Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening methods the organization can implement to address the vulnerabilities found are the following: 1. **Performing Firewall maintenance regularly**: Firewall maintenance entails checking and updating security configuration regularly to stay ahead of potential threats. 2. **Implementing Multi Factor authentication (MFA):** it requires users to verify their identity in two or more ways to access a system or a network. MFA options include passwords, pin number, badge, one-time password (OTP) set to a cell phone, fingerprint, and more. 3. **Enforcing strong Password policies:** Password policies can include guidelines on password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They may also define rules for handling unsuccessful login attempts, such as locking the user out of the network after five failed attempts.

Part 2: Explain your recommendations
Regular firewall maintenance is crucial. Network administrators should ensure that firewall rules are up to date and reflect the latest standards for allowed and denied traffic. Traffic from suspicious sources should be added to a deny list. Firewall rules should be reviewed and updated after any security incident, particularly those that involve suspicious network traffic. This proactive approach can help protect against various DoS and DDoS attacks. Enforcing multi-factor authentication (MFA) adds an extra layer of security beyond just a password. It reduces the likelihood of a malicious actor gaining network access through brute force or similar attacks, as additional authentication steps are required. MFA also discourages password sharing, as the person receiving the shared password would still need to provide another

form of authentication, making password sharing less effective.

Establishing and enforcing a strong password policy within the company can further protect the network from unauthorized access. Policies like locking accounts after a certain number of failed login attempts can prevent successful brute force attacks. Additionally, requiring complex passwords, enforcing regular password updates, and prohibiting password reuse can make it more difficult for malicious actors to breach the network.