Security risk assessment report

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

Three hardening tools the organization can employ to address the vulnerabilities found are:

Implementing multi-factor authentication (MFA): MFA necessitates users to verify their credentials through multiple means before accessing an application. This could involve methods such as fingerprint scans, ID cards, pin numbers, and passwords, enhancing the security of user authentication.

Setting and enforcing strong password policies: Password policies can be strengthened by specifying rules regarding password length, acceptable character sets, and discouraging password sharing through disclaimers. Additionally, implementing rules to restrict network access after a set number of unsuccessful login attempts can enhance security against brute force attacks.

Performing firewall maintenance regularly: Firewall maintenance involves regularly reviewing and updating security configurations to proactively mitigate potential threats. By staying vigilant and keeping firewall settings up-to-date, organizations can better defend against unauthorized access and malicious activities.

By implementing these hardening tools, the organization can significantly bolster its cybersecurity posture and mitigate the identified vulnerabilities effectively.

Part 2: Explain your recommendations

Enforcing multi-factor authentication (MFA) will reduce the likelihood that a a malicious actor can access a network through a brute force or related attack. MFA will also make it more difficult for people within the organization to share passwords. Identifying and verifying credentials is especially critical among employees with administrator level privileges on the network. MFA should be enforced regularly.

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.