Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
After inspecting the organization's network, we discovered four major vulnerabilities. The four vulnerabilities are as follows: 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. Password policies: The second vulnerability could be solved if we follow the password policies i.e. changing the password frequently, minimum 8 letters, a capital letter, a symbol, and a number. Thus preventing an attacker from brute force attack and a disclaimer to discourage password sharing. Firewall Maintenance: The third vulnerability Could be solved if we constantly keep updating firewall policies from the incoming and the outgoing traffic. This keeps our network safe to some extent. Multi Factor authentication (MFA): The fourth vulnerability could be solved if we implement MFA. This allows an extra layer of security to defend the network from attackers guessing the passwords.

Part 2: Explain your recommendations
Enforcing multi-factor authentication (MFA) will reduce the likelihood that a malicious actor can access a network through a brute force or related attack. MFA will also make it more difficult for people within the organization to share

passwords. Identifying and verifying credentials is especially critical among employees with administrator level privileges on the network. MFA should be enforced regularly.

Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. The rules that are included in the password policy will need to be enforced regularly within
the organization to help increase user security.

Firewall maintenance should happen regularly. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.