Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Here are three tools that the organization can employ to address the identified vulnerabilities: Implementation of Multi-Factor Authentication (MFA): MFA requires users to utilize multiple methods for identifying and verifying their credentials prior to accessing an application. Various MFA approaches encompass fingerprint scans, ID cards, PIN numbers, and passwords. By adopting MFA, potential unauthorized users would encounter significant challenges in their attempts to breach the system. Enforcement of Robust Password Policies: Strengthening password policies involves setting and enforcing stringent guidelines. These guidelines could encompass password length, acceptable character combinations, and disclaimers discouraging password sharing. Moreover, the policies might incorporate provisions related to unsuccessful login attempts, such as locking out users from the network after a designated number of failed tries. Regular Firewall Maintenance: Consistently performing firewall maintenance entails regular assessment and updating of security configurations. This proactive measure ensures that the organization remains well-prepared against potential threats. By staying ahead of emerging risks, the organization can maintain an effective defense posture. Incorporating these hardening tools will fortify the organization's security posture and enhance its ability to counter vulnerabilities effectively.

Part 2: Explain your recommendations
By implementing multi-factor authentication (MFA), the likelihood of malicious actors gaining unauthorized access to a network through methods like brute force attacks is substantially reduced. MFA also acts as a deterrent against password sharing within the organization. This is particularly crucial for individuals holding administrative privileges within the network. Regular and consistent enforcement of MFA policies is essential to its effectiveness. The establishment and enforcement of a comprehensive password policy within the company will significantly heighten the difficulty for malicious actors attempting to infiltrate the network. The stipulations laid out in the password policy need to be consistently upheld across the organization to bolster user security. Regular and routine maintenance of the firewall is imperative. The timely updating of firewall rules becomes especially crucial in response to security incidents, particularly those that allow potentially harmful network traffic into the system. This proactive approach serves as a protective measure against various types of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.