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 include:

1. Setting and enforcing strong password policies
2. Implementing multi-factor authentication (MFA)
3. Performing firewall maintenance regularly

Password policies can be refined to include rules regarding a password's list of accepted characters, length, and a disclaimer about discouraging password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after 3 unsuccessful attempts.

MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include ID card, pin numbers, passwords, and fingerprint scans.

Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations

Creating and enforcing a password policy within the company will make it more challenging for malicious actors to access the network. The rules that are included in the password poly will need to be enforced regularly in the organization to help increase user security passwords being updated every 6 months and/or to fit the new password policy as it is regularly updated.

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 new devices always requiring MFA and trusted devices needing to re register every 30 days.

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