# Network Hardening: Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Firewall maintenance 2. Password policies 3. Multifactor authentication |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Firewall maintenance needs to be completed because the organization does not have rules in place to filter network traffic. Having proper firewall rules protects from Denial of Service (DoS) attacks. This needs to be completed regularly to stay up to date with the latest anomalies in network traffic, and can be matched with making sure only the necessary ports are allowed.  Password policies need to be implemented because the organization’s employees share passwords and the admin password for the database is set to the default. Defining password requirements with sufficient length and variance combined with usage of hashing and salt will greatly reduce chances of brute force attacks being successful.  Multifactor authentication should be required considering that proper password policies have not been implemented. Making every employee use multifactor authentication further protects from brute force attacks and helps ensure confidentiality as access to certain assets will be limited to employees who need to see it. Implementing multifactor authentication will only need to be done once and maintenance only requires proper activation, deactivation, and collection of devices. |