Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
- Multi Factor authentication (MFA) - Password policies - Firewall maintenance Multifactor authentication requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. Password policies refer to the latest recommendations for password policies focusing on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Multifactor authentication is recommended because attackers have another obstacle in accessing an user account, and it would require more effort. It would also prevent password sharing because employees would have individual authentication and a shared password wouldn't work. Password policies are recommended because it makes sure that they are hard to guess from brute force attacks, since they are more complex, are updated constantly, and employees are required to change default passwords. Firewall maintenance is necessary because rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.