Vulnerability Assessment Report

12th August 2024

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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database serves a purpose of many employees around the world working to interact with the data from the server to find potential customers. Data on the server left unprotected can be vulnerable to threat actors obtaining sensitive information to perform identity theft or financial reasons. If the data on the server were to be disabled, then there would be serious consequences such as fines, lawsuits, and damage to the reputation. It can also slow down productivity and this would violate the CIA triad of Availability.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Conduct Denial of Service (DoS) attacks.	*2*	*2*	*4*
Competitor	Obtain sensitive information via exfiltration	*2*	*2*	*4*
Advanced persistent threat (APT)	Conduct "man-in-the-middle" attacks.	*1*	*3*	*3*

Approach

I chose Hacker as I think they're significant business risks because they may have knowledge to access the network server and perform Denial of Service attacks to disrupt the business operations and slow down by sending overwhelming numbers of requests. I chose Competitor because since the database server is open to the public, the competitor may gather sensitive information in order to understand the customers to deter them from the company. Lastly, I picked Advanced Persistent threat because since the network connection was using IPv4, it can be vulnerable to man in the middle attack when employees connect to the network.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. This reduces any chances of man in the middle attack. To address the exfiltration of sensitive information, I would implement public key infrastructure which contains the two step processes of the framework: Exchange of information encryption and establishing trust using digital certificates.