Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to address the vulnerabilities found include: 1. Password policies 2. Multifactor Authentication(MFA) 3. Firewalls maintenance Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts. MFA requires users to use more than one way to identify and verify their credentials before accessing the application. MFA combining what you know (like a password) with what you have (like a phone or security key) or what you are (like a biometric scan). Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Since the organization employees' share passwords and the admin password for the database is set to default, the best solution to address these vulnerabilities is implement a standardized password policies. This will make it increasingly challenging for malicious actors to access the network. Rules such as the user losing access to the network after few times of unsuccessful login attempt, this can create a barrier against brute force attack. Enforcing multi-factor authentication (MFA) adds an additional layer of security beyond a password. It will reduce the likelihood that a malicious actor can

access a network through a brute force or related attack since additional effort is required to authenticate in more than one way. MFA may also reduce the likelihood of people sharing passwords. Since the recipient of the shared password would need to possess additional authentication besides a password, MFA makes it less useful to share passwords, thereby making passwords less likely to be shared.

Firewall maintenance should happen regularly. Network administrators should ensure that firewall rules are in place that reflect the most up to date standards for allowed and denied traffic. Traffic from sources that are suspicious should be placed on a denied traffic list. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.