Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to address the vulnerabilities found: 1. Implementing multi-factor authentication (MFA) 2. Setting and enforcing strong password policies 3. Performing firewall maintenance regularly MFA works by requiring users to use more than one way to identify and verify their credentials before they are allowed to access an application. Some forms of MFA can include but are not limited to fingerprint scans, ID cards, pin numbers, and passwords. Password policies are rules that define certain standards for passwords to company accounts. These rules can include password length, acceptable characters, and a notice to discourage password sharing. There are also rules that limit the amount of attempts on an admin account. For example, after five failed attempts a user might lose access to the network. Firewall maintenance means consistently checking and updating the firewall configuration to stay ahead of potential threats.

Part 2: Explain your recommendations
When multi-factor authentication is enforced, it will reduce the likelihood of a malicious actor accessing a network through a brute force attack. MFA will also make it difficult for people within the organization to share their passwords with each other. This type of hardening is essential for the administrator level privileges on the network. MFA should be enforced regularly. By creating and enforcing a password policy within the company, there will be a highly reduced chance of a malicious actor accessing the network. The rules that are made need to be enforced regularly to increase user security.

Firewall maintenance should be carried out on a regular basis. Firewall rules should be updated when an event occurs, especially when the event allows suspicious traffic in the network. By implementing these measures, there will be protection against DoS and DDoS attacks.