

Security risk assessment report

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

- Implementing strong password policies that enforce minimum length and complexity requirements, while also educating users about the risks of password sharing.
- Implement MFA such as fingerprints, ID cards, PINs, and passwords.
- Configure and harden firewall rules to allow only necessary traffic, blocking unused ports and protocols. Enabling logging and monitoring will help detect and respond to suspicious activity.

Part 2: Explain your recommendations

Strong Passwords

Enforcing strong, complex passwords and discouraging sharing helps block unauthorized access.

MFA

MFA adds extra protection if passwords are compromised.

Firewalls

Limiting traffic and blocking unused ports reduces the risk of external threats such as DoS attacks.