Security risk assessment report (Network Hardening tools)

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

Three hardening tools that can be used to address the network issues and vulnerabilities include:

1. Implementing multi-factor authentication (MFA)
2. Updating and maintaining firewalls
3. Enforcing password policy

MFA requires users to identify themselves in more than one way. Either using something they know, something they have, or something they are. Since the firewalls do not have proper rules in place they are allowing access to outside threats. Updating firewalls helps to prevent potential threats. Password policies can be used to further secure a system and rules can be created on what standards and procedures need to be followed when creating a password or account.

Part 2: Explain your recommendations

MFA reduces unauthorized actions by requiring users to identify themselves with two or more authentication procedures. It can help to prevent repeated attacks like brute force. This along with creating and enforcing password policies will reduce the risk of employees sharing passwords. Password policies can be created to ensure that the default password for database admins are changed regularly. By making sure the firewall is up to date allows for the organization's network to prevent malicious activity from occurring.