Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
To address the vulnerabilities identified, the organization can implement the following three hardening tools and methods: Implementing multi-factor authentication (MFA): MFA enhances security by requiring users to verify their credentials through multiple factors before accessing an application. Examples of MFA methods include fingerprint scans, ID cards, pin numbers, and passwords. Setting and enforcing strong password policies: By refining password policies, the organization can promote the use of strong passwords. This can include rules for password length, acceptable character requirements, and disclaimers discouraging password sharing. Additionally, implementing rules for unsuccessful login attempts, such as locking out users after a certain number of failed attempts, further strengthens security. Performing regular firewall maintenance: Regular firewall maintenance involves consistently checking and updating security configurations to proactively address potential threats. This practice ensures that the firewall has effective rules in place to filter incoming and outgoing network traffic, bolstering the organization's overall security posture. By implementing these three hardening tools and methods, the organization can significantly enhance its network security and reduce the risk of future attacks and data breaches.

Part 2: Explain your recommendation(s)
Enforcing multi-factor authentication (MFA) serves as a vital measure to mitigate the risk of unauthorized access through brute force or similar attacks. By requiring multiple forms of verification, MFA significantly raises the barrier for malicious actors attempting to infiltrate the network. Moreover, MFA strengthens internal security by discouraging password sharing within the organization. It is particularly crucial for employees with administrator privileges to undergo rigorous identification and credential verification. To ensure optimal security, MFA should be consistently enforced and regularly reviewed for any necessary

updates.

The implementation of a comprehensive password policy within the organization will play a pivotal role in fortifying network security. Enforcing a password policy that encompasses factors like password length, complexity, and expiration will make it increasingly challenging for malicious actors to compromise user accounts. Regular enforcement of the password policy across the organization is crucial to maintain consistent and robust user security. Additionally, incorporating rules that limit unsuccessful login attempts and implementing lockout measures after a certain number of failed attempts will further enhance security by mitigating brute force attacks.

Regular firewall maintenance is essential to safeguard the network from emerging threats. By conducting routine maintenance, the organization can ensure that firewall rules are up to date and responsive to security events. Prompt updates and adjustments to the firewall rules, particularly in response to suspicious network traffic, are paramount to protect against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. These proactive measures enhance the organization's resilience against potential network-based security incidents.

By implementing and consistently enforcing multi-factor authentication (MFA), a robust password policy, and regular firewall maintenance, the organization can significantly bolster its network security posture and reduce the risk of unauthorized access, data breaches, and potential DoS/DDoS attacks.