Security risk assessment report

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

Recommended Security Hardening:

- Multifactor Authentication
- Password Policies
- Port Filtering

Part 2: Explain your recommendations

The vulnerabilities discovered in the network include:

- Employees sharing of passwords
- Default admin database password
- No firewall rules for filtering inbound and outbound traffic
- No use of MFA

MFA is recommended to provide an extra security measure when logging in to a secure application or network including the admin database, which would disallow outside intruders from accessing the network or database.

Password policies are recommended to reduce vulnerabilities in credential management. This would prohibit employees from sharing passwords, so only each individual employee knows their password to minimize risk. This would also require a certain password strength so passwords aren’t able to be easily guessed especially for the admin database.

Port filtering is recommended to reduce the available attack surface by disallowing traffic to specific ports, which would make a possible attack more difficult to conduct.