Security Risk Assessment Report

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

Thee hardening tools the organization can implement include:

- Enforcing strong password policies
- Using Multi-Factor Authentication (MFA)
- Performing firewall maintenance regularly

Password policies can be refined to improve security. These refinements can include specifying a minimum password length, a list of acceptable characters, and a disclaimer to discourage password sharing. Additionally, rules surrounding unsuccessful login attempts can be implemented, such as locking the user's account after five 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 fingerprint scans, ID cards, pin numbers, and passwords.

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

Part 2: Explain your recommendations

Enforcing a strong password policy will make it incredibly difficult for malicious actors to infiltrate the network. The rules and regulations of the password policy should be enforced regularly to ensure user security. This includes a strict no password sharing policy.

MFA implementation will reduce the risk of a malicious actor accessing the network through common brute force attacks. MFA will also help enforce the no password sharing policy due to the multi verification method of logging in.

Firewalls should continuously be updated every time a security event occurs such as allowing suspicious network traffic into the organization’s network.

Performing firewall maintenance will further slim the chance of a DoS or DDoS attack, and help protect against it.