Security risk assessment report

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

The 3 hardening tools we can use to address the vulnerabilities are :

1. Multi-factor authentication (MFA)
2. Strong password policies
3. Performing firewall maintenance regularly

MFA requires users to use multiple ways to identify and verify their credentials when trying to use an application. This can include fingerprint scans, ID cards, pin numbers, and passwords.

Password policies can be changed to require longer password length, a list of characters they have to use, and a disclaimer to discourage password sharing. They can also include rules 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: Explain your recommendation(s)

Using 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 to share passwords. Verifying credentials is especially critical among employees with administrator level privileges on the network.

Creating and enforcing a stronger password policy within the company will make it more challenging for malicious actors to access the network.

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.