# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| As a security analyst responding to the recent data breach at the social media organization, the most effective way to strengthen the organization's network and prevent future attacks is by implementing **network hardening techniques**.  I recommend the following two **primary hardening practices**:   1. **Implementing Strong Access Controls with Multifactor Authentication (MFA)** 2. **Configuring and Enforcing Firewall Rules**  **Why these are effective:**  1. **Multifactor Authentication (MFA):**     * **Effectiveness:** MFA adds an extra layer of protection beyond just a username and password. Even if a password is compromised (due to password sharing or brute-force attacks), the second factor (such as a code sent to a mobile device) significantly reduces the chances of unauthorized access.    * **Implementation Frequency:** MFA should be enforced across all accounts, especially admin accounts, and reviewed quarterly to ensure it's functioning and applied consistently across the organization. 2. **Firewall Rule Configuration:**     * **Effectiveness:** Firewalls serve as a critical barrier between internal and external networks. Without proper inbound and outbound traffic filtering, attackers can easily scan, exploit, and exfiltrate data from the network.    * **Implementation Frequency:** Firewall rules should be set based on the principle of least privilege (only allow what is necessary) and reviewed monthly or after any major network changes.   These practices reduce the surface area for attacks and help contain any intrusion that might still occur. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **Vulnerability 1: Password Sharing Among Employees**  * **Risk:** Shared passwords can be misused or leaked. There’s no way to track accountability. * **Mitigation:** Enforce **individual login credentials** and **user-specific access controls**. Use **password management tools** and enforce **strict password policies** (minimum length, complexity, expiration).  **Vulnerability 2: Default Admin Password**  * **Risk:** Default passwords are widely known and can be exploited easily. * **Mitigation:** Change **all default passwords immediately**. Implement **password complexity requirements** and **periodic credential audits**.  **Vulnerability 3: No Firewall Rules**  * **Risk:** Without filtering, any system can communicate in or out, increasing exposure to attacks like DDoS, malware, and data exfiltration. * **Mitigation:** Create **firewall rules** to limit traffic by IP address, port, and protocol. Apply **intrusion detection and prevention systems (IDPS)** for added monitoring.  **Vulnerability 4: No Multifactor Authentication**  * **Risk:** Single-factor authentication is easily bypassed with stolen credentials. * **Mitigation:** Deploy **MFA organization-wide**, especially for privileged accounts and remote access. Integrate it with directory services like LDAP, SSO, or Active Directory. |