Security risk assessment report

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

Three hardening tools the organization can use to address the vulnerabilities found include:

1. Implementing multi-factor authentication (MFA)
2. Setting and enforcing strong password policies
3. Performing firewall maintenance regularly

MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords.

Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts.

Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendation(s)

Enforcing multi-factor authentication (MFA) can significantly reduce the risk of malicious actors gaining network access through brute force or related attacks. Additionally, MFA serves as a deterrent against internal password sharing among organizational members, especially among those holding administrator-level privileges on the network. Regular enforcement of MFA is crucial for sustained security measures.

Establishing and rigorously enforcing a comprehensive password policy within the company significantly raises the bar for malicious actors attempting to infiltrate the network. Regular enforcement of these password policy rules throughout the organization is essential to bolster user security.

Regular maintenance of firewalls is imperative. Updating firewall rules promptly following any security incidents, particularly those permitting suspicious network traffic, is crucial. This practice acts as a proactive defense against a spectrum of DoS and DDoS attacks.