Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools I suggest to implement are: Multi Factor authentication (MFA) - A security measure which 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 - focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. Firewall maintenance- Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Multi Factor authentication (MFA) can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained. Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack). Firewall maintenance can happen regularly. Firewall 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.