Security Risk Assessment Report

Part 1: Select up to three hardening tools and methods to implement
Implement Strong Password Policies ● Enforce unique, strong passwords for all accounts. ● Require employees to create complex passwords using a mix of letters, numbers, and special characters. ● Prohibit password sharing and enforce periodic password changes. Enable Multi Factor Authentication (MFA) ● Require employees and administrators to verify their identity with both a password and an additional factor, such as a one-time passcode (OTP) sent to their email or phone, or a biometric scan. Configure Firewall Rules ● Establish firewall rules to filter inbound and outbound traffic. ● Block unauthorized access attempts and restrict traffic to only trusted sources and protocols. ● Implement logging and monitoring to track suspicious activity.

Part 2: Explain your recommendations
Sharing passwords and using default credentials create a significant security risk. Enforcing strong password policies ensures that each user account is protected individually. This eliminates vulnerabilities caused by shared or weak passwords. MFA adds an essential layer of security by requiring a second authentication factor. Even if a password is compromised, the attacker cannot access the account without the additional factor. This significantly reduces the likelihood of unauthorized access to sensitive systems and databases.

A lack of firewall rules allows unrestricted access to the network, making it vulnerable to attacks. Configuring firewalls to filter traffic prevents unauthorized connections and blocks malicious data packets. Monitoring traffic logs helps identify and respond to suspicious activity, enhancing overall security.