Vulnerability Assessment Report

Mike Thomas

Cybersecurity Analyst

Date: July 1, 2025

1. System Description

The assessed system is a small business database server running Linux and MySQL. It stores sensitive customer and internal data. The server is currently exposed to public access and lacks robust access controls, creating a significant security risk.

2. Scope

The assessment focuses on evaluating access control vulnerabilities and risks related to the publicly accessible database server. The analysis was guided by NIST SP 800-30.

3. Purpose

The goal of this assessment is to:

- Identify vulnerabilities and potential attack vectors

- Evaluate the likelihood and impact of threats

- Recommend mitigation strategies to strengthen the server's security

4. Risk Assessment

Below is a summary of identified risks and their ratings (Likelihood x Severity):

Threat Source	Threat Event	Risk Score
Hacker	Exfiltrate sensitive data	High (9)
Employee	Disrupt operations	Medium (6)
Customer	Alter/Delete data	Low (3)

5. Approach

Risks were assessed based on potential exploitation and impact on business operations. Special attention was given to the server's public exposure and lack of authentication mechanisms.

6. Remediation Strategy

Recommended actions include:

- Enforce multi-factor authentication and role-based access controls

- Restrict database access using IP allowlists or VPN
- Apply regular patch management for OS and database
- Encrypt data in motion (TLS 1.3) and at rest (AES-256)
- Monitor logs and run periodic vulnerability scans

7. Tools Used

- Linux terminal commands (ls -l, chmod, nmap)
- SQL queries for database review
- NIST SP 800-30 framework for risk analysis
- Spreadsheet software for risk tracking

8. Key Takeaways

This assessment improved understanding of vulnerability management and risk prioritization. It demonstrates my ability to analyze threats and communicate actionable security recommendations.