# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three hardening tools and methods that the organization can implement to address the identified vulnerabilities include:   1. Implementing Multi-Factor Authentication (MFA): MFA requires users to verify their identity using more than one method of authentication before gaining access to an application. This could include fingerprint scans, ID cards, pin numbers, and passwords. 2. Setting and Enforcing Strong Password Policies: Refining password policies to include rules regarding password length, a list of acceptable characters, and discouraging password sharing can enhance network security. Policies could also include rules surrounding unsuccessful login attempts, such as locking network access after a certain number of unsuccessful attempts. 3. Performing Regular Firewall Maintenance: Regularly checking and updating security configurations can help stay ahead of potential threats. This includes setting up rules to filter traffic coming in and out of the network. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Enforcing Multi-Factor Authentication (MFA) will reduce the likelihood of a malicious actor gaining access to the network through a brute force or related attack. MFA also makes it more difficult for people within the organization to share passwords, enhancing overall network security.  Creating and enforcing a strong password policy within the company will make it increasingly challenging for malicious actors to access the network. Regular enforcement of the rules included in the password policy will help increase user security.  Regular firewall maintenance is crucial. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can protect against various DoS and DDoS attacks. |