Kicho Yu
2025-03-03

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to address the vulnerabilities found include: 1. Firewall maintenance 2. Multifactor authentication (MFA) 3. Password policies Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. MFA requires users to use more than one way to identify and verify their credentials before accessing an application. Some MFA methods include ID cards, pin numbers, passwords, and biometrics such as fingerprint or iris. 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 about unsuccessful login attempts, such as the user losing access to the application after five unsuccessful attempts.

Part 2: Explain your recommendations
Why is the recommended security hardening technique effective? ● Firewall maintenance is effective because it is a gateway to port numbers. Network admin can allow only a handful of port numbers and block the rest. This way filters traffic coming in and out of the network, and especially filters out malicious traffic. ● Multifactor authentication (MFA) is effective, because this is another layer of security. Employees need an ID and a password to access the company servers as the first layer of security. Then MFA is another protection against brute force attacks. ● Password policies should illustrate such that no default password is used, how often the password should be updated, and how long and

complex the password should be.

How often does the hardening technique need to be implemented?

- Firewall maintenance should be implemented when a network admin sets it up. Then it will be updated, but not very frequently. Basically, the allowlist is small and barely changing. So there is no need for a frequent update.
- Multifactor authentication (MFA) is mostly set up once and then maintained by a system admin.
- Password policies are mostly set up once and then are used to alert employees to update their password in a set cadence. A company can send out a reminder to employees about the password policy about every quarter.