# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| After organization undergoing latest cyberattack, which leads to data breach, specific vulnerabilities were identified, based on these vulnerabilities, the security analyst recommend network hardening practices which are as follows:  Password policies  Firewall maintenance  Multi Factor Authentication | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Based on given vulnerabilities, security analyst recommended three network hardening tools which are password policies, firewall maintenance and multi factor authentication. Firstly, he recommended a change in password policies to implement strong password by users or admins across organizations, to ensure robust practice and strong security against attacks or a remediation against default passwords. Secondly, he suggested implementing a network hardening method of firewall maintenance, which involves regularly checking and configuring firewalls across the network , as well as adding new or refined rules. Finally, he recommended Multi Factor Authentication solution, for hardening network access points. |