Vulnerability Assessment

Work Sample by Francheska Fernandez

Scenario

This scenario is based on a fictional company as part of Coursera's Google Cybersecurity Professional Certificate.

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.

My tasks:

1. *Review information about the vulnerable server, including the provided system description and scope.*
2. *Perform risk assessment (explanation of information system purpose, identification of potential threat sources, events, and risk levels).*
3. *Propose security recommendations that align with best practices from NIST SP 800-30.*

Work Sample: Vulnerability Assessment

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 is used to guide the risk analysis of the information system.

Purpose

The database server is a critical asset to the business because it stores and manages essential operational and financial data that supports daily activities and decision-making. Securing the data on the server is vital to protect sensitive information from unauthorized access, data breaches, or corruption. If the server were disabled, business operations could be disrupted, resulting in downtime, financial loss, and reduced customer trust.

Risk Assessment

Threat Source	Threat Event	Likelihood	Severity	Risk
Outsider (Hacker)	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Privileged User (System Admin)	*Alter/Delete critical information*	*2*	*3*	*6*
Outsider (Hacktivist)	*Conduct Denial of Service (DoS) attacks*	*2*	*2*	*4*

Approach

These threats were selected because they directly relate to vulnerabilities in the described Linux-based MySQL database server.

- An **outside hacker** could exploit network or software weaknesses, posing a severe risk to **data confidentiality**.
- A **privileged use**r could accidentally or intentionally alter or delete critical information, **disrupting operations**.
- A **hacktivis**t may conduct DoS attacks against the server's IPv4 network, **impacting system availability**.

Security Recommendations

To reduce the identified risks, several key security controls should be implemented.

- Public Key Infrastructure (PKI) and strict encryption policies can help prevent data exfiltration.
- Role-based access control (RBAC) and regular privilege reviews can mitigate risks of altering and deleting critical data.
- Network intrusion detection systems (IDS) and rate limiting can help defend against DoS attacks, maintaining system availability and reliability.

Written Recommendation 1: Implement PKI and encryption to secure data in transit and at rest. This should be the top priority because the MySQL database contains sensitive business information, and preventing data exfiltration is essential to maintaining confidentiality and compliance.

Written Recommendation 2: Enforce role-based access control (RBAC) and audit privileged user activity. This is critical because misuse or errors by system administrators can lead to significant data loss or service disruption, directly impacting business continuity and trust.