Security risk assessment report

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

Three tools organization can use to deal with vulnerability found follows:

1. Implementing and adhering strong password policies
2. Implementing Multi Factor Authentication (MFA)
3. Maintaining Firewall regularly and adding proper port filtering

Password policies should implement rules based on NIST password standards and should also add rules on maximum attempt for wrong password. Password sharing should be discouraged.

To strengthen authentication, MFA should be implemented to accurately identify before accessing services. It could include Id card, face id, fingerprint scan, OTP etc.

Firewall should be maintained properly to protect the network from potential threats.

Part 2: Explain your recommendations

Strengthening password policies will make it extremely hard for malicious threat actors to guess passwords and gain access to the network. The maximum number of login attempts will increase safety from brute-force attacks. Changing passwords frequently and not using old passwords will make it even harder for malicious actors to harm the company.

Implementing Multi-Factor Authentication will add an additional layer of security to the already implemented passwords. It will make it even harder for malicious actors to perform brute-force attacks or other attacks to gain access to the network. It will also reduce password sharing as people will need an additional way to verify besides passwords.

Firewall rules should be properly configured to allow only trusted traffic and deny potentially suspicious traffic. It should also be maintained regularly to ensure it is updated to new types of suspicious activities. It should also be updated if new incidents occur. It will help keep our network safe from potential DoS and DDoS attacks.