Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools that will address the vulnerabilities found are: ● Performing Firewall maintenance regularly ● Setting and enforcing strong password policies ● Implementing multi-factor authentication (MFA) Keeping up with firewall maintenance is important as it keeps the firewalls security configuration kept up to date in order to prevent any threat actors. MFA is a multifactor authentication system that requires the user to set up multiple ways verifying the user's identity. This makes it significantly harder for threat actors to brute force attack weak passwords. Password policies enforce stronger security on passwords by making sure they have strict requirements such as special characters. Making sure the passwords are being updated regularly will also make it harder for threat actors to obtain passwords.

Part 2: Explain your recommendations
My recommendation would be to implement MFA. This adds another layer of security making it significantly harder for threat actors to get access to users accounts and it is easy to set up. MFA would also incentivise less password sharing because the user would also have to share the alternative form of authentication. Password policies is another simple implementation that will also enforce tighter security on passwords. Increasing password complexity and requiring more frequent password updates will slow down malicious attempts at gaining access to accounts.