Security risk assessment report

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

The organization can employ three security enhancement tools to mitigate identified vulnerabilities:

1. Implementation of Multi-Factor Authentication (MFA):
MFA mandates that users verify their identity through multiple methods before gaining access to an application. These methods encompass fingerprint scans, ID cards, PIN numbers, and passwords.

2. Establishment and Enforcement of Robust Password Policies:
Password policies can be enhanced by specifying criteria like password length, acceptable character sets, and including disclaimers discouraging password sharing. Additionally, rules addressing unsuccessful login attempts can be incorporated, such as locking a user out of the network after five unsuccessful tries.

3. Regular Firewall Maintenance:
Firewall maintenance involves periodic assessment and updates to security configurations, ensuring proactive defense against potential threats.

Part 2: Explain your recommendations

Implementing multi-factor authentication (MFA) not only reduces the likelihood of unauthorized network access through brute force attacks but also enhances internal security by discouraging password sharing within the organization. This heightened level of identity verification is particularly crucial for employees with administrator privileges, making regular MFA enforcement imperative.

The institution of a comprehensive password policy serves as a robust defense against malicious actors attempting to infiltrate the network. Consistent enforcement of these policy rules within the organization enhances user security and raises the bar for potential attackers.

Regular maintenance of the firewall is essential. Updating firewall rules in response to security incidents, especially those permitting suspicious network traffic, is critical for safeguarding against various types of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.