Security risk assessment report

Part 1: Network Hardening Methods
In response to the vulnerabilities identified in the organization's network, I recommend implementing the following network hardening tools and methods: **1. Multi-factor Authentication (MFA)** – This prevents unauthorized access even if passwords are weak or shared, as attackers will need a second form of verification. **2. Firewall Maintenance and Port Filtering** – Regular updates to firewall rules and filtering unused or vulnerable ports can significantly reduce exposure to external threats and limit inbound/outbound malicious traffic. **3. Strong Password Policies** – Enforcing strong password creation, disabling default passwords, and using hashed/salted storage mechanisms help protect against brute force attacks and insider misuse. These techniques directly address the key vulnerabilities found in the organization's environment and can be enforced with minimal disruption to operations.

Part 2: Explain your recommendations
Multi-factor Authentication (MFA) is highly effective because it ensures that even if a password is compromised, access to the network is still blocked without a second verification step. This drastically reduces the chance of a successful unauthorized login. MFA should be implemented immediately and maintained consistently. **Firewall Maintenance and Port Filtering** limit the attack surface by controlling what traffic is allowed in or out of the network. Regular firewall audits and port filtering help identify vulnerabilities and block unauthorized access. This should be performed weekly or monthly, depending on traffic patterns and threats. **Password Policies** aligned with NIST standards prevent weak or shared password usage. Replacing default credentials and enforcing strong authentication practices drastically reduce risk from brute force and credential stuffing attacks. These policies should be enforced on all new users and reviewed quarterly.