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.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
MFA/2FA should be implemented Password Policies should be used to ensure safe passwords Firewalls/port-filtering should be configured to filter out traffic.

Part 2: Explain your recommendations

Issue 1: Issue that was discovered is that the employees share their Passwords.
Remediation: To mitigate the threat of somebody other than the desired user manipulating sensitive information we need to implement 2FA to make sure the user meant to access the information is actually accessing the information

Issue 2:Admin password is set to default
Remediation: Password policies need to be implemented to make sure complex and secure passwords are being used so malicious/Threat actors cannot access and manipulate sensitive information easily

Issue3: Firewalls are not configured/Maintained
Remediation:Firewalls play a very important role in filtering out malicious data/ packets from reaching the device and add an extra layer of security which is why they need to be configured properly to disallow the passing of data from unused ports and filter out data coming from ip addresses that the firewall does not recognize.