Security risk assessment report

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

A major vulnerability to the organization's network found during inspection is that the admin password for the database is set to default. A password policy is strongly recommended to be put in place to mitigate this risk. Another recommendation is to disable unused ports to have more control over your network traffic. Lastly highly recommend is to implement MFA (Multi-factor authentication).

Part 2: Explain your recommendations

Inspection found that the admin password is set to default and that employees seem to share their passwords frequently. This poses a grave risk to the organization and can be simply mitigated by establishing some aforementioned password policy. This policy would include character requirements, length requirements, and disallow password copies. Following this policy there would be some form of MFA to further add a layer of security and OTP (One time password) use so that threat actors will have a harder time attempting to log in as an employee. Finally during inspection we found that the firewall has not been configured to control traffic in and out of the network. A simple policy to implement to start configuring the firewall is to implement some port filtering. This allows the organization to have more control on what traffic is allowed onto their network by disabling ports that are useless and unnecessary, ultimately reducing the organization's attack surface.