Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Implement password policies utilizing NIST  2. Set up Multifactor Authentication  3. Set up firewall rules to filter traffic coming in and out of the network. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. By implementing the NIST password policy, organizations can improve the overall security posture of their systems by promoting the use of stronger passwords, reducing the likelihood of successful brute-force attacks, and encouraging the adoption of additional security measures like MFA. It helps strike a balance between security and usability, considering the limitations and challenges associated with traditional password-based authentication.  2. Multi-factor authentication (MFA) is an effective hardening technique because it adds an extra layer of security beyond just a password. Instead of relying solely on something the user knows (password), MFA incorporates one or more additional factors to verify the user's identity. Even if one factor is compromised, the attacker would still need to bypass or possess the other factors to gain unauthorized access. This technique also prevents credential theft through the means of phishing, keylogging, or data breaches. Many industries and regulatory frameworks require the use of MFA as part of their security standards, so enforcing this would help your organization meet compliance requirements.  3. Setting up firewall rules is an effective hardening technique because it helps secure computer networks by controlling incoming and outgoing network traffic based on predefined rules. They help protect networks by allowing or blocking different types of network traffic based on specific rules. By using firewall rules, organizations can control who can access their network and what kind of data can enter or leave. This prevents unauthorized access, blocks suspicious or harmful traffic, and keeps the network safe from malware and attacks. Firewall rules also allow networks to be divided into separate sections, limiting the impact of any potential breaches. Implementing firewall rules is an important security measure that helps organizations meet compliance requirements and keep their networks secure. |