Network Hardening: Security Risk Assessment Report

Part 1: Select up to three hardening tools and methods to implement
1. Firewall maintenance 2. Password policies 3. Multi-Factor authentication

Part 2: Explain your recommendations
The organization lacks proper network traffic filtering rules, necessitating firewall maintenance. Implementing appropriate firewall rules is crucial for safeguarding against Denial of Service (DoS) attacks. To remain effective, this process should be performed regularly, allowing for adaptation to the latest network traffic anomalies. Concurrently, it's advisable to review and restrict port access to only those essential for operations. The absence of robust password policies has led to password sharing among employees, and the database's admin password remains at its default setting. To mitigate the risk of successful brute force attacks, it's imperative to establish password requirements that mandate sufficient length and character diversity. Additionally, incorporating hashing and salting techniques will significantly enhance password security. Given the current lack of proper password policies, it's crucial to implement multifactor authentication (MFA). Requiring all employees to use MFA provides an additional layer of defense against brute force attacks and enhances confidentiality by limiting access to sensitive assets only to authorized personnel. The implementation of MFA is typically a one-time process, with ongoing maintenance primarily involving the proper activation, deactivation, and management of authentication devices.