# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
|  |
|
| 1) Improving password requirements/Requiring Multi-Factor Authentication (MFA)  2) Firewall Maintenance  3) Penetration Test |

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1) It’s mentioned in the assessment report that: A) The employees of the organization frequently share passwords and B) The admin password for the database is still set to default. The former can be potentially solved by implementing strict password requirements and Multi-Factor Authentication methods. The latter can be solved by setting the admin password to something other than the default. |
| 2) It’s made clear in the assessment report that no rules are in place to filter ingoing or outgoing traffic utilizing a firewall. This might have helped prevent or mitigate the attack that caused the breach to begin with, if implemented correctly and with rules maintained on the regular.  3) A proper penetration test to unveil whether or not there are **even more** security vulnerabilities that exist would help improve security further by hardening the network, and mitigating threats before a potential threat actor discovers them first.   These methods would strongly improve and harden the network security of this organization by making it far more difficult for a threat actor by reducing attack surface overall; it would also prevent employees and others from having access to resources they shouldn’t, by ensuring they only have access to assets they require to complete their day-to-day tasks and responsibilities. |