# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Three hardening tools to address vulnerabilities include:   1. **MFA (Multi-factor authentication)**: Requires multiple methods, like fingerprints, PINs, or passwords, to verify identity. 2. **Strong password policies**: Define rules for password length, characters, and lock accounts after failed login attempts. 3. **Firewall maintenance**: Regularly update security settings to protect against new threats. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Enforcing **MFA** adds a security layer beyond passwords, making it harder for attackers to gain access and discouraging password sharing, as additional authentication is required.  A **password policy** with account suspension after failed logins, complex passwords, frequent updates, and no reuse helps prevent brute force attacks and strengthens network security.  Regular **firewall maintenance** ensures up-to-date rules for allowed and denied traffic, blocking suspicious sources and protecting against DoS and DDoS attacks. |