Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Multi-factor Authentication - 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. Strong password policies - include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts. 3. Port Filtering - entails checking and updating security configurations regularly to stay ahead of potential threats through firewall maintenance.

Part 2: Explain your recommendations
By implementing multi-factor authentication (MFA), the risk of malicious actors gaining unauthorized access to the network through brute force or related attacks can be significantly reduced. MFA also serves as a deterrent against password sharing within the organization, particularly among employees with administrative privileges. Regular enforcement of MFA is crucial for maintaining security. To enhance network security further, it is essential to establish and uphold a robust password policy throughout the company. The password policy should include stringent rules and should be consistently enforced across the organization to bolster user security. Frequent maintenance of the firewall is paramount. Updating firewall rules promptly, especially after security events that permit suspicious network traffic, provides protection against various DoS and DDoS attacks. This proactive measure helps safeguard the network from potential threats.