Security risk assessment report

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

1. Multi Factor authentication (MFA)
2. Password policies
3. Firewall maintenance

Part 2: Explain your recommendations

1. The organization doesn't use Multi factor authentication which makes adversaries easier to gain access to their network by breaking into one of the employees accounts. MFA needs to be implemented to check if the correct user is gaining access to their own account. This will prevent brute force attacks.
2. The organization's employees share passwords and the admin's password for the database is set to default. This creates risk for the adversary to gain easy access to the organization's database because everyone knows each other's password and the admin's password is default. The organization needs to follow the password policies set by NIST.
3. The organization's firewall doesn't have set rules to filter out incoming traffic which causes risk for adversaries to send DDoS attacks. Proper firewall rules and maintenance needs to be implemented in order to prevent DDoS attacks and any other unwanted traffic.