Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The 3 recommended hardening tools are: 1. Password policies 2. 2FA/MFA 3. Port filtering

Part 2: Explain your recommendations
These recommendations are based on the following reasons. 1. Password policies are needed because passwords are currently being shared by employees. This makes it easy to use a brute force attack and gain access to any of the data on the network 2. In conjunction with implementing stronger password policies, an MFA should be implemented to ensure that each user on the network is who they claim to be . This ensures that everyone on the network is not sharing a password and that they are securely accessing the system and not a malicious actor. 3. This is recommended to block unused or unneeded ports from being accessible on the network. This will reduce the attack surface area that a potential malicious actor has access to better enabling the security team to protect the network.