Security Risk Assessment Report

Part 1: Select up to three hardening tools and methods to implement
Organization should consider use of: 1. Multi-factor authentication (MFA) - MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords. 2. Setting and enforcing strong password policies - password policies should be refined with proper length, a list of acceptable characters, and a forbidden password sharing. The unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts should be also implemented. 3. Performing regular firewall maintenance - it entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Requiring multi-factor authentication (MFA) significantly diminishes the chances of an unauthorized user breaching a network through brute force or similar methods. Not only does MFA deter external threats, but it also discourages internal personnel from sharing their credentials. This is particularly vital for staff with administrator access. Consistent enforcement of MFA is paramount. Establishing and upholding a robust password policy augments the defenses against potential external intruders. For the policy to be effective, it must be diligently implemented and monitored throughout the organization, bolstering user security. Routine maintenance of firewalls is non-negotiable. Anytime a security incident arises, especially those that permit questionable traffic, firewall configurations should be revised. Such practices aid in defending against a range of DoS and DDoS assaults.