Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The hardening tools and methods that can be implemented to safeguard our organizations are as follows. **1)**Firewall maintenance **2)**Configuration checks **3)**Multi Factor authentication (MFA) **4)**Password policies

Part 2: Explain your recommendations
The four major vulnerabilities which were found in the organization's network can be patched with the help of the recommendations provided . As the organization's firewall does not have rules in place to filter the traffic coming in and out of the network, firewall maintenance methods can help to update the existing rules to respond to an event that allows abnormal traffic into the network. This method can be used to protect against DDoS attacks. The admin password for the database is set to default which means any one with the basic knowledge about the database system can access it and tamper with the database. So, Configuration checks must be applied so that the encryption standards for the data stored in the database are up to date, by implementing this we can identify any unauthorized changes made to the system. The multifactor authentication is not used by the organization which may result in compromise of identity as one can access another's account without any verification. By using multi factor authentication like otp, fingerprint, etc.. We can verify users' identity when they are logging in. As there are password sharing among the employees and default passwords being used in the organization by using password policies this will help us to

prevent attackers from easily guessing user passwords, either manually or by using a script (brute force).