# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** |
| --- |
| The social media organization suffers vulnerabilities such as : Shared passwords, admin password for the database is set to the default, firewalls do not have rules in place to filter traffic coming in and out of the network, multifactor authentication (MFA) is not used.  Therefore the three hardening tools and methods to implement are:  1. Password Policies.  2. Firewall Maintenance.  3. Multifactor authentication (MFA). |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. 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). These method will curb password sharing and default setting of important password such as; admin database password.  2. Firewall Maintenance can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. This necessitate the firewall rules for incoming and outgoing traffic to be set at all time.  3.Multifactor Authentication (MFA) can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained. |