Vulnerability Assessment Report

December 15, 2024 – Created by me

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The following are the reasons for conducting the security analysis:-

1. Database servers are the backbone of businesses, providing a centralized repository for critical data. They enable efficient data storage, retrieval, and management, facilitating informed decision-making.

2. It stores sensitive data like PII and SPII that must be protected at any cost per laws.

3. *If the server crashes it will stop day to day operation of an organization and will cause severe damage.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Competitors may take advantage to infiltrate the server and then destroy, erase, manipulate, or steal data that may harm an organization, such as damaging its reputation.*	*3*	*3*	*9*
Hacker	*Hackers will definitely try to breach the server security and install malicious software into the system, which will lead to multiple negative impacts on an organization such as data loss, data theft, finances, and reputation.*	*3*	*3*	*9*
Employees	*They might do some misconfiguration or try to alter data in many ways.*	*2*	*3*	*6*

Approach

Based on risk assessment every threat source can cause serious harm to an organization in many ways depending on their intentions. These threats were evaluated based on how likely this can happen, and the damages that can cause to an organization.

Remediation Strategy

- To prevent or control such threats we need to properly configure the organization's firewall so that only valid or allowed IPs can enter the internal network and connect to the database.
- We can use an authentication, authorization, and accounting framework for access control.
- Data access must be only given based on the role and the task they need to complete.
- We also need to Audit the system regularly so, that only valid and authorized users have access to the database and proper permission is in place.