Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Hardening tools the organization can use to address the vulnerabilities found include: 1. Implementing multi-factor authentication (MFA) 2. Setting strong password policies 3. Performing firewall maintenance MFA requires users to use more than one form of authentication before accessing an application. MFA can include face recognition, fingerprint, one time password, pin number or ID cards. Password policies can be set to include the rules regarding password length, a list of required characters like number, small letters, big letters or special characters. Also passwords should not be common words or variations of them. In addition user passwords stored in the database should be salted and than hashed. Firewall maintenance entails updating the security configurations regularly.

Part 2: Explain your recommendations
Enforcing multi-factor authentication (MFA) will reduce the likelihood that a thread actor can access the company infrastructure through brute force attack. MFA will also make it more difficult for employees to share passwords. Creating and enforcing the strong password policy within the company will make it challenging for malicious actors to access the network. Also implementing the salting and hashing passwords will make it practically impossible or ineffective to decode the users passwords. Firewall maintenance should happen regularly. Firewalls should be updated whenever a security event occurs, especially an event that allows the suspicious network traffic into the network.