Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Implement and enforce strong password policies. 2. Conduct regular firewall maintenance. 3. Implement Multi Factor Authentication (MFA) Strong password policies can include rules regarding password length and complexity, acceptable characters, how often users are required to change their passwords and a disclaimer to discourage password sharing. They can also include rules regarding unsuccessful login attempts, such as locking a user account after five unsuccessful attempts. Firewall maintenance enables security teams to regularly check and update security configurations and rules to stay ahead of potential threats. MFA requires users to verify their identity in two or more ways to access a system network. This can be via a one-time passcode sent to a device, a biometric scanner to check fingerprint data and more.

Part 2: Explain your recommendations
Enforcing strong password policies will prevent users from selecting weak passwords which can be easily guessed or brute forced via a dictionary attack. Additionally, enforcing an account lockout policy after several failed attempts will add to this resilience. Conducting regular firewall maintenance will allow security teams to regularly update rules and configurations in line with the current threat landscape. This measure can be used to protect against DoS and DDoS attacks. Implementing MFA will not only make it much harder for people in the organisation to share passwords, but it will also bolster the protection

provided by the account lockout policy from brute force attacks.