Security risk assessment report

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

Network hardening tools can be implemented to protect the organization’s overall security.

Below are the list which can be implemented.

Tool	Implementation
Firewall	Deploy at network perimeter; define inbound/outbound rules; segment networks
Penetration test (pen test)	A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.
Password policies	Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).

Part 2: Explain your recommendations

Tool	Explanation
Firewall	This can happen regularly. 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.
Pen testing	With penetration testing, we can identify existing vulnerabilities in the network, application, system and services that can be exploited. This can also prevent any future breach.
Password policies	We can enforce password policies that includes MFA and avoid users to share passwords. MFA adds an extra layer of security protection so an account cannot be easily compromised. We can also implement