Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
After discovering these 4 vulnerabilities in the organization's network: 1. The organization's employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multifactor authentication (MFA) is not used. The 3 hardening tools and methods I suggest implementing are: 1. Strong password policies and using Multifactor Authentication (MFA) 2. Tighten Role-Based Access Control (RBAC) and network access privileges 3. Conduct firewall maintenance regularly

Part 2: Explain your recommendations
Implementing strong password policies that enforce complexity, (e.g. requiring passwords to be at least 12 characters long, a mix of uppercase letters, lowercase letters, numbers, and special characters) can significantly reduce the risk of brute-force attacks. Additionally, policies should lock user accounts after a specified number of failed login attempts (e.g., 5 unsuccessful tries), which prevents brute-force attacks from continuing indefinitely. It's also crucial to prevent password reuse by enforcing that passwords cannot be reused within a specified time frame (e.g., six months) and requiring employees to update their passwords every 90 days. Multifactor Authentication (MFA) brings additional layer of security by requiring users to verify their identity through multiple methods. This could include passwords, PINs, biometrics (like fingerprint or facial recognition), or security tokens. MFA is effective because even if a password is compromised or shared, the attacker would still need access to the second form of authentication, making it much harder for unauthorized users to gain entry.

Role-Based Access Control (RBAC) limits employees' access to only the resources they need for their jobs, following the principle of least privilege. This reduces the overall impact of password sharing by ensuring that, even if credentials are shared, the unauthorized person will not gain access to sensitive systems or information beyond what is needed for the original user's role.

Network access privileges further limit exposure by controlling who can access different parts of the network, databases, or other critical systems. By tightening access controls, the organization can restrict access to sensitive areas (like the admin account for the database), ensuring that only specific roles, like system administrators, have the necessary permissions.

Firewall maintenance ensures it can detect unusual patterns or access attempts that may indicate password sharing or compromised credentials, especially if someone is trying to access the system from untrusted locations. By updating the firewall rules, the organization can block malicious traffic, detect anomalies, and prevent external access to systems that may still have vulnerabilities (e.g., unpatched or default passwords). After a security event or a major system update, the firewall should be reviewed to ensure that new vulnerabilities are not exposed.

As an additional measure, maintaining a baseline configuration provides a secure starting point for all systems. This includes ensuring that default passwords are changed, unnecessary services are disabled, and critical security settings (e.g., encryption standards, firewall rules) are uniformly applied across all systems. The baseline should be reviewed quarterly and updated after significant events, such as a security incident or patch release. By regularly auditing and refining the baseline configuration, the organization ensures compliance with evolving industry standards (e.g., NIST, ISO). Furthermore, having a baseline allows the organization to quickly identify deviations from secure configurations, which is crucial in responding to incidents rapidly and minimizing downtime.