# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Three hardening tools the organization can use to address the vulnerabilities  found include:   * Implementing Password Policies * Implementing Multifactor authentication/MFA * Implementing firewall maintenance   Methods to implement the hardening tools for the organizations:   * Implementing the password policies can be done by several ways:   + Include password rules such as password length, acceptable characters, discourage of password sharing between the employees   + Include counting system for failed login attempts, by doing it when the account reach its failed login attempts limit, the system will block the account immediately to prevent further action of treat actor * Implementing MFA requires users to use more than two ways to identify their credentials such as fingerprint, face recognition, OTP, passwords, etc. * Implementing firewall maintenance checking and updating security configurations regularly to stay ahead of potential threats. To prevent threats by removing outdated or unused software or hardware that do not have the latest security patches or updates. Unpatched devices can allow malicious actors to easily access the network. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| * Implementing the password policies within the organization will make it more difficult for threat actors to gain access to the password of company’s employees and by implementing the password policies it will make the safety or user security increase also will make people between the organizations share passwords or use the default password. * Implementing the MFA will reduce the probability of attack from threat actors such as a brute force or related attack. By implementing the MFA will make password sharing between people of the organization become more difficult because the need to pass the MFA system too. * Implementing the firewall maintenance will update the response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. |