Security risk assessment report

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

Password Policies

Enforce strict password policies that prevent sharing passwords and ensure all passwords are complex, unique, and regularly updated.

Multifactor Authentication (MFA)

Implement multifactor authentications for all accounts, especially for accessing critical systems and databases.

Firewall Maintenance and Port Filtering

Configure firewalls with specific rules to filter traffic in and out of the network, ensuring that only legitimate and necessary traffic is allowed, and unnecessary ports are closed.

Part 2: Explain your recommendations

1. Password Policies
Effectiveness: Enforcing a strict password policy will prevent employees from sharing passwords and using weak, default, or easily guessable passwords. This significantly reduces the risk of unauthorized access to sensitive systems. By requiring employees to use strong, unique passwords and change them regularly, you can greatly improve the organization's security posture.

Implementation Frequency: This policy should be implemented immediately and revisited regularly (at least once every 6 months) to ensure compliance. In addition, training should be provided to employees to educate them about the importance of strong password management.

2. Multifactor Authentication (MFA)

Effectiveness: MFA adds an additional layer of security by requiring users to provide two or more forms of identification (such as a password and a phone-based authentication code) before accessing systems. Even if an attacker obtains a user's password, they will still need the second factor, significantly reducing the likelihood of unauthorized access.

Implementation Frequency: MFA should be implemented immediately for all critical systems and sensitive data access. It should be reviewed annually to ensure it remains effective and up-to-date with the latest security trends.

3. Firewall Maintenance and Port Filtering

Effectiveness: Configuring and maintaining firewalls with proper filtering rules will help block malicious traffic and unauthorized access attempts to the network. By closing unused or unnecessary ports and allowing only specific types of traffic, firewalls act as a strong barrier to external threats, preventing many common attacks.

Implementation Frequency: Firewalls should be configured and updated immediately. Ongoing maintenance should occur regularly (at least monthly) to ensure that firewall rules are up-to-date and that any new vulnerabilities are mitigated. Routine monitoring should be performed to identify and block any suspicious activity.