Maestría en Seguridad de Tecnología de Información
Seguridad en la Infraestructura de Tecnología de Información
2023-2

Profesor: Herrera Araiza Israel Alejandro

ENTREGABLE FINAL:

"PROPUESTA DE DESARROLLO DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL"

Alumna: Kuhliger Martínez Martha Guadalupe

19 de marzo del 2023

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente trabajo consiste en implementar y reforzar los conceptos y las tecnologías que se aprendieron en el curso de Seguridad en la Infraestructura de Tecnología de Información para el diseño y desarrollo de una propuesta que proporcionará seguridad perimetral a la infraestructura de una organización para un caso de estudio de una empresa real, la cual se llamará *Kuhliger S.A. DE C.V*. para este efecto.

El caso de estudio consistió en desarrollar una arquitectura de seguridad perimetral para proteger la empresa y guiarla adecuadamente para prevenir amenazas dañinas debido a la explotación de vulnerabilidades causadas por intrusos o ciberdelincuentes.

Se realizó una recopilación y análisis de la información con respecto a las herramientas que se implementaron de la propuesta; siendo la máquina virtual *VMware Workstation*, el sistema operativo *Kali Linux*, la herramienta de escaneo de vulnerabilidades *Acunetix*, el estándar *ISO 27001*, así como la biografía de la empresa *Kuhliger S.A. DE C.V*. y su diagrama de red con el propósito de conocer el negocio y las funciones de la organización, las tecnologías y políticas de seguridad que se pueden implementar para brindar y garantizar una protección eficiente en la infraestructura del servidor web de la organización *Kuhliger S.A. DE C.V*.

Con base en lo anterior, se desarrolló una propuesta para garantizar un mejor control en el servidor web y gestionar los riesgos y las vulnerabilidades, ejecutando herramientas de escaneo de vulnerabilidades, analizar las vulnerabilidades y los riesgos que se presentaron, establecer la probabilidad, el impacto y el nivel de riesgo de cada vulnerabilidad para determinar si estas vulnerabilidades son amenazas potenciales para la organización *Kuhliger S.A. DE C.V.,* investigar y proponer una solución para estas vulnerabilidades y finalmente implementar una solución para corregirlas.

Con esta estrategia se ejecutó un escaneo de vulnerabilidades al servidor web de la organización *Kuhliger S.A. DE C.V.* utilizando la herramienta *Acunetix*, instalada en el sistema operativo *Kali Linux* operado por la máquina virtual *VMware Workstation*. Se detectaron las vulnerabilidades y se identificaron los riesgos para desarrollar una matriz de riesgos que permitió determinar la probabilidad, el impacto y el nivel de riesgo de cada una. La organización *Kuhliger S.A. DE C.V*. cuenta con medidas de seguridad, por lo tanto, no se detectaron vulnerabilidades que podrían convertirse en amenazas.

Se describen soluciones que se deben implementar para las vulnerabilidades que se presentaron en el análisis de vulnerabilidades del servidor web de la organización *Kuhliger S.A. DE C.V.*

De esta forma se podrá minimizar y mitigar los riesgos para proteger la información y los sistemas de la organización *Kuhliger S.A. DE C.V*. ante un ataque voluntario o involuntario que pudiera surgir y causar un daño en la organización.

Por confidencialidad se ha modificado el nombre de la organización por *Kuhliger S.A. DE C.V*., así como algunos detalles de la biografía de la organización.

ABSTRACT

This work consists of implementing and reinforcing the concepts and technologies learned in the Information Technology Infrastructure Security course for the design and development of a proposal that provides perimeter security to the infrastructure of an organization for a case study of a real company, which will be called *Kuhliger S.A. DE C.V*. for this purpose.

The case study consisted of developing a perimeter security architecture to protect the company and guide it appropriately to avoid harmful threats due to the exploitation of vulnerabilities caused by intruders or cybercriminals.

A compilation and analysis of information regarding the tools that were implemented from the proposal was carried out; being the VMware Workstation virtual machine, the Kali Linux operating system, the *Acunetix* vulnerability scanning tool, the ISO 27001 standard, as well as the biography of the company *Kuhliger S. A. DE C.V*. and its network diagram in order to know the business and functions of the organization, the technologies and security policies that can be implemented to provide and ensure efficient protection in the web server infrastructure of the organization *Kuhliger S.A. DE C.V.*

Based on the above, a proposal was developed to safeguard better control over the web server and manage risks and vulnerabilities, running vulnerability scanning tools, analyze the vulnerabilities and risks that were presented, establish the probability, impact and risk level of each vulnerability to determine whether these vulnerabilities are potential threats to the organization *Kuhliger S.A. DE C.V*., investigate and propose a solution for these vulnerabilities and finally implement a solution to correct them.

With this strategy, a vulnerability scan was performed on the web server of the *Kuhliger S.A. DE C.V*. organization using the *Acunetix* tool, installed on the Kali Linux operating system operated by the VMware Workstation virtual machine. Vulnerabilities were detected and risks were identified to develop a risk matrix to determine the probability, impact and risk level of each one of them. The organization *Kuhliger S.A. DE C.V*. has security measures in place, so no vulnerabilities that could become threats were detected.

The solutions to be implemented for the vulnerabilities that were presented in the vulnerability analysis of the web server of the organization *Kuhliger S.A. DE C.V*. are described.

In this way it will be possible to minimize and mitigate the risks to protect the information and systems of the organization *Kuhliger S.A. DE C.V*. against a voluntary or involuntary attack that could occur and cause damage to the organization.

Due to confidentiality, the name of the organization has been changed to *Kuhliger S.A. DE C.V*., as well as some details of the organization's biography.