Security Risk Assessment Report

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

The company can utilize the following three hardening instruments to address the discovered vulnerabilities:

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

Before gaining access to an application, MFA mandates that users employ several methods of identification and credential verification. Fingerprint scans, ID cards, pin codes, and passwords are a few MFA techniques.

Password regulations can be improved to include requirements for password complexity and length, a list of permitted characters, and a disclaimer to prevent password sharing. They can also specify conditions for failed login attempts, such as denying access to the network after five failed tries.

Regular security configuration checks and updates are part of firewall maintenance in order to stay ahead of emerging threats.

Part 2: Explain your recommendation(s)

The likelihood that a malicious threat actor can gain access to a network using brute force or equivalent assault will decrease if multi-factor authentication (MFA) is mandated. MFA will also make it more challenging for employees to share credentials within the company. It's crucial to identify and validate credentials, especially for staff members with administrator-level access to the network. MFA should be periodically enforced.

Making and implementing a password policy in your organization will make it harder for hackers to access your network. To help strengthen user security, the company must frequently enforce the requirements outlined in the password policy.

Regular maintenance should be performed on firewalls. Every time a security event takes place, especially one that lets suspect network traffic into the network, firewall rules should be modified. You can use this method to defend against different DoS and DDoS attacks.