**Security Risk Assessment Report: Network Hardening**

**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. 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.

**Respond**

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

1. Implementing multi-factor authentication (MFA) MFA requires users to use more ways to identify and verify their credentials before accessing an application. Some may include fingerprint and retina scans, facial recognition (Something you are), ID cards and phone numbers or devices (Something you have/possess), PINs and passwords (Something you know).
2. Enforcing strong password policies It requires the employees to include rules regarding the strength of the passwords, the combination of text, numbers, and symbols and discourage password sharing. Additionally, the organization can set up a prompt that the user will lose access to the network after three unsuccessful attempts.
3. Performing firewall maintenance regularly and port filtering Firewall maintenance checks and updates security configurations to detect threats. Additionally, the firewall can block specific port numbers to limit unwanted communication (Port filtering).

**Part 2: Explain your recommendations**

1. With MFA, the organization can reduce the likelihood of malicious actors accessing a network. Under normal circumstances, the malicious actors will use "Brute Force Attack" or other related attacks to conduct the attacks. MFA also promotes secure identity access to the network.
2. Strong password policies will make the company powerful against hackers trying to hack the network.

3. A firewall can detect suspicious incoming and outgoing traffic. The administrator should monitor this regularly. In addition, this measure is to protect against various DoS and DDoS attacks. Also, port filtering can control the network traffic and prevent attackers from entering a private network.