# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three hardening tools that this organization should implement that address the vulnerabilities found include:   1. Implement MFA 2. Setup password policies 3. Perform regular maintenance on the firewall |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Implementing multi-factor authentication (MFA) adds a layer of security to login credentials that reduce the impact of brute force attacks and make it more difficult for external threats to gain all the information for one login.  Creating and enforcing password policies will make it increasingly more difficult for an attacker to break into the network due to randomization. Additionally, this allows for controls to be put in place to catch suspicious activity, such as many failed login attempts, which further the resiliency of the attack surface. Furthermore, adding password complexity, frequent password updates, and multiple previous passwords for users to prevent re-use allows for social engineering attempts to be more difficult to pull off.  Firewall maintenance should be a regular occurrence for network administrators to ensure proper configurations are in place and baseline trends for traffic flows are being adhered to. This will allow for suspicious activity to be caught before an incident occurs. |