# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| To address the identified vulnerabilities, the organization can implement the following three hardening tools:   1. **Multi-factor Authentication (MFA)** – MFA adds an extra layer of security by requiring users to verify their identity through multiple methods before gaining access to systems or applications. This can include something the user knows (like a password or PIN), something the user has (such as an ID card or authentication app), or something the user is (like a fingerprint or facial recognition). 2. **Enforcing Strong Password Policies** – Requiring users to create complex passwords and enforcing regular updates helps minimize the risk of credential-based attacks. Policies should include minimum length, a mix of characters, and restrictions against using common or previously used passwords. 3. **Regular Firewall Maintenance** – Conducting routine updates and reviews of firewall configurations ensures that the system continues to block unauthorized access and adapts to evolving threats. Regular audits help identify misconfigurations or outdated rules that could create vulnerabilities. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| **Enforcing Multi-Factor Authentication (MFA):** MFA enhances security by requiring users to authenticate using more than just a password. This significantly reduces the risk of unauthorized access from brute force or similar attacks, as multiple forms of verification are needed. Additionally, MFA discourages password sharing, as possession of a password alone is insufficient to gain access.  **Implementing Strong Password Policies:** A well-defined password policy makes it more difficult for malicious actors to compromise network access. Key measures include locking accounts after repeated failed login attempts, enforcing complex password requirements, mandating regular password changes, and prohibiting password reuse. These practices collectively deter brute force attacks and strengthen user account protection.  **Maintaining and Updating Firewalls:** Regular firewall maintenance is crucial to ensure only authorized traffic enters the network. Administrators should consistently review and update firewall rules to align with current security best practices. Suspicious traffic should be actively blocked, and firewall configurations should be revised following any security incidents. This proactive approach helps defend against various types of DoS and DDoS attacks. |