# 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:   1. Port filtering: To implement port filtering, it involves setting rules to control network traffic based on the ports used by applications and services.  Define rules on the firewall or router to allow or deny traffic based on specific ports 2. Setting and enforcing strong password policies: password policies could include setting a minimum password length, Discourage weak passwords and shared passwords 3. Multi-Factor Authentication: Require MFA to add an extra layer of security, making password sharing insufficient for access. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **Enforcing Port filtering** will help restrict access to the network from unwanted access.  **Setting and enforcing strong password policies**: weak passwords are easily exploited. Strong passwords are harder to crack. It reduces the risk of credential stuffing. Enforcing strong passwords ensures compliance and avoids penalties for non-compliance. It minimizes insider threats, that even within the organization, employees cannot easily access accounts or systems they are not authorized to use.  **Enforcing Multi-Factor Authentication** will reduce the likelihood that a malicious actor can access a network through a brute force or related attack since additional effort is required to authenticate in more than one way. It would discourage sharing of passwords as additional authentication beside a password is required. |