Security risk assessment report

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.

Part 1: Select up to three hardening tools and methods to implement

1. Password policies
2. Multifactor Authentication
3. Firewall Configuration

Part 2: Explain your recommendations

Password Policies:

- By enforcing strong password policies, we can discourage employees from sharing passwords. These policies should include requirements for complexity, minimum length, and regular updates. Additionally, educating employees on the risks of password sharing and implementing unique login credentials for each user will further reduce this risk. Enforcing a policy that mandates the use of strong, unique passwords for all accounts, especially admin accounts, will ensure that default passwords are changed to more secure ones. Regular audits can help verify compliance with these policies.

Multifactor Authentication (MFA):

- MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access to an account. This significantly reduces the risk of unauthorized access, even if a password is compromised. Protection Against Shared Passwords: In cases where passwords might still be shared, MFA ensures that an additional authentication step is needed, making it much harder for unauthorized users to gain access.

Firewall Configurations:

- Properly configured firewalls can monitor and control incoming and outgoing network traffic based on predetermined security rules. This can help block malicious traffic and prevent unauthorized access to the network. Firewalls can also be used to segment the network into different zones, isolating sensitive areas such as the database. This limits the exposure of critical assets and reduces the potential attack surface.