Scenario

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. Multi-factor 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.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Password Policies 2. Port Filtering 3. Multi-Factor Authentication (MFA)

Part 2: Explain your recommendations

Password Policies:

- **Current Issue**: The organization’s employees are sharing passwords, and the admin password for the database is set to the default. This lax approach to password management significantly increases the risk of unauthorized access.
- **Recommendation**: Implement a robust password policy that follows the National Institute of Standards and Technology's (NIST) guidelines. Additionally, enforce unique and strong passwords for each user and ensure that the default admin password is changed to a strong, unique password.
- **Benefit**: Strengthening password policies will make it more difficult for attackers to gain access through brute force attacks or password guessing, thereby protecting sensitive data.

Port Filtering:

- **Current Issue**: The organization’s firewalls do not have rules in place to filter traffic coming in and out of the network. This lack of port filtering allows any sort of traffic, which can lead to vulnerabilities such as Denial of Service (DoS) attacks.
- **Recommendation**: Implement port filtering on firewalls to block or allow specific port numbers. This will limit unwanted communication and ensure that only necessary ports for network operations are open. Regularly update and review firewall rules to stay ahead of potential threats.
- **Benefit**: Port filtering helps control network traffic and prevents potential attackers from entering the network through open ports, thereby reducing the risk of attacks.

Multi-Factor Authentication (MFA):

- **Current Issue**: The organization does not use Multi-Factor Authentication (MFA), making it easier for attackers to log in if they gain access to passwords.
- **Recommendation**: Implement MFA, which requires users to verify their identity in two or more ways, such as a password, a one-time password (OTP) sent to a cell phone, or biometric verification. This additional layer of security ensures that even if a password is compromised, unauthorized access is still prevented.
- **Benefit**: MFA significantly enhances security by adding an extra layer of verification, making it much harder for attackers to gain unauthorized access to the network.