# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Password policies 2. Port filtering 3. Disabling unused ports 4. Firewall maintenance 5. Multi-factor authentication |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. Employees should not be sharing passwords and the admin panel should have a unique password. 2. Control network traffic and limit unwanted communication. 3. Can prevent future attacks on unnecessary opened ports, ports should only opened based on what the organization is using. 4. Firewall rule should always be implemented and updated to respond to an abnormal network traffic, it can be a solid protection against DDoS Attacks. 5. The more ways to identify an authorized user the better this involves using more ways to authenticate users such as passwords, OTP, fingerprint, biometrics, etc. |