Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
There are a number of vulnerabilities present that are leaving the organization extremely susceptible to attacks. Many of these are easily fixable with the implementation of a few hardening tools. These are: ● MFA - Multi-Factor Authentication requires the user to identify themselves in a few ways in order to gain access to the network. This can prevent disgruntled employees from causing damage to the organization's business operations and/or network system. Will also lower the risk due to employees sharing passwords. ● Password Policies - This will help with brute force attacks. Password policies will help prevent passwords from being easily guessed. They can also be used to not only discourage password sharing amongst employees but help implement password attempt limitations. ● Firewall Maintenance - Firewall maintenance involves checking and updating security consistently to stay ahead of threats.

Part 2: Explain your recommendations
Enforcing MFA will reduce the likelihood of a brute force attack making it through to the network. It will also help against password sharing among employees by forcing verification and identification of the user. It's also necessary for employees with high levels of access and privilege on the network. Implementing password policies will allow for tighter restrictions and a smaller attack surface. This will make it much harder for malicious actors to affect the organization's network. Firewall maintenance can be used to protect against DoS and DDoS attacks. Firewalls help defend against suspicious activity on the network.