Security risk assessment report

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 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 risks experiencing another data breach or other attacks in the future.

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

1. Implementing Multifactor authentication (MFA)
2. Creating Strong Password Policies
3. Ensuring frequent Firewall maintenance

Part 2: Explain your recommendations

1. Since Multifactor Authentication is not used. I recommend implementing an MFA because it ensures that users can verify their identity in two or more ways to access a system or network. Using methods like a password, a one-time password (OTP) sent to a cell phone, fingerprint, and a PIN gives an extra layer of safety to avoid another major data breach. Using MFA, sharing passwords or passwords getting stolen would not be a problem because the real user has to authenticate the log however they are prompted to.

2. Enforcing a password policy makes preventing malicious attacks on the network difficult. Implementing password policies like limiting how many times a password is guessed when logging in within the company will make it easier to avoid brute-force attacks. Increasing password difficulty and complexity makes it harder for malicious actors to guess password combinations and infiltrate the network. Finally, they should ensure that there are password updates and that passwords are not being reused.

3. Firewall maintenance should happen on a frequent basis. This way, admins can monitor traffic and deny certain traffic. Traffic being denied would be from suspicious sources and should be blacklisted. When a security event occurs, no matter how minor or major, firewall rules should be updated, ensuring safety against DoS and DDoS attacks.