Security risk assessment report

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

Multifactor Authentication (MFA) Implementation

- **Explanation**: Implement MFA to add an extra layer of security. MFA requires users to verify their identity using two or more authentication methods. This will mitigate the risk of unauthorized access, especially when employees share passwords.
- **Reasoning**: MFA is effective in preventing unauthorized access even when passwords are compromised. It improves security by requiring additional verification methods besides passwords, such as one-time passwords (OTP), fingerprints, or security tokens.

Firewall Rule Configuration

- **Explanation**: Configure firewall rules to filter incoming and outgoing traffic, stopping unauthorized access and potential attacks. This addresses the issue of firewalls lacking proper traffic filtering rules.
- **Reasoning**: By specifying allowed and blocked traffic based on rules you made, firewall configurations can control network access. This helps in stopping malicious traffic and unauthorized connections.

Password Policy Enforcement

- **Explanation**: Enforce strong password policies, discourage password sharing, and make secure password practices. This addresses the issue of employees sharing passwords and the use of default admin passwords.
- **Reasoning**: Strong password policies as recommended by NIST, improve security by requiring complex and unique passwords. This makes it harder for attackers to guess/brute force passwords.

Part 2: Explain your recommendations

Multifactor Authentication (MFA) Implementation:

- Why is the recommended security hardening technique effective?
  - MFA is effective because it adds a layer of authentication besides just passwords. This makes it harder for attackers to gain unauthorized access even if passwords are compromised. This helps protect sensitive information like customer data.
- How often does the hardening technique need to be implemented?
  - MFA needs to be implemented once for each user account, and any changes or updates to authentication methods should be performed regularly. Especially in response to security best practices and evolving threats.

Firewall Rule Configuration:

- Why is the recommended security hardening technique effective?
  - Configuring firewall rules is effective because it allows organizations to control and monitor incoming and outgoing traffic. By defining specific rules, the firewall can prevent unauthorized access and protect against various types of cyber threats, including those exploiting open ports or vulnerabilities in the network.
- How often does the hardening technique need to be implemented?
  - Firewall rules should be reviewed and updated regularly, particularly when there are changes to the network architecture, services, or emerging threats. Regular maintenance ensures that the firewall remains effective in mitigating potential risks.

Password Policy Enforcement:

- Why is the recommended security hardening technique effective?
  - Enforcing strong password policies helps prevent common security risks associated with weak or shared passwords. By mandating complex and unique passwords, organizations can thwart brute force attacks and enhance overall account security.
- How often does the hardening technique need to be implemented?
  - Password policies should be enforced continuously and reviewed periodically. Updates may be necessary to align with the latest security recommendations and to adapt to evolving threats, making sure that the organization maintains a strong defense against unauthorized access.