Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

To strengthen the organization’s network security and address identified vulnerabilities, the following three measures are recommended:

1. **Multi-Factor Authentication (MFA)**
2. **Robust Password Policies**
3. **Regular Firewall Maintenance**

Multi-Factor Authentication (MFA) requires users to verify their identity using multiple methods before gaining access to applications. Common MFA methods include fingerprint scans, ID cards, PIN codes, and passwords. By requiring more than one form of authentication, MFA adds a critical layer of protection against unauthorized access.

Strong Password Policies ensure that user credentials are more resilient to attacks. These policies can enforce rules regarding minimum password length, acceptable characters, and measures to discourage sharing. Additionally, they can include security measures such as temporarily locking accounts after multiple failed login attempts, requiring regular password updates, and preventing password reuse.

Firewall Maintenance involves continuously reviewing and updating firewall configurations to defend against potential threats. Keeping firewall rules up-to-date ensures that only authorized traffic is allowed and that suspicious or malicious traffic is blocked effectively.

Part 2: Explain your recommendations

Multi-Factor Authentication (MFA) significantly reduces the risk of unauthorized access. Even if a password is compromised, an attacker cannot access the network without the additional authentication factor. MFA also discourages password sharing, since the second factor cannot be easily replicated or shared.

Strong Password Policies create additional hurdles for attackers. Locking accounts after multiple failed login attempts prevents brute-force attacks, while complex and regularly updated passwords make it more difficult for malicious actors to gain access. Preventing password reuse further enhances overall security by reducing predictable vulnerabilities.

Firewall Maintenance is crucial to network defense. Administrators must ensure firewall rules are aligned with the latest security standards, blocking traffic from suspicious sources and allowing only trusted communications. Rules should be updated in response to any security events, especially when unusual traffic is detected. Proper firewall maintenance protects against a range of attacks, including Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attempts.