Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Password Management and Policies **Firewall Configuration** **Multi Factor Authentication (MFA)**

Part 2: Explain your recommendations
1. Password Management and Policies **Explanation:** Implementing strong password management and policies is crucial to securing the network. Shared passwords and default admin passwords are significant security risks, as they are easily exploitable by attackers. **Recommendations:** ● **Unique Passwords:** Ensure that every employee has a unique password that is not shared with anyone else. Implement a password manager to help employees generate and store strong, unique passwords. ● **Password Complexity:** Enforce password policies that require a minimum length (e.g., at least 12 characters) and the inclusion of uppercase and lowercase letters, numbers, and special characters. ● **Regular Password Changes:** Require employees to change their passwords regularly (e.g., every 90 days) to reduce the risk of compromised credentials. ● **Default Passwords:** Immediately change any default passwords to strong, unique passwords, especially for critical accounts like the database admin account.

2. Firewall Configuration

Explanation: Properly configured firewalls are essential for controlling and monitoring the traffic entering and leaving the network. Without rules in place, the organization is vulnerable to unauthorized access and potential data breaches.

Recommendations:

- **Traffic Filtering:** Configure firewalls to filter traffic based on IP addresses, protocols, and ports. Only allow traffic that is necessary for business operations and block any suspicious or unauthorized traffic.
- **Intrusion Detection and Prevention Systems (IDPS):** Implement IDPS to monitor network traffic for malicious activities and automatically block detected threats.
- **Regular Audits:** Conduct regular firewall rule audits to ensure that only necessary rules are in place and that outdated or unnecessary rules are removed.

3. Multifactor Authentication (MFA)

Explanation: MFA adds an additional layer of security by requiring users to provide two or more verification factors to gain access to the network. This significantly reduces the risk of unauthorized access, even if passwords are compromised.

Recommendations:

- **Implement MFA:** Require MFA for all employees, especially for accessing sensitive systems and data. This can include a combination of something the user knows (password), something the user has (security token or mobile app), and something the user is (biometric verification).
- **Educate Employees:** Train employees on the importance of MFA and how to use it effectively. Ensure they understand how to handle MFA tokens and what to do if they lose their second-factor device.
- **Continuous Monitoring:** Regularly monitor and review MFA logs to detect and respond to any suspicious activities or attempted unauthorized access.