# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three hardening tools the organization can utilize to address identified vulnerabilities include:   1. Implementing multi-factor authentication (MFA) 2. Setting and enforcing strong password policies 3. Conducting regular firewall maintenance   MFA requires users to verify their identity using multiple methods before gaining access to an application. Some common MFA techniques include fingerprint scans, identification cards, PINs, and passwords.  Password policies can be enhanced to establish rules regarding password length, acceptable character sets, and warnings against sharing passwords. They may also incorporate guidelines on handling failed login attempts, such as revoking network access after five unsuccessful tries.  Regular firewall maintenance involves reviewing and updating security configurations to proactively guard against potential threats. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Enforcing multi-factor authentication (MFA) introduces an extra layer of security beyond just a password. This measure will decrease the chances of a malicious actor gaining access to a network via brute force or similar attacks, as more effort is required to authenticate through multiple methods. Additionally, MFA may deter individuals from sharing passwords. Since anyone receiving a shared password would need extra authentication beyond just that password, MFA renders password sharing less beneficial, thus decreasing the likelihood of shared credentials.  Establishing and enforcing a password policy within the organization will significantly hinder malicious actors from accessing the network. Policies such as locking accounts after a specific number of login attempts can thwart successful brute force attacks. Enhancing password complexity, mandating more frequent password changes, and preventing the reuse of old passwords also serve to impede malicious actors trying to infiltrate the network.  Regular firewall maintenance is essential. Network administrators should verify that firewall rules align with the latest standards for permitted and blocked traffic. Traffic from suspicious sources should be added to a denied traffic list. Firewall rules must be updated whenever a security incident occurs, particularly when an event allows dubious network traffic access. This proactive approach can protect against various DoS and DDoS attacks. |