Security risk assessment report

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

1. Password Policies.
   Setting minimum password length, complexity rules (uppercase, lowercase, numbers, symbols), and expiration periods.
2. Firewall Maintanance
   Regularly reviewing and updating firewall rules to match current network needs and security policies.
3. MFA authentication
   Choosing MFA factors such as passwords, OTPs (via SMS or authenticator apps), hardware tokens, or biometrics.

Part 2: Explain your recommendations

1. Password policies are designed to prevent attackers from easily guessing credentials, whether manually or through automated scripts. These policies often require passwords to be longer than eight characters and include a mix of uppercase and lowercase letters, numbers, and symbols.
2. Firewall maintenance involves regularly updating and reviewing firewall rules to ensure they remain current and effective in controlling network traffic. This helps block unauthorized access, mitigate DDoS attacks, and implement port filtering to manage which network traffic is allowed or denied.
3. Multi-Factor Authentication (MFA) is a security measure that requires users to verify their identity using two or more authentication methods before accessing a system or network. This could include a password, PIN, security badge, one-time password (OTP), fingerprint, or other methods. MFA significantly reduces the risk of brute force and similar types of attacks.