Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three tools the organization can use to fix the vulnerabilities are: 1. Using multi-factor authentication (MFA) 2. Enforcing strong password rules 3. Regularly maintaining firewalls MFA requires users to verify their identity in more than one way before accessing an application. This can include fingerprint scans, ID cards, PIN numbers, and passwords. Password rules should include guidelines about password length, acceptable characters, and discouraging password sharing. They can also include locking the user out of the network after five failed login attempts. Firewall maintenance involves regularly checking and updating security settings to prevent potential threats.

Part 2: Explain your recommendations
Implementing multi-factor authentication (MFA) adds extra security beyond just using a password. This makes it harder for hackers to break into the network through brute force or similar attacks since they need more than just the password. MFA also discourages password sharing because even if someone shares their password, the recipient would still need the additional authentication to access the network. Creating and enforcing a strong password policy helps keep the network secure. Policies can include suspending an account after a certain number of failed login attempts to prevent brute force attacks. Requiring complex passwords, frequent updates, and preventing password reuse also make it

more difficult for hackers to gain access.

Regular firewall maintenance is crucial. Network administrators should ensure firewall rules are up-to-date and reflect the latest standards for allowed and denied traffic. Suspicious traffic should be blocked, and firewall rules should be updated after any security event, especially those allowing suspicious traffic. This helps protect against various types of attacks, including DoS and DDoS attacks.