Security risk assessment report

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

To mitigate the vulnerabilities identified in the organization's network, the following hardening tools and methods are recommended:

1. **Password Policy Enforcement Tools**
2. **Firewall Configuration and Management Tools**
3. **Multi-Factor Authentication (MFA) Systems**

Part 2: Explain your recommendations

1. **Password Policy Enforcement Tools**

This tool will prevent employees from sharing passwords by enforcing strong, unique credentials across all accounts. It can automatically require password changes at regular intervals and ensure complexity requirements (e.g., minimum length, special characters). This is particularly effective for addressing the shared password and default admin password vulnerabilities.

- **Effectiveness**: Helps prevent unauthorized access due to weak or shared passwords.
- **Implementation Frequency**: Enforced continuously; passwords should be reviewed/updated every 60–90 days.

2. **Firewall Configuration and Management Tools**

   Currently, the organization lacks firewall rules for filtering inbound and outbound traffic. A firewall configuration tool allows administrators to set and maintain robust traffic filtering policies. This protects internal systems from external threats and restricts suspicious data transmissions.

- **Effectiveness**: Blocks unauthorized access, limits data exfiltration, and can log suspicious traffic.
- **Implementation Frequency**: Configurations should be reviewed monthly or whenever significant network changes occur.

3. **Multi-Factor Authentication (MFA) Systems**
   Implementing MFA adds an extra layer of security beyond just usernames and passwords. It requires users to verify their identity with a secondary factor (like a code sent to a mobile device), making it significantly harder for attackers to compromise user accounts.

- **Effectiveness**: Drastically reduces risk of unauthorized access, even if credentials are compromised.
- **Implementation Frequency**: Enforced continuously for all systems, especially those with sensitive data.