**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 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](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose:**

* the database server is so important for the Business because we cant complete the work without it Work fully and efficiency because it will establishes the connection.
* For that reason we have to secure the server to protect it from any malicious attacks like DDOS or others because if it not work the Business and the Reputation will get damage and we will miss the Compliance and that’s will bring problems
* So if the server not work or disabled we will not able to have Connection to it and take the Info we want for jobs , also the data will leak and the damage for the company of all ways financial operational etc.

# **Risk Assessment:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| Craft counterfeit certificates | Threat source compromises a certificate authority to make their connections appear legitimate. | *2* | *2* | *6* |
| Disrupt mission-critical operations. | Threat source compromises the integrity of information in such a way that prevents the business from carrying out critical operations. | *2* | *3* | *8* |

# **Approach**:

* 1. The competitor can reach the database because its open so if this competitor have any (DDoS) attacks it will give severe Action for the *organization. And its* severe because they maybe wants to effect the company server to damage the Reputation.
* 2. Threat actor can Craft counterfeit certificates Threat source compromises a certificate authority to make their connections appear legitimate. And if this happen it can effect the customers and effect the organization Business
* 3.Disrupt mission-critical operations can this happen if the server got attacked so the Business will got effected by this.

# **Remediation Strategy :**

1. We must first of all Implement vulnerability Scanner to detect the vulnerabilities after that assess these vulnerabilities and solve it .
2. Make defense in depth strategy with strong implantation for each layer
3. Include the (Authentication – Authorization – accounting ) framework in the layers of the defense in depth
4. (MFA) to mitigate the risk of non real users

In the end if these access controls done well. We will have strong defense and limit the risks from hackers.