Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

- Password Policies: Implement password "salting" and "hashing", following NIST recommendations, to protect stored credentials.
- Firewall Maintenance: Regularly update and apply security rules to filter network traffic and stay ahead of threats.
- Multifactor Authentication (MFA): Require a second form of verification for access, protecting against the use of stolen passwords and brute force attacks.

Part 2: Explain your recommendations

- Password Policies: Directly resolve the issue of the database administrator password being set to default by preventing attackers from easily guessing passwords.
- Firewall Maintenance: Corrects the vulnerability of having no traffic filters, which is essential for network defense and blocking abnormal traffic.
- Multifactor Authentication (MFA): Renders shared and stolen passwords useless without access to the second verification factor, protecting against unauthorized access.