Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

Adhere to NIST’s latest recommendation to Password policies.Focus on using salt and hash techniques while setting password policy.

Firewall mantainance and Port filtering.Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.That is Update and check Firewall security configuration regularly.

Enable MFA(Multi Factor Authentication), so that whenever server comes across Brute force attack,it will be really difficult to exploit.

Part 2: Explain your recommendations

Enforcing multi-factor authentication (MFA) will reduce the likelihood that a malicious actor can access a network through a brute force or related attack. MFA will also make it more difficult for people within the organization to share passwords. Identifying and verifying credentials is especially critical among employees with administrator level privileges on the network. MFA should be enforced regularly.

Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. The rules that are included in the password policy will need to be enforced regularly within
the organization to help increase user security.

Firewall maintenance should happen regularly. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.