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. Multifactor authentication

Part 2: Explain your recommendations
Firewall maintenance is necessary because the organization currently lacks rules to filter network traffic. Proper firewall rules are crucial for protecting against Denial of Service (DoS) attacks. Regular updates are needed to stay current with the latest network traffic anomalies and to ensure only necessary ports are open. Password policies need to be implemented because employees are sharing passwords, and the admin password for the database is still set to the default. Establishing password requirements with sufficient length and character variety, along with the use of hashing and salting, will significantly reduce the risk of successful brute force attacks. Multifactor authentication (MFA) should be mandatory, especially since proper password policies are not yet in place. Requiring MFA for all employees enhances protection against brute force attacks and ensures confidentiality by restricting access to sensitive assets to only those who need it. Implementing MFA is a one-time process, with ongoing maintenance involving the activation, deactivation, and management of devices.