Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Multifactor Authentication (MFA): MFA is a highly effective security measure that requires users to verify their identity using two or more authentication methods. This is a crucial security control to address the vulnerability of employees sharing passwords. MFA adds an additional layer of protection to user accounts, making it significantly more difficult for unauthorized individuals to gain access. MFA should be implemented organization-wide and maintained consistently to enhance security. 2. Password Policies: Updating and enforcing robust password policies following the National Institute of Standards and Technology's (NIST) latest recommendations is essential. Password policies can address the vulnerability of weak or shared passwords. This method is effective because it promotes the use of strong, complex passwords, making it much harder for attackers to guess or brute force their way into accounts. It should be consistently implemented and enforced to ensure ongoing security. 3. Firewall Configuration: Implementing proper firewall rules and maintaining firewall configurations is critical. This addresses the vulnerability related to the lack of firewall rules to filter traffic. Effective firewall configuration and rule management can control and filter both incoming and outgoing traffic, helping to prevent unauthorized access and data exfiltration. Firewall maintenance should be performed regularly to stay ahead of evolving threats.

Part 2: Explain your recommendations
1. Multifactor Authentication (MFA): MFA is a highly effective security hardening technique because it adds an extra layer of identity verification beyond passwords. By requiring users to provide additional forms of authentication, such as a one-time password sent to their

mobile device or a fingerprint scan, it significantly reduces the risk of unauthorized access, even if passwords are shared. MFA should be implemented immediately and maintained as part of the organization's standard security protocols.

2. Password Policies: Strong password policies, following NIST recommendations, are effective because they encourage the use of complex passwords and discourage password sharing. Complex passwords are much more resistant to both manual and automated attacks, such as brute force attacks. This hardening technique should be implemented immediately and enforced consistently to ensure that all users follow the best practices for password security.
3. Firewall Configuration: Properly configured firewalls are essential for protecting the network. By filtering and controlling traffic, firewalls can prevent malicious actors from entering the network through unused or unnecessary open ports. Regular firewall maintenance ensures that the rules remain effective against evolving threats. It should be implemented immediately, and ongoing maintenance is vital to keep the network secure.

In summary, implementing multifactor authentication, strong password policies, and proper firewall configuration with ongoing maintenance will collectively contribute to a more secure network. MFA reduces the risk of unauthorized access due to shared passwords, strong password policies make it difficult for attackers to compromise accounts, and effective firewall configuration guards against malicious network traffic. These measures should be consistently maintained to ensure the ongoing security of the organization's network and protect against future attacks.