|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Firewall Maintenance 2. MFA2 3. Password Policies |
|  |

|  |
| --- |
| **Part 2: Explain your recommendations** |
| During our investigation we found the following issues-   1. The organization’s employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multi Factor authentication (MFA) is not used.   Going forward Password policies need to be put into place or updated. Using MFA and changing password parameters (IE Length, symbols, numbers, sharing of passwords discouraged and time between mandatory password changes). Admin PW should be changed from default password to a secure password.  Firewalls need to have rules set in place that will help with the filtering of traffic in and out of the network. Currently, with no rules set in place, the firewall is essentially nonexistent.  Firewall maintenance should happen regularly. Network administrators should  ensure that firewall rules are in place that reflect the most up to date standards  for allowed and denied traffic. Traffic from sources that are suspicious should be  placed on a denied traffic list. Firewall rules should be updated whenever a  security event occurs, especially an event that allows suspicious network traffic  into the network. This measure can be used to protect against various DoS and  DDoS attacks. |