# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** |
| --- |
| Three security hardening methods that can be implemented to address these vulnerabilities include below.<br><br>1.Introducing strong password policies .<br>2.Implementing multifactor authentication.<br>3.Maintaining firewall configurations frequently . |

| **Part 2: Explain your recommendations** |
| --- |
| MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. It will reduce the chance of Brute force attack .Maintenance is not needed for MFA.<br><br>By analysing the vulnerabilities we can see that the employees are less known about security risks .Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).<br><br>Firewall maintenance should be done frequently .Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.<br><br>Apart from all these, conducting a session on cybersecurity events in a regular intervels will help to prevent threats ,up to a certain limit . |