Security risk assessment report

Problem Statement

You have been tasked with creating a security risk assessment report for an organization. The goal is to identify common security vulnerabilities and recommend up to three tools or methods to harden the organization's system and improve its overall security posture.

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

1. Multifactor Authentication (MFA)
Implementing MFA will add an additional layer of security to the login process, making it more difficult for attackers to gain access to the system using stolen or guessed passwords.

2. Firewall maintenance and port filtering
Regularly updating firewall configurations and implementing port filtering will help block unnecessary traffic and prevent potential attackers from entering the network through open ports.

3. Password policies and password management
Establishing strong password policies, including unique and complex passwords for each employee, and enforcing regular password changes will reduce the risk of unauthorized access to the system.

Part 2: Explain your recommendations

Recommendation 1: Implement Multifactor Authentication (MFA)

Implementing MFA is an effective way to address the vulnerability of shared passwords and default admin passwords. MFA adds an additional layer of security to the login process, making it more difficult for attackers to gain access to the system using stolen or guessed passwords. This technique is effective because it requires users to provide additional verification factors beyond just a password, such as a one-time code sent to their phone or a biometric scan. MFA needs to be implemented once, and then maintained regularly to ensure that it remains effective.

Recommendation 2: Implement Firewall Maintenance and Port Filtering

Implementing firewall maintenance and port filtering is an effective way to address the vulnerability of open ports and unnecessary traffic. By regularly updating firewall configurations and blocking unused ports, we can prevent potential attackers from entering the network through open ports. This technique is effective because it reduces the attack surface of the network and prevents malicious traffic from entering the system. Firewall maintenance and port filtering need to be implemented regularly, ideally as part of a routine security maintenance schedule.

Recommendation 3: Implement Strong Password Policies and Password Management

Implementing strong password policies and password management is an effective way to address the vulnerability of weak passwords. By requiring unique and complex passwords for each employee, and enforcing regular password changes, we can reduce the risk of unauthorized access to the system. This technique is effective because it makes it more difficult for attackers to guess or crack passwords using brute-force methods. Password policies need to be implemented and enforced regularly, with periodic reviews to ensure that they remain effective and aligned with industry best practices.