# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The three hardening tools and methods to implement are firewall maintenance, multifactor authentication (MFA) and password policies. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| In this scenario, the social media organization faces significant vulnerabilities, including password sharing among employees, default admin passwords in the database, the absence of firewall rules, and the lack of multifactor authentication (MFA). These vulnerabilities expose the organization to a high risk of data breaches and cyberattacks.  Implementing strong network hardening practices is crucial to mitigate these risks. Firewall maintenance, as the first measure, will allow the organization to enforce access controls, block unauthorized access attempts, and filter incoming and outgoing traffic effectively.  Multifactor authentication (MFA), as the second measure, adds an additional layer of security by requiring multiple forms of verification before granting access. It combats the risk of password sharing and helps safeguard critical systems from unauthorized entry.  Lastly, password policies, as the third measure, will enforce strong password requirements, reducing the likelihood of weak or default passwords being used, and ensuring that MFA is consistently applied throughout the organization.  Together, these measures will significantly enhance the organization's security posture, protect customer data, and decrease the likelihood of future data breaches and cyber threats. |