Security risk assessment report

Part 1: Hardening Tools and Methods to Implement

To address the identified vulnerabilities, the organization can utilize three effective hardening tools:

1. Implementing multi-factor authentication (MFA)
2. Enforcing strong password policies
3. Performing regular firewall maintenance

MFA adds an extra layer of security by requiring users to provide multiple forms of identification and verification, such as passwords, fingerprints, or ID cards, before accessing the network. This method helps mitigate the risk of brute force attacks and discourages password sharing. Regular enforcement of MFA is necessary to maintain its effectiveness.

Enforcing strong password policies involves implementing rules regarding password length, acceptable characters, and discouraging password sharing. Additionally, setting limitations on unsuccessful login attempts, such as account lockouts after a certain number of failed attempts, enhances network security. Regular enforcement of these policies within the organization is crucial to reinforce user security.

Regular firewall maintenance is essential to keep up with evolving threats. By regularly checking and updating security configurations, the organization can stay ahead of potential attacks. Firewall rules should be promptly updated in response to security events, particularly those that allow suspicious network traffic. This measure effectively safeguards against various types of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Part 2: Reasoning Behind the Recommendation(s)

Enforcing multi-factor authentication (MFA) significantly reduces the likelihood of unauthorized access to the network, particularly through brute force or related attacks. MFA also serves as a deterrent against password sharing within the organization. It is crucial to regularly enforce MFA to maintain its effectiveness and protect the network.

By implementing and enforcing a strong password policy, the organization raises the difficulty for malicious actors to breach the network. Password policies encompassing rules on length, characters, and discouraging password sharing enhance overall security. Regular enforcement of these policies within the organization is vital to reinforce user security and protect against unauthorized access.

Regular firewall maintenance is necessary to proactively address emerging threats. By promptly updating security configurations and firewall rules, the organization can stay resilient against potential attacks. This measure is particularly effective in defending against DoS and DDoS attacks. Regular maintenance ensures that the firewall remains up-to-date and can adapt to evolving security challenges.

Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. The rules that are included in the password policy will need to be enforced regularly within the organization to help increase user security.

Firewall maintenance should happen regularly. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.