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. Multi Factor 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
1. Instantiate quarterly cybersecurity training for all staff to include password security and phishing identification. 2. Review administrative passwords and define a policy for quarterly administrative password changes. Instantiate a hardened password policy requiring strong character counts and the use of numbers/special characters. 3. Configure firewall rules to exclude traffic to unused ports, or unnecessary traffic that does not benefit the organization. 4. Instantiate a 2FA policy and provide necessary employees with login token devices.

Part 2: Explain your recommendations
1. Employees are a primary and frequent target for threat actors. Training employees to be aware of, and identify social engineering attacks is a primary focus to prevent unauthorized access to organizational systems. 2. Administrative passwords must be kept specifically to those employees who require access to conduct their business operations. Passwords must be kept strong to prevent brute force attacks. Policies must be put in place to require frequent changing to assuage long term threat actor presence. 3. Reduce attack surface by preventing all but necessary activity into the organization's network by configuring encompassing and effective firewall rules. 4. Requiring 2FA reduces the impact of failed security on credentials, creating multiple layers of defense against a threat actor.