Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Password policies - the organization should have standards for their password policies such as discouraging sharing of passwords amongst employees 2. Network access privileges - this reduces the likelihood of unauthorized users from accessing the internal network 3. Disabling unused ports - any open ports that are not needed or actively being used on firewalls, routers, servers and any other network device should be disabled

Part 2: Explain your recommendations
1. Password policies will reduces chances of a social engineering attack such as sharing passwords with friends who could potentially gain access to the internal network 2. By limiting access of important parts of the network to admins, unauthorized access to the internal network by malicious actors is reduced. 3. Unused open ports can allow intrusions to data. Disabling them reduces chances of future breaches on the network.