Security risk assessment report

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

3 hardening tools to implement can be :

1. MFA (Multi-factor authentication)
2. Port filtering
3. Password Policies

1. Multi-factor authentication which requires users to verify their identity in two or more ways to access the system or network.
2. Port filtering is a firewall function that can block certain port numbers which are not useful and limit unwanted communications.
3.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.

Part 2: Explain your recommendations

1. Multi-factor authentication 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.
2. Port filtering is used to control network traffic and can prevent potential attackers from entering a private network.
3.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).

- **Kushagra Gupta**