Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Password policies Firewall Maintenance Multifactor authentication(MFA)

- **The organization's employees' share passwords.**
- **The admin password for the database is set to the default.**
- **The firewalls do not have rules in place to filter traffic coming in and out of the network.**
- **Multifactor authentication (MFA) is not used.**

Part 2: Explain your recommendations
Password policies focus on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. It prevents attackers from easily guessing user passwords which would solve the problem of organization's employees' sharing passwords and admin password for the database being set to the default. This should be implemented regularly. Firewall maintenance entails checking and updating security configuration regularly to stay ahead of potential threats. It helps protect against various DDoS attacks which would solve the problem of them not having rules for firewalls in place to filter traffic coming in and out of the network. This should be performed regularly. MFA requires a user to verify their identity in two or more ways and help

protect against brute force and similar security events. This would help the organization solve the problem of not having MFA and many unsafe password policies they have. This should be performed regularly.