Security risk assessment report

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

Three network hardening tools the organization can use to address the identified vulnerabilities include:

- Implementing multifactor authentication (MFA)
- Setting and enforcing strong password policies
- Performing regular firewall maintenance

Multifactor authentication (MFA) requires users to verify their identity using more than one authentication factor before gaining access to systems or applications. These factors can include passwords, PINs, biometric data, or authentication tokens.

Password policies can be strengthened by enforcing rules related to password length, character complexity, and expiration requirements. These policies can also include disclaimers that discourage password sharing and rules that lock accounts after a specific number of unsuccessful login attempts.

Firewall maintenance involves regularly reviewing and updating firewall rules to ensure that only authorized traffic is allowed to enter or leave the network.

Part 2: Explain your recommendation(s)

Enforcing multifactor authentication (MFA) adds an additional layer of security beyond a username and password. MFA reduces the likelihood that malicious actors can gain access to the network through brute-force or credential-based attacks, since authentication requires more than one verification method. MFA also discourages password sharing because possessing a password alone is not sufficient to gain access.

Creating and enforcing strong password policies makes it more difficult for attackers to compromise user accounts. Security measures such as account lockouts after multiple failed login attempts help prevent brute-force attacks. Additional requirements, including increased password complexity, regular password changes, and restrictions on password reuse, further reduce the risk of unauthorized access.

Regular firewall maintenance ensures that firewall rules reflect current security standards and organizational needs. Administrators can block traffic from suspicious sources and update filtering rules after security incidents. Properly maintained firewalls help protect the network from unauthorized access, malicious traffic, and denial-of-service (DoS and DDoS) attacks.