Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools to use to patch vulnerabilities are: 1. Multi-factor authentication (MFA) 2. Enforcing better password policies 3. Perform maintenance on the firewall MFA requires all users to add another layer of verification to identify the proper user. Some methods could use fingerprint scanning, ID cards, pin numbers or passwords. Password policies could strengthen passwords making it harder to brute force. Enforcing rules that must add capital letters and special characters increase the permutation of the amount of passwords that can be guessed. Also locking users after a few failed attempts can discourage brute force attacks. Firewall maintenance or security configurations will stop most threats.

Part 2: Explain your recommendations
Enforcing multi-factor authentication will reduce bad actors from accessing the network using a brute force tactic or other related attacks. Which also stops people from sharing passwords as well making it harder to log into any account. Administration accounts will be protected and not gotten into that easily. Creating and enforcing powerful password policies will make it harder to brute force anyone's account. It raises the challenge of guessing anyone's password. Updating the firewall regularly will catch suspicious movement in the network. WIll detect most DOS or DDos attacks and stop it from ever occurring.