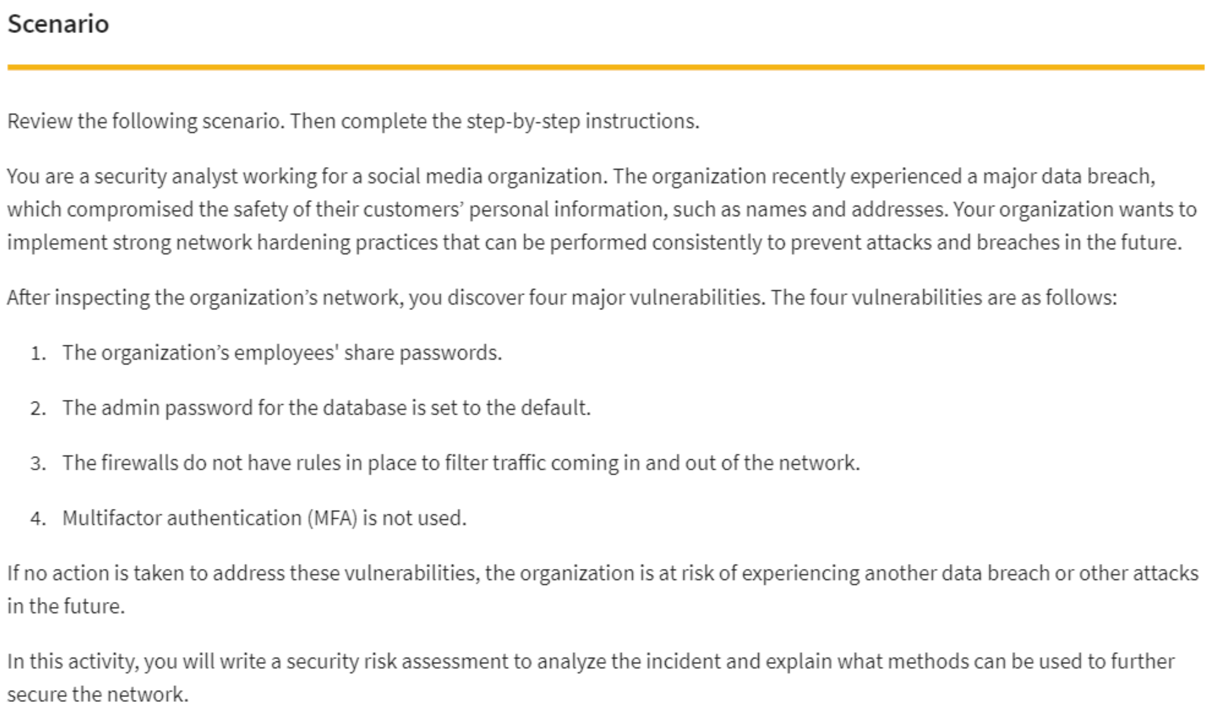
Security risk assessment report



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.

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

1. **Disabling unused port**

Access the switch's configuration interface, locate the unused port, deactivate it using the appropriate command, and save the changes to ensure its inactivity within the network.

2. **Multifactor authentication (MFA)**

Multifactor Authentication demands users to employ multiple methods to confirm their identity before accessing an application, such as fingerprint scans, ID cards, PIN numbers, and passwords.

3. **Firewall Maintenance**

Firewall maintenance involves regular checks, updates, and configurations to ensure its optimal performance in protecting networks, which includes tasks like reviewing rules, updating firmware, monitoring logs, and implementing security patches.

Part 2: Explain your recommendations

1. Disabling unused ports on a network switch helps enhance security by reducing potential entry points for unauthorized access, prevents network loops that can cause disruptions, and optimizes network performance by eliminating unnecessary traffic and potential points of vulnerability.
2. MFA enhances security by requiring multiple ways to verify identity, reducing the risk of unauthorized access if passwords are stolen.
3. Regular firewall maintenance ensures ongoing protection by reviewing and updating rules, checking logs, applying security patches, and keeping the firewall's software up-to-date, all vital in safeguarding networks against evolving threats.