**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**

Consider the following questions to help you write:

* *How is the database server valuable to the business?*
* *Why is it important for the business to secure the data on the server?*
* *How might the server impact the business if it were disabled?*

The database server is used by employees of the e-commerce company to regularly query, or request, data to find potential customers. It is important for the business to secure the data on the server so that the threat actors would not take advantage of sensitive personal data of customers just to exploit them for their own personal gains. If the server is disabled then the business cannot be able to find potential customers to attend to.

# **Risk Assessment**

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Nation state* | *Perform reconnaissance and surveillance of organization* | *3* | *3* | *9* |
| *Networking* | *Conduct Denial of Service (DoS) attacks* | *3* | *3* | *9* |
| *Networking* | *Conduct “man-in-the-middle” attacks* | *2* | *3* | *6* |

# **Approach**

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

* *What was your rationale for selecting the risks that you evaluated?*
* *How were you deriving the likelihood and severity scores of each risk?*
* *What were the limitations of the assessment?*

Since the database has been open to the public since the start of the company, there are most likely going to be more threats protruding into the database server, which they can exploit its vulnerabilities. The threats could be performing reconnaissance and surveillance of an organization, conducting Denial of Service (DoS) attacks, and conducting “man-in-the-middle” attacks because the company stores information on a remote server due to the employees who work remotely from all locations around the globe and the database is opened to the public which means more threats to penetrate the server than a local server.

With many threats coming into the system from all corners of the world, it means that the business would be at risk losing a lot of money and the information of the employees and potential customers would be compromised severely. The limitations of the assessment are that since there are a lot of threats pointing at which direction they are heading because there would be a lot of them, the security teams just have a lot of vulnerabilities to focus on.

# **Remediation Strategy**

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Consider the following questions to help you write a remediation strategy:

* *Which technical, operational, or managerial controls are currently implemented to secure the system?*
* *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?*
* *How will the results of the assessment improve the overall security of the system?*

*Managerial and technical controls can help with remediate the risks since the security teams need to follow specific guidelines or regulations to properly mitigate the risks as well as using the proper tools to prevent the risks from happening. The results of the assessment will also help the company to know the best method to prevent the risks from happening as much as possible.*