Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to address the vulnerabilities found include: 1. Implementing multi-factor authentication (MFA) MFA adds a secondary verification method beyond traditional passwords. Common MFA factors include biometric scans (face I.D., fingerprint), security tokens, ID cards, and time-based PINs. This reduces reliance on passwords alone and helps prevent unauthorized access. 2. Setting and enforcing strong password policies Establishing and enforcing harder password rules like minimum length, character complexity, and limits on reused words to reduce the likelihood of attacks. Policies can also include account lockout mechanisms after multiple failed login attempts to prevent brute-force attacks. 3. Performing firewall maintenance regularly Firewalls should be audited and updated frequently to ensure traffic rules are current and effective. Maintenance includes reviewing access logs, applying security patches, and blocking suspicious IPs or ports to guard against external threats.

Part 2: Explain your recommendation(s)
Add a Multi-Factor Authentication, it adds a critical layer of defense beyond simple credentials. By requiring users to verify their identity through multiple means, MFA significantly decreases the risk of successful brute force and credential stuffing attacks. It also is against password sharing, as the second factor is typically unique to the authorized user. Be sure to add a password policy enforcement ensures that users follow security best practices. Mandating complex passwords, regular updates, and automatic account lockouts after failed login attempts limits the success of dictionary and brute force attacks. These measures collectively enhance the integrity of account access controls. Lastly, firewall maintenance is important for preventing unauthorized network access. Keeping firewall rules updated based on threat intelligence and recent incidents helps reduce exposure to denial of service (DoS) and distributed denial of service (DDoS) attacks. Regular audits ensure that outdated or overly

permissive rules are removed, keeping the perimeter defenses strong.