Security risk assessment report

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

The following hardening tools and methods should be implemented:

1. Setting and enforcing strong password policies.
2. Implementing Multi Factor Authentication(MFA).
3. Performing Firewall Maintenance regularly.

Strong passwords (includes special characters, numbers, alphabets in uppercase and lowercase, password length should be 8, etc.) should be implemented in order to change the default passwords and make it unpredictable by the attacker. Limiting login attempts should be implemented.

MFA should be implemented so that at least 1 more factor is needed for login except the password. Factors like fingerprint scans, OTP, pin numbers, ID cards etc. can be used.

Firewall configuration should be done. Specific rules should be set for incoming and outgoing traffic. It should monitor the traffic and block malicious traffic.

Part 2: Explain your recommendations

Strong password policies like having a password length of 8 characters, numbers, special characters, uppercase and lowercase alphabets should be used to make the password unpredictable and hence preventing brute force attack. Login attempts for the user can also be restricted to 5, to restrict malicious logins. Passwords can be kept using hash and salt, to stop enforcing frequent changes to passwords. Adding extra characters to the password and making it unreadable by the humans is called hashing and to make each hashes unique salt is added. This process can help in the integrity of the password.

Multi Factor authentication should be applied so that the account remains protected because other than the password another factor will be needed to enable login, which can only be given by the authenticated user as the 2nd factor includes biometrics, ID cards, Pin numbers, OTP given on the connected mobile or user account, which are generally not present to the attacker.

Firewall maintenance should happen regularly. Network administrators should ensure that firewall rules are in place that reflect the most up to date standards for allowed and denied traffic. Traffic from sources that are suspicious should be placed on a denied traffic list. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.