Security risk assessment report

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

Three hardening tools and methods that need to be implemented to address vulnerabilities are:

- Password policies
- Firewall maintenance
- Multifactor authentication (MFA)

Part 2: Explain your recommendations

MAJOR VULNERABILITIES

1. The organization’s employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor authentication (MFA) is not used.

A password policy will cover the first two major vulnerabilities as it will make it much more difficult for threat actors to intercept the network. A strong password policy needs to be implemented regularly to ensure that users are following procedure.

Firewall maintenance is an effective way of preventing potential DoS attacks as it can alert security professionals quickly of suspicious activity appearing on their network. This hardening technique should be implemented very regularly to ensure that servers are not vulnerable.

MFA addresses both the vulnerability that it is not implemented at all, as well as the fact that users are sharing passwords. It is an effective way of making sure that a user is genuinely who they say they are when trying to login to their account. MFA only needs to be implemented once but needs to be enforced when users are setting up their accounts.