Security risk assessment report

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

Multi-Factor Authentication (MFA): Implementing MFA adds an extra layer of security by requiring users to provide two or more forms of verification before granting access. This could involve something the user knows (password), something they have (a smartphone or hardware token), or something they are (biometric data).

Strong Password Policy: Enforcing a strong password policy ensures that users create complex passwords that are difficult to guess. This policy should require a combination of uppercase and lowercase letters, numbers, and special characters. Regular password updates should also be mandated.

Regular Firewall Configuration: Regularly configuring and updating the firewall rules and settings helps prevent unauthorized access to the network. By allowing only necessary traffic and blocking potentially malicious traffic, the firewall acts as a critical defense mechanism.

Part 2: Explain your recommendations

MFA Implementation: Multi-Factor Authentication adds an extra layer of protection by requiring users to provide multiple forms of identification. Even if an attacker manages to obtain a user's password, they would still need the secondary authentication method, which is difficult to replicate. This significantly reduces the risk of unauthorized access.

Strong Password Policy: Requiring strong passwords makes it challenging for attackers to guess or crack them. Complex passwords are less susceptible to dictionary attacks and brute force attempts. Regularly changing passwords prevents the prolonged use of compromised credentials.

Regular Firewall Configuration: Firewalls act as the first line of defense against external threats. Regularly reviewing and updating firewall rules helps ensure that only legitimate traffic is allowed and potential attack vectors are blocked. This continuous monitoring reduces the risk of unauthorized access and data breaches.

By implementing these hardening tools and methods, the organization can significantly enhance its cybersecurity posture, making it more difficult for attackers to exploit vulnerabilities and gain unauthorized access to the system.