Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

Given that these were the four vulnerabilities discovered:

- The company’s employees' sharing passwords
- The admin password for the database is set to the default
- The firewalls do not have rules in place to filter traffic coming in and out of the network
- MFA is not used

These are the hardening tools that should be implemented:

- Disabling unused ports on the firewalls
- Port filtering
- Firewall maintenance
- MFA
- Network access privileges
- Network log analysis
- Password policies

Part 2: Explain your recommendations

Password policies, MFA, and network access privileges will enforce that employees should not share passwords, and ensure that only the true user is signing in, with only the access they need to perform their job. Network access privileges need to be implemented once, and occasionally revisited. Password policies and MFA can be set up once/any time, and maintained regularly to ensure that users are adhering to guidelines and policies. This also ensures that users with higher privileges will not be vulnerable to brute force attacks.

Disabling unused ports, port filtering, firewall maintenance, and network log analysis all adhere to the goal of defense in depth. These ensure firewalls are filtering unwanted traffic, in case there is an attempted attack that could cause the network to become compromised or unresponsive. These can be implemented and regularly maintained. Network log analysis will be regularly maintained with the implementation of a SIEM tool.