# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| To address current vulnerabilities, the organization should implement:   1. Multi-Factor Authentication (MFA): Requires multiple forms of verification (e.g., password and fingerprint) to prevent unauthorized access. 2. Strong Password Policies: Enforce rules for password complexity, prevent reuse, and lock accounts after multiple failed login attempts. 3. Firewall Maintenance: Regularly review and update firewall settings to block unauthorized traffic and reduce exposure to threats. | |
|

| **Part 2: Explain your recommendation(s)** |
| --- |
| Enforcing multi-factor authentication (MFA) adds an extra security layer, reducing brute force attacks and discouraging password sharing.  A strong password policy with complexity rules, account lockouts, and regular updates helps prevent unauthorized access.  Regular firewall maintenance, including updated rules to block suspicious traffic, mitigates risks like DoS/DDoS attacks. Keeping rules current after security incidents ensures continued protection. |