Security risk assessment report

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

1. **Multifactor authentication (MFA)**: Implement MFA to require employees to verify their identity using at least two factors before accessing sensitive systems or data. This will significantly reduce the risk of unauthorized access due to shared passwords.
2. **Password policies**: Enforce strong password policies that require employees to create complex passwords, regularly update them, and prohibit the use of default passwords. This will address the vulnerability of the admin password being set to the default.
3. **Firewall maintenance and configuration checks**: Ensure that firewalls are properly maintained and regularly updated with the latest security patches. Additionally, implement firewall rules to filter incoming and outgoing traffic based on established security policies. This will help prevent unauthorized access and data breaches.

Part 2: Explain your recommendations

Multifactor Authentication (MFA):

- Implement MFA for all user accounts, requiring users to provide multiple authentication factors during login.
- Use a combination of something they know (password), something they have (smartphone, token), and something they are (biometrics).
- Ensure that MFA is enforced for remote access, privileged accounts, and sensitive data access.

Password Policies:

- Enforce strong password policies that require complex passwords with a mix of uppercase, lowercase, numbers, and special characters.
- Set password expiration and encourage regular password changes to reduce the risk of password-based attacks.
- Educate employees about the importance of password confidentiality and the dangers of password sharing.
- Implement password history and reuse restrictions to prevent the reuse of old passwords.

Firewall Maintenance and Configuration Checks:

- Regularly update firewall firmware and security patches to address known vulnerabilities.

- Perform periodic configuration checks to ensure that firewall rules align with security policies and business needs.
- Establish proper ingress and egress filtering rules to control incoming and outgoing network traffic.
- Monitor firewall logs and alerts to identify suspicious activities and potential security breaches.