# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Based on the identified vulnerabilities, I recommend implementing the following hardening tools and methods:   1. Password Policies 2. Network Access Privileges 3. Multifactor Authentication (MFA) |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| **Recommendation 1: Password Policies**  **Why is this technique effective?**  Implementing strict password policies is crucial to mitigate the risk associated with password sharing and weak passwords. Password policies enforce the creation of strong, unique passwords, reducing the likelihood of unauthorized access due to password cracking or guessing attacks. Password policies can include:   * Regular password changes. * Minimum password length and complexity requirements (e.g., including upper and lower case letters, numbers, and special characters). * Prohibition of password reuse. * Avoidance of common passwords.   **Implementation Frequency**  Password policies should be reviewed and updated regularly, at least annually, to ensure they meet current security standards. Password changes should be enforced every 60-90 days, with immediate changes required if a compromise is suspected.  **Recommendation 2: Network Access Privileges**  **Why is this technique effective?**  Configuring network access privileges involves implementing the principle of least privilege (PoLP), which ensures that users have the minimum level of access necessary to perform their duties. This reduces the risk of internal threats and limits the potential damage from compromised accounts. Network access privileges can be enforced through:   * Role-based access control (RBAC), where permissions are assigned based on roles rather than individual users. * Regular audits of access privileges to ensure they are still appropriate. * Removing access immediately when an employee leaves the organization or changes roles.   **Implementation Frequency**  Network access privileges should be reviewed and updated regularly, at least quarterly, to ensure that users only have access to what they need. Immediate updates are required when roles change or when an employee leaves the organization.  **Recommendation 3: Multifactor Authentication (MFA)**  Why is this technique effective?  Multifactor Authentication (MFA) adds an additional layer of security beyond just passwords by requiring users to provide two or more verification factors to gain access. This can include something the user knows (password), something the user has (a smartphone or hardware token), and something the user is (biometric verification). MFA significantly reduces the risk of unauthorized access even if passwords are compromised.  **Implementation Frequency**  MFA should be implemented for all critical systems and accounts immediately. Once implemented, it should be maintained continuously. Periodic testing and updates to the MFA system should be performed to ensure it remains effective and up-to-date with current security practices.  **Summary**  Implementing password policies, network access privileges, and multifactor authentication will effectively address the identified vulnerabilities by strengthening password security, limiting access to sensitive information, and adding an extra layer of authentication. Regular reviews and updates are essential to maintaining the effectiveness of these hardening measures and ensuring ongoing protection against future attacks. |