Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Some of the tools and methods that can be implemented are: port filtering, regular firewall maintenance, and strong password policies. Port filtering is a firewall function that blocks or allows certain communications based on the port number to eliminate unwanted traffic. Password policies are used to prevent attackers from being able to guess passwords either manually or by using scripts. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Currently, there are many access related vulnerabilities within the organisation. A strong password policy should be implemented to eliminate many major vulnerabilities that are discovered. The employees should not be sharing passwords, they should have their own password that allows them to access only the segment they are required to do their work. The admin password should be changed to a more complex password that is regularly changed while disabling previous passwords from being used. MFA should be implemented to add a layer of security to the authentication system. This should be updated as new standards are released and enforced regularly. Port filtering should be implemented to block certain port numbers to limit unwanted communication. Currently there is no port filtering in place so all of the traffic is being allowed into the network, including malicious traffic. By eliminating any ports that are not in use, network traffic can be controlled and attackers can be prevented from entering the organisation network. This will need to be implemented once then updated as necessary.