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:

The organization's employees' share passwords.

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

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

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.

section 1: select upto three hardening tools or methods to implement.

Think about all of the network hardening tools and methods you have learned about in this course that can protect the organization's network from future attacks. What hardening tasks would be the most effective way to respond to this situation?

section 2 : provide and explain 1-2 recommendation
You recommended one or two security hardening practices to help prevent this from occurring again in the future. Explain why the security hardening tool or method selected is effective for addressing the vulnerability. Here are a couple questions to get you started:

Why is the recommended security hardening technique effective?

How often does the hardening technique need to be implemented?

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Implement Multifactor Authentication (MFA): MFA adds an additional layer of security beyond just usernames and passwords by requiring a second form of identification (such as a mobile code or fingerprint). **Enforce Strong Password Policies and User Education:** Require complex, unique passwords and prohibit password sharing among employees. Combine this with training to educate users about secure password practices. **Configure and Enforce Firewall Rules:** Set up inbound and outbound firewall rules to control the flow of traffic, allowing only authorized traffic and blocking potentially harmful connections.

Part 2: Explain your recommendations
Recommendation 1: Implement Multifactor Authentication (MFA) **Why it's effective:** MFA is a highly effective technique for securing user access to critical systems, even if a password is compromised. By requiring a second form of verification (like a code sent to a phone or biometric input), it becomes significantly harder for attackers to gain unauthorized access, even if they obtain login credentials. **How often it needs to be implemented:** MFA should be **enforced organization-wide** and **used continuously**. It should be required for all logins, especially for admin accounts and systems containing sensitive data. Regular audits should be performed (e.g., quarterly) to ensure compliance and effectiveness.

Recommendation 2: Configure Firewalls with Proper Rules

Why it's effective:
Firewalls are a fundamental network defense mechanism. By setting up specific rules to control which types of traffic can enter or leave the network, organizations can block unauthorized access and reduce the risk of malicious data exfiltration or intrusion attempts.

How often it needs to be implemented:
Firewall rules should be **set up immediately** and **reviewed regularly**, ideally every **quarter** or after any major network change. Regular monitoring should also be performed to detect anomalies and unauthorized attempts to bypass the firewall.