Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
After examining the organization's network, four significant vulnerabilities were discovered. To address these vulnerabilities, it is necessary to implement these hardening tools and methods: - Setting up password policies - Multifactor authentication (MFA) - Performing firewall maintenance

Part 2: Explain your recommendations
By regularly checking and updating firewall security configurations, implementing multi-factor authentication (MFA), and enforcing strong password policies, you can stay ahead of potential threats and protect against brute force attacks and similar security events. MFA can be set up once and maintained to provide an additional layer of security, while password policies make it harder for attackers to guess user passwords, whether through manual attempts or automated scripts used in brute force attacks. Together, these measures help safeguard your system from unauthorized access and mitigate the risk of data breaches and other security breaches.