# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| After reading the Scenario for the Social Media business and current highlights of the security report the three recommendations are below.   1. Disabling unused ports to filter traffic - Implemented at Firewall level, router level and even server level. 2. Multifactor authentication (MFA) - Using third party tools such as authentication apps from Microsoft or from Google. 3. Password policies - Implemented at Server level by Admin creating policy for minimum requirements and policy length if required. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Disabling unused ports to filter traffic to prevent potentially dangerous network traffic from passing through from the firewall and ensure regular maintenance of firewall to stay ahead of potential threats. 2. Multifactor authentication (MFA) - extra security layer for users who access accounts 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. 3. Password policies - Implemented to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (Brute force) which has happened in organization previously and make sure all admin passwords are changed from the default. |