Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Password policies: The organizations should implement strong and better policies such as ● Every employee having a unique password, and password sharing should be strongly discouraged. ● Passwords being a certain length with at least two of these: unique characters, numbers, capital, and small letters, etc. ● Avoid using default passwords, especially for the admin panels. Firewalls: using stateful or Next Generation Firewall (NGFW) for the company's network. Or setting predefined rules when stateless firewalls are used. Multifactor authentication (MFA): This is a security measure that requires a user to verify their identity in 2 or more ways to access the system or network. This can include having to send a one-time password to a phone number or email; fingerprints or facial recognition, having to scan an ID card, etc.

Part 2: Explain your recommendations
● Better password policies can reduce the chances of threat actors gaining access to a network or system through brute force ● Stateful firewall is a class of firewall that keeps track of information passing through it and proactively filters out threats. ● NGFW has deep packet inspection, intrusion protection, and threat intelligence. These firewalls would have better rules in place to filter incoming and outgoing traffic. ● Multifactor authentication (MFA) : this adds an extra level of protection that authenticates and verifies anyone before they have access to certain data or networks. This also reduces the chance that a threat actor can access a device or network through brute force.