Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Password policies - Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).

Part 2: Explain your recommendations
Implementing strong password policies is a critical step in hardening systems against unauthorized access. Weak or reused passwords are common attack vector exploited through brute-force attacks, credential stuffing, and password spraying. By enforcing rules such as: - Minimum password length and complexity - Blocking reuse of previous passwords - Mandatory periodic password changes - Limiting login attempts ...the organization can significantly reduce the chances of attackers successfully guessing valid credentials. This policy also encourages user accountability and sets a standard baseline for credential hygiene across the enterprise. When paired with multi-factor authentication and user training, password policies from the foundation of access control in a secure environment.