Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of the 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

This vulnerability analysis assesses potential threats to the Linux-based MySQL database server, which is critical to the organization's data management and operational efficiency. Securing the data on this server is vital to protecting sensitive business information and maintaining the integrity of day-to-day operations. A successful attack or server failure could lead to data breaches, financial losses, and disruptions to business processes. This analysis aims to identify and mitigate risks, ensuring the server's stability and the organization's continued success.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacktivist	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Business Partner	*Craft counterfeit certificates*	*2*	*3*	*6*
Competitor	*Perform reconnaissance and surveillance of the organization.*	*2*	*2*	*4*

Approach

This qualitative vulnerability assessment focuses on three specific threat sources: hacktivists, business partners, and competitors. These threats were selected because they significantly impact the organization's sensitive data and operational continuity. Hacktivists pose a high risk of data breaches through unauthorized access, while compromised business partners could weaken encrypted communications. Competitors engaging in surveillance could exploit vulnerabilities for a competitive advantage. By evaluating these threats, the assessment aims to highlight the most significant risks to guide resource allocation and security measures effectively.

Remediation Strategy

Implementing multi-factor authentication (MFA) and the principle of least privilege is essential to mitigate the risks of hacktivists, business partners, and competitors. MFA can prevent unauthorized access even if credentials are compromised, while least privilege limits access to sensitive data based on user roles. Additionally, deploying a public key infrastructure (PKI) can help secure encrypted communications with business partners and prevent the misuse of certificates. A defense-in-depth strategy, combining network segmentation and intrusion detection systems, can further safeguard against surveillance and data exfiltration attempts..