# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The hardening tools that the organization can use to address the vulnerabilities are below:   * **Password Policies** * **Implement multi-factor authentication (MFA)** * **Firewall Maintenance**   Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).  A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.  Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Since it has been common practice for users to share passwords with one another and the administrator password being set to default, I recommend the creation, implementation, and enforcement of a uniform password policy. This should include required minimum length and the use of numbers and special characters. Additionally, the policy should include an automatic lock-out if an incorrect password is entered too many times. This will greatly reduce the likelihood of an attacker executing a successful brute-force attack.  Implementation of MFA will prevent users from continuing to participate in the risky practice of password sharing and will ensure that confidentiality is maintained.  Regular firewall maintenance should be implemented by the network security team and reflect the most up to date standards. Firewall rules should be created to block suspicious traffic and deny access to ports that are not in use. Additionally, firewall rules should be updated upon the occurrence of security events in order to maintain the security of the network. |
|  |