Security risk assessment report - Network Hardening

Part 1: Select up to three hardening tools and methods to implement
Based on the identified vulnerabilities in the organization's network, I recommend implementing the following security hardening tools and methods: 1. **Password Policies** 2. **Multifactor Authentication (MFA)** 3. **Firewall Maintenance**

Part 2: Explain your recommendations
1. Password Policies **Description:** Password policies help prevent unauthorized access by enforcing strong authentication practices. The National Institute of Standards and Technology (NIST) recommends using techniques like salting and hashing instead of frequent password changes. **Implementation:** ● Implement a **password manager** for employees to store and retrieve strong, unique passwords. ● Require **minimum password complexity**, such as 12+ characters, a mix of uppercase, lowercase, numbers, and symbols. ● Prohibit **password sharing** through policy enforcement and security awareness training.

- Enable **failed login attempt monitoring** to detect brute-force attacks.

Common Uses:

- Protect against credential stuffing and brute-force attacks.
- Ensure employees follow secure password practices.

2. Multi Factor Authentication (MFA)

Description: MFA adds an extra layer of security by requiring users to verify their identity using two or more authentication methods, such as passwords, OTPs, biometrics, or security tokens.

Implementation:

- Deploy **MFA on all critical systems** (database, employee accounts, admin portals).
- Require employees to use **app-based authentication (Google Authenticator, Microsoft Authenticator)** or **hardware security keys (YubiKey).**
- Implement **adaptive authentication**, which prompts for MFA when logging in from an unknown device or location.

Common Uses:

- Prevent unauthorized access even if credentials are compromised.
- Reduce risk of phishing attacks targeting employee login credentials.

3. Firewall Maintenance

Description: A properly configured firewall protects the network by filtering traffic based on predefined rules, blocking malicious connections, and preventing unauthorized access.

Implementation:

- Define and enforce **strict inbound and outbound traffic rules**.
- Enable **intrusion prevention and detection systems (IPS/IDS)** to monitor unusual activity.
- Regularly **update firewall rules** based on emerging threats and attack patterns.
- Implement **port filtering** to block unnecessary open ports that could be exploited.

Common Uses:

- Mitigate unauthorized network access and data exfiltration.
- Prevent malicious actors from exploiting open ports.