Security risk assessment report

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

Part 1: Select up to Three Hardening Tools and Methods to Implement

Tool/Method	Description	Common Uses
Multifactor Authentication (MFA)	A security measure requiring a user to verify their identity in two or more ways to access a system or network.	Can help protect against brute force attacks and similar security events. Implemented once, then maintained.
Configuration Checks	Updating the encryption standards for data stored in databases.	To see if there are any unauthorized changes to the system.
Firewall Maintenance	Checking and updating security configurations regularly to stay ahead of potential threats.	Regularly updated. Can protect against various DDoS attacks and abnormal network traffic.

Part 2: Explain your recommendations

Part 2: Explain Your Recommendations

1. Multifactor Authentication (MFA)

- **Description:** MFA adds an extra layer of security by requiring users to provide two forms of identification before gaining access.
- **Effectiveness:** Significantly reduces the risk of unauthorized access, even if passwords are compromised. It is effective against brute force

attacks.
- **Implementation Frequency:** MFA is typically set up once and maintained, with periodic reviews to ensure continued effectiveness.

2. Configuration Checks

- **Description:** Regularly update and review encryption standards for data stored in databases to ensure they meet the latest security protocols.
- **Effectiveness:** Helps identify and address unauthorized changes to the system, ensuring data remains secure. It prevents potential data breaches caused by outdated encryption methods.
- **Implementation Frequency:** Should be conducted regularly to ensure compliance with the latest security standards.

3. Firewall Maintenance

- **Description:** Regularly check and update firewall rules to filter inbound and outbound traffic based on IP addresses, ports, and protocols.
- **Effectiveness:** Controls the flow of network traffic, reducing the risk of unauthorized access and data exfiltration. It helps protect against DDoS attacks and other abnormal network activities.
- **Implementation Frequency:** Initial configuration with continuous monitoring and updates to address emerging threats.