Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Implementing a password management system will help mitigate the vulnerability caused by employees sharing passwords. A robust password management system can enforce strong password policies, facilitate secure password storage, and ensure each employee has a unique set of credentials for accessing sensitive systems and data. Changing the default admin password for the database is crucial to prevent unauthorized access. By setting a strong, unique password for the admin account, the organization can significantly reduce the risk of attackers exploiting default credentials to gain entry into critical systems. Establishing firewall rules to filter traffic entering and leaving the network is essential for enhancing network security. By configuring firewall rules, the organization can control which types of traffic are allowed or denied, thereby minimizing the exposure to potential threats and malicious activities.

Part 2: Explain your recommendations
The recommended security hardening technique of implementing a password management system is effective because it addresses the vulnerability of employees sharing passwords. The password management system ensures that each employee has unique credentials by enforcing strong password policies, such as minimum length, complexity requirements, and regular password rotations. Additionally, centralized storage of passwords in an encrypted format enhances security and prevents unauthorized access. This hardening technique must be implemented continuously, with regular audits and updates to password policies and configurations. Changing the default admin password is an effective security hardening method because it mitigates the risk of using easily guessable or widely known

default credentials. The organization can significantly reduce the likelihood of unauthorized access to critical systems and databases by setting a strong, unique password for the admin account. This hardening technique should be implemented immediately upon deploying any new system or application and enforced as part of the organization's password management policy.

Configuring firewall rules for traffic filtering is crucial for enhancing network security by controlling traffic flow entering and leaving the network perimeter. The organization can mitigate the risk of unauthorized access and potential attacks by defining specific rules to allow or block certain types of traffic based on predefined criteria, such as IP addresses, ports, and protocols. This hardening technique should be implemented as an ongoing process, with regular reviews and updates to firewall rules to adapt to evolving threats and network requirements.