Security risk assessment report

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

Here are the Three hardening methods that should be implemented:

1. Multi-Factor Authentication (MFA)
2. Password Policies
3. Firewall Maintenance

Part 2: Explain your recommendations

MFA requires a user to verify in two or more ways. Some options are pin number, one time password or fingerprint. MFA can help protect against brute force attacks and similar security events. MFA can be implemented at any time.

Password Policies are used to help prevent attackers from using brute force to acquire a user's password. Password policies use salt and hash passwords for encrypted passwords to protect against threat actors.

Firewall Maintenance requires checking and updating security configurations regularly to stay up ahead of potential threats. Rules can be updated in response to an event that allows abnormal traffic into the network.