Security Risk Assessment Report

Part 1: Selected Network Hardening Tools and Methods

1. Multi-Factor Authentication (MFA)
2. Strong Password Policies
3. Firewall Rule Configuration

Part 2: Explanation and Recommendations

1. Multi-Factor Authentication (MFA):
Implementing MFA adds a critical layer of protection by requiring users to verify their identity in more than one way—such as with a mobile code or biometric verification—in addition to their password. This helps prevent unauthorized access, even when passwords are compromised, which is a common scenario in phishing or credential reuse attacks. MFA should be rolled out company-wide and reviewed at least annually, or anytime user access policies are updated.

2. Strong Password Policies:
Weak or shared passwords significantly increase the risk of unauthorized access. By enforcing strong password policies—such as requiring complexity, expiration, and preventing reuse—we can reduce this risk across the organization. For high-privilege accounts like database administrators, unique and complex credentials should be mandatory. Password policy enforcement should be ongoing using directory services or group policy, and the policy itself should be reviewed every 90 days.

3. Firewall Rule Configuration:
Firewalls act as the first line of defense in blocking unwanted or malicious traffic. Without specific rules in place, all network traffic is treated equally—leaving the system vulnerable. By configuring rule sets based on business needs, such as only allowing specific protocols or ports, we can better control the flow of network traffic. Firewall rules should be reviewed on a monthly basis and immediately after any security incident or significant network change.