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.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to address the vulnerabilities found include: 1. Implementing multi-factor authentication (MFA) 2. Setting and enforcing strong password policies 3. Performing firewall maintenance regularly MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords. Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendation(s)
Enforcing multi-factor authentication (MFA) adds an additional layer of security beyond a password. It will reduce the likelihood that a malicious actor can access a network through a brute force or related attack since additional effort is required to authenticate in more than one way. MFA may also reduce the likelihood of people sharing passwords. Since the recipient of the shared password would need to possess additional authentication besides a password, MFA makes it less useful to share passwords, thereby making passwords less likely to be shared. Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. Policies such as suspending the account after a certain number of logins can prevent successful brute force attacks. Increasing password complexity, requiring more frequent password updates, and not allowing passwords to be reused also help stall malicious actors from infiltrating the network.

Firewall maintenance should happen regularly. Network administrators should ensure that firewall rules are in place that reflect the most up to date standards for allowed and denied traffic. Traffic from sources that are suspicious should be placed on a denied traffic list. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.