Security risk assessment report

Part 1: Selecting hardening tools and methods to implement
Three hardening tools the organization can use to address the vulnerabilities found include: 1. Implementing multi-factor authentication (MFA) 2. Setting and enforcing strong password policies 3. Performing firewall maintenance regularly MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords. Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explaining my recommendation(s)
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.