Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

Security hardening task	Description	Common uses
Password policies	The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords.	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).
Port filtering	A firewall function that blocks or allows certain port numbers to limit unwanted communication.	Port filtering is used to control network traffic and can prevent potential attackers from entering a private network.
Multifactor 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.	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.

Part 2: Explain your recommendations
The initial hardening measure pertains to password policies, addressing concerns associated with password sharing and the utilization of default passwords. This involves implementing policies that explicitly prohibit the sharing of passwords, while encouraging the utilization of password management tools and generators. The subsequent hardening initiative, port filtering, serves to permit only authorized and secure connections to the company's reverse proxy server. Additionally, a proactive approach involves the closure of unused open ports, and the strategic deployment of honeypots on open ports can function as an effective cyber deception technique. The third hardening measure ensures the implementation of multi-factor authentication. This approach mitigates the risk of compromise even in scenarios where passwords are breached. Factors such as biometrics or hardware passkeys are incorporated, thereby augmenting the security posture and preventing a single point of failure in the authentication process.