Security risk assessment report

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

1. Multi-Factor Authentication (MFA): MFA strengthens access control by requiring users to verify their identity using two or more authentication factors—such as a password, a one-time code sent to a mobile device, a biometric scan (like a fingerprint), or a security token.
2. Password Policies: Following the latest NIST recommendations, secure password practices now prioritize hashing and salting techniques over enforcing complex characters or frequent password resets. This approach ensures stronger protection against credential-based attacks.
3. Firewall Maintenance: Regularly reviewing and updating firewall rules helps secure the network perimeter. Proper firewall maintenance blocks unauthorized access and adapts defenses to new threats, such as DDoS attacks or unusual traffic patterns.

Part 2: Explain your recommendations

1. MFA adds an essential security layer, reducing the risk of unauthorized access due to stolen or guessed credentials. Once configured, it requires minimal upkeep while significantly boosting security posture. It is especially effective in defending against brute force and credential stuffing attacks.
2. Strong password policies prevent easy exploitation of user credentials. By using cryptographic techniques like hashing and salting instead of relying on complex rules or frequent changes, organizations can defend against both manual password guessing and automated attack scripts.
3. Firewalls serve as a first line of defense. Keeping them updated ensures that only legitimate traffic is allowed in or out of the network. Regular maintenance is critical, especially when responding to new threats or detecting abnormal network behavior. It plays a key role in preventing intrusions and mitigating the impact of DDoS attacks.