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) Enforcing a strong password policy
2) Enforcing Multifactor authentication (MFA)
3) Have port filtering in place and performing firewall maintenance regularly

Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules such as requiring new password within a certain period and not reusing old passwords.

MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords.

Firewall maintenance include checking and updating security configurations regularly to stay ahead of potential threats. Also a rule needs to be added in order to filter ports that can be allowed into the system.

Part 2: Explain your recommendations

Enforcing a strong password policy within the company will make it increasingly challenging for malicious actors to access the network. Due to the fact that the admin password for the database is currently set to the default, this is a vulnerability that would be open to exploit from unauthorized access, such as brute-force attack because someone who previously worked there, could easily guess or remember the password. Therefore, it is important to have a password policy in place, such as requiring new password within a certain period and not reusing old passwords.
Having MFA will also add another layer of security to that access control. Because the employees share passwords, MFA will help tackle this issue. The MFA

is unique to a user, therefore makes it harder for the employees to share passwords, without going through MFA.

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. Port filtering can block and allow certain port numbers to limit unwanted communication. This could also help to minimize risk of getting suspicious traffic into the system. This measure can be used to protect against various DoS and DDoS attacks.