Security risk assessment report

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

Password Manager and Policy Enforcement: Implement a password manager tool that encourages employees to use strong, unique passwords. Enforce password complexity rules, regular password changes, and educate employees about the importance of not sharing passwords. Additionally, set up alerts for password sharing or weak password usage.

Database Security Best Practices: Change the default admin password for the database to a strong, unique password. Consider implementing role-based access control (RBAC) for database users to ensure that only authorized personnel can access sensitive data. Regularly audit database access logs for suspicious activities.

Firewall Rules and Intrusion Detection/Prevention System (IDPS): Configure firewalls with strict rules to filter incoming and outgoing traffic. Allow only necessary ports and protocols and implement deep packet inspection to identify and block malicious traffic. Deploy an Intrusion Detection/Prevention System (IDPS) to monitor network traffic for signs of attacks and automatically block or alert on suspicious behavior.

Part 2: Explain your recommendations

Password Manager and Policy Enforcement: Passwords are often the weakest link in security. By implementing a password manager and enforcing strong password policies, such as minimum length, complexity, and regular changes, the organization can significantly reduce the risk of unauthorized access through password guessing or sharing. Educating employees about these policies will help raise awareness of the importance of password security.
Database Security Best Practices: Changing the default admin password is a basic step in securing the database. Role-based access control ensures that only authorized individuals can interact with the database and limits the potential for insider threats. Regularly auditing database access logs will help detect and respond to any suspicious activities promptly, minimizing the impact of any potential breaches.
Firewall Rules and Intrusion Detection/Prevention System (IDPS): Configuring strict firewall rules is essential for controlling incoming and outgoing network traffic. By allowing only necessary ports and protocols, the organization can minimize the attack surface. Deep packet inspection enhances security by identifying and blocking malicious traffic patterns. Additionally, deploying an IDPS provides real-time monitoring and threat detection, allowing the organization to respond quickly to potential threats, further reducing the risk of data breaches.

Luca Forma