Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Password policies - implement hard password policy. These passwords have to be replaced every X time and can't be repeated. 2. Disabling unused ports, to make sure that password will better filter any data. This practice should be constantly maintained to make sure it's actually useful and doesn't interfere with our organization's workflow. 3. Firewall maintenance. This method can update the firewall regularly, in case of an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. On top of this, we can add an IPS to automate and improve our organization protection. These systems need to be constantly maintained to have the maximum impact on the security of our network.

Part 2: Explain your recommendations
1. Currently passwords are being shared, which is a major security issue. Password policy can stop this. 2. Unused ports are a security issue that can be disabled easily without hurting the company workflow. 3. Firewall maintenance makes sure that any information coming into our organization is safe. This is one of the basic pillars of securing our organization. IPS will further improve our organization's security.