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 enhances security by requiring users to authenticate their credentials through multiple means before accessing an application. Methods may include fingerprint scans, ID cards, PIN numbers, and passwords. By implementing and enforcing robust password policies, organizations can enhance security. These policies should specify password length, acceptable characters, and discourage password sharing. Additionally, rules regarding unsuccessful login attempts can be established, such as restricting access after a certain number of failed attempts. Consistent monitoring and updating of firewall configurations are essential to stay ahead of potential threats. Regular maintenance ensures that the firewall is effectively safeguarding the network by identifying and blocking unauthorized access attempts.

Part 2: Explain your recommendation(s)
Enforcing multi-factor authentication (MFA) serves as a robust defense against unauthorized access attempts, including brute force attacks. By requiring multiple forms of verification, MFA not only deters malicious actors but also discourages password sharing within the organization. Particularly for employees with elevated privileges like administrators, verifying credentials through MFA is crucial. Regular enforcement of MFA policies is essential to uphold network security standards. Establishing and upholding a stringent password policy is vital for fortifying network security. Enforcing password complexity rules and regular updates within the organization heightens the difficulty for malicious entities attempting unauthorized access. Regular enforcement of password policies ensures consistent user security standards.

Regular firewall maintenance is imperative to network security. Updating firewall rules promptly in response to security events, especially those involving suspicious network traffic, bolsters defense against potential Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. This proactive measure reinforces network security resilience against evolving threats.