Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three networking hardening tools that I would recommend to address the vulnerabilities found: 1. Password policy 2. MFA 3. Firewall maintenance Having a password policy is important when trying to prevent malicious attackers from accessing the network. This can range from having employees regularly update their passwords, to making them have requirements. Such as 8 characters, a capital letter, and a symbol. Implementing MFA would be beneficial for the company because it's another way for someone to identify and verify their credentials before accessing a system or network. Some options include a password, pin number, OTP, fingerprint, and more. Firewall maintenance involves checking and updating security configurations regularly to stay ahead on potential threats.

Part 2: Explain your recommendations
The first hardening tool I recommended was: a password policy. Not only do the employees share their passwords with each other, the administrator has the default password set for the database. This can lead to vulnerabilities such as a malicious actor using brute force to gain access to the company's information. The second hardening tool that I recommended was: MFA , multi factor authentication. After inspecting the network, I found that this was one of the major vulnerabilities that the company has. Since everybody shares passwords, it would be easy for an attacker to brute force their way into someone's

account, and then gain access to the company network.

The third hardening tool that I recommended was: firewall maintenance. Firewall maintenance should happen regularly so that the system can stay up to date on standards and procedures. Having a strong firewall can prevent unwanted traffic from entering the network. There's multiple firewalls that can be implemented, such as stateful which has predefined rules and tracks the state of network connections. Having a strong firewall can prevent DoS attacks.