Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Firstly, Multi-Factor Authentication (MFA) needs to be implemented where it adds another layer of security in the authentication section. Examples are iris scanning, fingerprint and ID card. Secondly, password policies should be tightened up where the password should contain the alphabet,numbers and symbols with minimum characters. Password sharing should be avoided by the users. Thirdly, the firewall should be updated to its latest patch to make sure it has the latest security. The unused ports also needed to be disabled in the firewall configuration.

Part 2: Explain your recommendations
MFA will prevent brute force attack because even if the attacker successfully entered the first security layer, they cant access the system because they will not have the information or device that allows them to authenticate the user. Password policy needs to be updated regularly because it helps to make the attackers work more challenging to get into the system. A good password policy gives a good security. Firewall maintenance helps to make sure that the firewall has the latest patch installed which tightens up the firewall security inside and outside. Firewall should be only enable using ports, so even if attacker use other ports, it will be blocked by the firewall.