Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Password Policies - Password policies can be refined to include rules regarding password length, a list of acceptable characters, and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, such as the user losing access to the network after five unsuccessful attempts. Multifactor Authentication (MFA) - MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords. Network Access Privileges - Network access privileges can be implemented by enforcing the principle of least privilege and role-based access control, ensuring users only receive the minimum permissions required for their job responsibilities. Additionally, organizations can strengthen access security by applying network segmentation, enabling multi-factor authentication, and monitoring access logs to detect unauthorized activity.

Part 2: Explain your recommendations
Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. Policies such as suspending the account after a certain number of logins can prevent successful brute force attacks. Increasing password complexity, requiring more frequent password updates, and not allowing passwords to be reused also help stall malicious actors from infiltrating the network. Enforcing multi-factor authentication (MFA) adds a layer of security beyond a password. It will reduce the likelihood that a malicious actor can access a network through a brute force or related attack since additional effort is required to authenticate in more than one way. MFA may also reduce the likelihood of people sharing passwords. Since the recipient of the shared password would need to possess additional authentication besides a password, MFA makes it

less useful to share passwords, thereby making passwords less likely to be shared.

Implementing strong network access privileges significantly reduces the risk of unauthorized access to critical systems and sensitive data. By enforcing the principle of least privilege and role-based access control, employees only receive the permissions required for their job duties, which minimizes the potential damage if an account is compromised. Network segmentation further limits an attacker’s ability to move laterally across the environment. Adding multi-factor authentication strengthens login security and protects against brute force attacks. Finally, logging and monitoring access activity allows the security team to quickly detect and respond to suspicious behavior. Together, these measures improve the organization’s overall security posture and reduce the likelihood of successful attacks.