Security risk assessment report - Don Wickramanayake

Part 1: Select up to three hardening tools and methods to implement
There are four major vulnerabilities in the Organization's network: 1. The organization's employees' share passwords. 2. The admin password for the database is set to the default. 3. The firewalls do not have rules in place to filter traffic coming in and out of the network. 4. Multifactor authentication (MFA) is not used. Three hardening tools we can implement to mitigate above vulnerabilities: 1, 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).** 2. 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.** 3. Firewall maintenance - Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. - **This 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.** 4. 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
Implementing password policies and MFA can be a solution to the vulnerabilities such as shared passwords among employees, default admin password and not having the MFA set up. Especially attackers will not be able to do a brute force attack as MFA requires you to authenticate access with more than one factor. Regular firewall maintenance and port filtering can be a solution to the unsecured firewall without rules in the organization network. Having a firewall without rules is not effective as it can not allow or block traffic based on rules.