Improvements

The organization can use three hardening tools to address identified vulnerabilities:

1. **Implement multi-factor authentication (MFA)**
2. **Enforce strong password policies**
3. **Conduct regular firewall maintenance**

Multi-factor authentication (MFA) enhances security by requiring users to provide multiple forms of verification before accessing an application. Examples include fingerprint recognition, identification cards, PINs, and passwords.

Strong password policies should specify requirements such as minimum password length, acceptable character types, and clear guidelines that discourage password sharing. Policies can also include actions following repeated failed login attempts, such as temporarily locking an account after five unsuccessful tries.

Firewall maintenance involves reviewing and updating security configurations regularly to ensure protection against emerging threats and to maintain effective network security.

Recommendations

Enforcing multi-factor authentication (MFA) adds an extra layer of protection beyond standard passwords. This reduces the risk of unauthorized access from brute-force or similar attacks because more than one form of authentication is required. MFA also discourages password sharing since a shared password alone cannot grant access. The additional verification factor makes password sharing less useful, which helps improve overall password security.

Developing and enforcing a comprehensive password policy further strengthens defenses against malicious actors. Measures such as account suspension after several failed login attempts help prevent brute-force attacks. Requiring complex passwords, mandating regular updates, and preventing password reuse make it more difficult for unauthorized users to compromise the network.

Regular firewall maintenance is necessary to ensure strong network protection. Administrators should review and update firewall rules so they align with the latest security standards for allowed and denied traffic. Suspicious traffic sources should be placed on a deny list, and firewall rules should be updated promptly after any security incident. Maintaining accurate and current firewall configurations helps defend against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.