is set to the default.
    - **Password policies:** Implement strong password policies that require administrators to create complex passwords, regularly change them, and prohibit the use of default passwords.
    - **Baseline configurations:** Ensure that the admin password for the database is not set to a default value during the initial configuration.
    - **Configuration checks:** Regularly perform configuration checks to identify any insecure configurations, including default passwords, and rectify them promptly.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
    - **Port filtering:** Implement strict port filtering rules on firewalls to block unnecessary ports and restrict access to only essential services.
    - **Disabling unused ports:** Disabling unused ports on firewalls helps reduce the attack surface by closing off entry points that are not required for legitimate network traffic.
    - **Network log analysis:** Continuously monitor and analyze network logs to detect any unauthorized or suspicious traffic patterns, allowing for timely response and adjustment of firewall rules.

- **Firewall maintenance:** Regularly maintain firewalls by reviewing and updating the rule set to filter traffic based on predefined security policies.

4. Multifactor authentication (MFA) is not used.
    - **Multifactor authentication (MFA):** Implement MFA for all user accounts, requiring additional authentication factors beyond passwords.
    - **Password policies:** Enforce strong password policies to ensure that even if passwords are compromised, the additional factor required by MFA adds an extra layer of security.
    - **Network access privileges:** Combine MFA with proper network access privileges to limit access to sensitive systems and data only to authorized individuals.