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

Multi Factor Authentication (MFA)
Password Policies
Firewall Rules

Part 2: Explain your recommendations

To boost our network security and protect sensitive customer information, I recommend starting with Multi Factor Authentication (MFA). MFA adds an extra layer of security by requiring users to provide multiple forms of verification before gaining access. This makes it much harder for unauthorized users to breach our accounts.

Next, we need to implement strong password policies. This means requiring employees to create complex passwords and change them regularly. Strong passwords are our first line of defense against attacks, so they must be robust and unique.

Lastly, I suggest tightening network access privileges. We should regularly review who has access to what and make sure employees only see the data they need to do their jobs. This way, even if an account is compromised, the damage can be limited.