Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools that can be used to address the vulnerabilities found are: - Multi Factor Authentication - Setup Firewalls - PAssword Policies MFA requires you to provide other forms of verification like personal information about you or biometric scans Firewall maintenance includes checking and updating firewalls to ensure they meet the standards of protection required by the organization Password policies help provide a set of guidelines to prevent simple passwords from being predicted through brute force attacks

Part 2: Explain your recommendations
Password policies should be put in place since all employees all use the same default passwords. This provides risks as if the password is breached all devices on the network will be put at risk. Appropriate password policies will ensure passwords are difficult to breach and if one password is retrieved it does not affect others. This can be implemented immediately by ensuring all new passwords are setup with specific requirements being met Multi Factor authentication adds an extra layer to the previously discussed and is effective as it provides multiple layers of security if a breach occurs. It can be implemented at anytime making it a quick and efficient way to provide immediate necessary protection