Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

The three hardening tools and methods that should be implemented are:
1. MFA
    a. A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.
2. Stronger password policies
    a. The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords.
3. Firewall maintenance and configuration
    a. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Enforcing multi-factor authentication (MFA) adds an additional layer of security beyond a password. It will reduce the likelihood that a malicious actor can access a network through a brute force or related attack since additional effort is required to authenticate in more than one way. MFA may also reduce the likelihood of people sharing passwords. Since the recipient of the shared password would need to possess additional authentication besides a password, MFA makes it less useful to share passwords, thereby making passwords less likely to be shared. Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. Policies such as suspending the account after a certain number of logins can prevent successful brute force attacks. Increasing password complexity, requiring more frequent password updates, and not allowing passwords to be reused also help stall malicious actors from infiltrating the network.

Firewall maintenance should happen regularly. Network administrators should ensure that firewall rules are in place that reflect the most up to date standards for allowed and denied traffic. Traffic from sources that are suspicious should be placed on a denied traffic list. 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