Universidad Tecnológica Ecotec

Facultad de ingenierías

Título del trabajo:

Evaluación de la seguridad informática mediante pruebas de intrusión: Caso de estudio Acromax S.A.

Línea de investigación:

Tecnologías de la información y comunicación

Modalidad de titulación:

Trabajo de integración curricular

Carrera:

Ingeniería de Software

Título a obtener:

Ingeniero en Software

Autor:

Dennis Alexander Cali Galarza

Tutor(es):

Mgtr. Lissenia Sornoza,

Dr. Cesar Alcácer

Samborondón-Ecuador

2023

Agradecimientos

En primer lugar, quisiera expresar mi sincera gratitud a Dios, que ha sido una fuente inagotable de sabiduría y guía constante a lo largo de este apasionante viaje académico. Su inquebrantable inspiración y fortaleza han sido mi faro a cada paso del camino. Con profunda gratitud y gran humildad deseo reconocer y agradecer a las personas que han desempeñado un papel esencial en la realización de esta tesis. Mis padres merecen un agradecimiento especial por su apoyo inquebrantable, sus sacrificios y su amor incansable. Su aliento y confianza en mí han sido el motor de mis esfuerzos. Sin su apoyo constante, este logro no habría sido posible. A mis distinguidos tutores de tesis ya que sin su sabiduría, dedicación y asesoramiento experto han sido inestimables. Sus consejos críticos y su perspicaz enfoque han dado forma y profundidad a este trabajo. También quiero dar las gracias a mis profesores universitarios por compartir sus conocimientos conmigo y alimentar mi espíritu crítico y mi gusto por la investigación. Al Ing. Henry Menoscal, jefe de Informática de la prestigiosa empresa Acromax, cuyo incansable apoyo ha hecho posible este trabajo. Sin su visión estratégica y sus consejos, esta tesis no habría sido posible.

Cada uno de vosotros ha desempeñado un papel esencial en esta aventura. Vuestro apoyo y asesoramiento han dado forma a esta tesis y han contribuido a mi desarrollo personal y académico. Mi más sincero agradecimiento a todos.

Universidad Ecotec

ANEXO N° 7.1

UNIDAD DE INTEGRACIÓN CURRICULAR
CERTIFICADO DE APROBACIÓN DEL TUTOR METODOLÓGICO Y CIENTÍFICO PARA LA PRESENTACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Samborondón, 30 de Noviembre de 2023

Magíster
Erika Ascencio Jordán
Decana de la Facultad
Ingenierías
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de integración curricular TITULADO: **"Evaluación de la seguridad informática mediante pruebas de intrusión: Caso de estudio Acromax S.A"** según su modalidad PROYECTO DE INTEGRACIÓN CURRICULAR; fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, Por lo que se autoriza al estudiante: **Cali Galarza Dennis Alexander**, para que proceda con la presentación oral del mismo.

ATENTAMENTE,

CESAR| ALCACER| SANTOS

Firmado digitalmente por CESAR|ALCACER| SANTOS
Fecha: 2023.12.01 18:03:36 +01'00'

PhD. César Alcácer Santos
Tutor metodológico

Mgtr. Lissenia Isabel Sornoza Quijije
Tutora científica

Universidad Ecotec

Universidad Ecotec

ANEXO N°7.2

UNIDAD DE INTEGRACIÒN CURRICULAR
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Habiendo sido revisado el trabajo de integración curricular TITULADO:

Evaluación de la seguridad informática mediante pruebas de intrusión: Caso de estudio Acromax S.A

elaborado por **Cali Galarza Dennis Alexander** fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje de coincidencias del 3 %, mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del Trabajo de integración curricular. Se puede verificar el informe en el siguiente link:

https://app.compilatio.net/v5/report/c55bbd52b4a16a23ed0e827431c82fcbd9c92ff9/summary

Adicional se adjunta el informe de dicho resultado.

ATENTAMENTE,

CESAR| ALCACER| SANTOS

Firmado digitalmente por CESAR|ALCACER| SANTOS
Fecha: 2023.12.01 17:57:26 +01'00'

PhD. César Alcácer-Santos
Tutor metodológico

Mgtr. Lissenia Isabel Sornoza Quijije
Tutora científica

Universidad Ecotec

CERTIFICADO DE ANÁLISIS
magister

CALI GALARZA DENNIS ALEXANDER_TESIS

3% Textos sospechosos

- 3% Similitudes
- < 1% similitudes entre comillas
- 0% Idioma no reconocido
- 0% Textos potencialmente generados por la IA

Nombre del documento: CALI GALARZA DENNIS ALEXANDER_TESIS.pdf
ID del documento: d9a2a68a4980a7457bf47f22420c413e6b570b59
Tamaño del documento original: 2,45 MB

Depositante: CESAR ALCACER SANTOS
Fecha de depósito: 1/12/2023
Tipo de carga: interface
fecha de fin de análisis: 1/12/2023

Número de palabras: 14.829
Número de caracteres: 111.891

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**cybermap.kaspersky.com** | FUENTES DE INFORMACIÓN | Mapa en tiempo real de... https://cybermap.kaspersky.com/es/subsystems#:~:text=ODS (On Demand Scanner) muestra el flujo... 1 fuente similar	< 1%		Palabras idénticas: < 1% (167 palabras)
2	**www.controlsanitario.gob.ec** | Agencia Nacional de Regulación, Control y Vigilanci... https://www.controlsanitario.gob.ec/arcsa-una-institucion-que-mejora 2 fuentes similares	< 1%		Palabras idénticas: < 1% (65 palabras)
3	**owasp.org** | A01 Pérdida de Control de Acceso - OWASP Top 10:2021 https://owasp.org/Top10/es/A01_2021-Broken_Access_Control/	< 1%		Palabras idénticas: < 1% (52 palabras)
4	**repositorio.utc.edu.ec** | Potencialización del laboratorio de procesos lácteos de la ... http://repositorio.utc.edu.ec/handle/27000/10154 2 fuentes similares	< 1%		Palabras idénticas: < 1% (43 palabras)
5	**www.ambit-bst.com** | 5 riesgos de seguridad de las compañías farmacéuticas https://www.ambit-bst.com/blog/5-riesgos-de-seguridad-de-las-compañías-farmacéuticas	< 1%		Palabras idénticas: < 1% (37 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**www.seguridadenamerica.com.mx** | Seguridad en América | CIBERSEGURIDAD Y ... https://www.seguridadenamerica.com.mx/34118/ciberseguridad-y-transporte-en-la-industria-farma...	< 1%		Palabras idénticas: < 1% (18 palabras)
2	**revista.seguridad.unam.mx** | Frameworks para monitoreo, forense y auditoría de t... https://revista.seguridad.unam.mx/numero24/frameworks-para-monitoreo-forense-y-auditor-de-tr...	< 1%		Palabras idénticas: < 1% (13 palabras)
3	**www.doi.org** | Towards Lightweight Mobile Pentesting Tools to Quickly Assess Mac... https://www.doi.org/10.1109/TLA.2019.8931199	< 1%		Palabras idénticas: < 1% (15 palabras)
4	**www.kreston.com** | Seguridad digital frente a ciberamenazas | Kreston global https://www.kreston.com/es/article/digital-security-against-cyber-threats/#:~:text=Según CISCO, la c...	< 1%		Palabras idénticas: < 1% (10 palabras)
5	**curiosaweb.com** | La historia de la seguridad informática: evolución y desafíos https://curiosaweb.com/la-historia-de-la-seguridad-informatica-evolucion-y-desafios/	< 1%		Palabras idénticas: < 1% (10 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://cybermap.kaspersky.com/es
2 https://www.exploit-db.com/google-hacking
3 https://www.wappalyzer.com/
4 https://www.shodan.io/
5 https://archive.org/web/

Resumen

La seguridad informática es esencial en las empresas, especialmente en el sector farmacéutico. Debido a la constante evolución de la tecnología dentro de las corporaciones, la dependencia de los sistemas informáticos ha traído consigo desafíos que afrontar en las organizaciones. Salvaguardar la infraestructura TI y los datos es una tarea crucial. Los datos que las empresas albergan como información crítica y de alto valor deben ser gestionados manera apropiada debido que su pérdida o acceso no autorizado puede tener consecuencias muy significativas a nivel empresarial. En el sector farmacéutico se maneja datos sensibles como: desarrollo, análisis y acuerdos comerciales relacionado al campo farmacéutico. La seguridad informática es vital por lo cual en este trabajo de tesis se evaluó la seguridad TI de Acromax "Empresa farmacéutica de desarrollo, fabricación y comercialización de medicamentos de consumo humano", mediante pruebas de intrusión “pentesting” de hacking ético, siguiendo metodologías de código abierto altamente respetadas en la comunidad de la seguridad informática, las mismas que proporcionaron un marco de referencia y las directrices esenciales para llevar a cabo evaluaciones exhaustivas de seguridad como lo dictaminado por la metodología OWASP. La cual permitió simular ataques informáticos como un ciberdelincuente lo haría. Este análisis buscó verificar la eficacia de las medidas de seguridad implementadas dentro de la organización e identificar posibles vulnerabilidades existentes dentro de la misma. El estudio ofreció información valiosa para el análisis de brechas de seguridad dentro infraestructura TI mediante un informe de auditoría, que fue de uso exclusivo y confidencial de la organización.

Palabras claves: seguridad informática, infraestructura TI, pentesting, hacking ético, ciberseguridad.

Abstract

IT security is essential in companies, especially in the pharmaceutical sector. Due to the constant evolution of technology within corporations, the reliance on IT systems has brought with it challenges to face in organizations. Safeguarding IT infrastructure and data is a crucial task. The data that companies house as critical and high-value information must be managed appropriately because its loss or unauthorized access can have significant consequences at the enterprise level. The pharmaceutical sector handles sensitive data such as: development, analysis and commercial agreements related to the pharmaceutical field. IT security is vital, so in this thesis work the IT security of Acromax "Pharmaceutical company of development, manufacturing and marketing of medicines for human consumption" was evaluated through ethical hacking "pentesting" intrusion tests, following open-source methodologies highly respected in the IT security community, which provided a framework and essential guidelines to carry out comprehensive security assessments as dictated by the OWASP methodology. This allowed to simulate computer attacks as a cybercriminal would do. This analysis sought to verify the effectiveness of the security measures implemented within the organization and to identify vulnerabilities within the organization. The study provided valuable information for the analysis of security breaches within the IT infrastructure through an audit report, which was for the exclusive and confidential use of the organization.

Keywords: computer security, IT infrastructure, pentesting, ethical hacking, cybersecurity.

Índice general

Abreviaturas y simbologias

IP: Protocolo de internet.

PUERTO: Interfaz dedicada al envío y recepción de datos.

PROXY: Hardware o software dedicado a interceptar conexiones de redes desde un cliente a un servidor de destino de manera segura.

CMS: Sistema de gestión de contenido digital.

HTTP: Protocolo de transferencia de hipertexto.

GET: Modo de petición en código HTTP para indicar una acción de recuperación de datos.

POST: Método HTTP que envía datos al servidor.

MITM: Ciberataque mediante intervención del tráfico de los datos.

SQL: Lenguaje de consulta estructurado.

XSS: Inyección de scripts maliciosos dentro de sitios webs.

CSRF: Vulnerabilidad de falsificación de solicitudes entre sitios.

DNS: Sistema de nombres de dominio.

FUZZING: Técnica de pruebas de software, dedicada a determinar puntos débiles dentro de los sistemas.

PII: Información de identificación personal.

PATH: Técnica para referenciar un archivo o directorio en un sistema de archivos dentro de un sistema operativo.

WAF: Software que protege múltiples ataques al servidor de aplicaciones mediante análisis de paquetes de petición y modelos de tráfico.

Índice de tablas

Índice de figuras

INTRODUCCIÓN

En la era digital actual, la seguridad informática se ha vuelto esencial para empresas medianas y grandes. El uso de sistemas de información y las redes informáticas ha ampliado las oportunidades de mejora continua, pero también ha dado lugar a desafíos y riesgos en cuanto a la protección de la infraestructura tecnológica y la información que ésta alberga. La implementación adecuada de medidas de seguridad se ha vuelto fundamental para garantizar la integridad de los recursos y prevenir accesos no autorizados hacia la infraestructura de las organizaciones. La información es un activo valioso para las empresas, ya que en ella se encuentran datos críticos, como información financiera, estratégica, datos personales, entre otros datos de interés. La pérdida, alteración o acceso no autorizado a esta información puede tener consecuencias significativas, como pérdida de la confianza del cliente, daño a la reputación de la empresa, pérdida de ventaja competitiva, sanciones legales y financieras. Que, según La Ley Orgánica de Protección de Datos Personales del Ecuador, Art. 72 establece que “Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios” (Asamblea nacional del Ecuador, 2023). La ausencia de pruebas de intrusión de manera continua puede acarrear graves desventajas para las empresas, tal como ser objetivo de un ataque cibercriminal. Existen varios métodos usados por cibercriminales para atacar a las empresas, entre los más conocidos tenemos: phishing, ransomware, malware, ataques DDoS, entre otros mencionados en el OWASP top10 (OWASP, 2021). Los cibercriminales estudian a sus víctimas, no siempre usarán las mismas técnicas o ataques para realizar actos delictivos. Como, por ejemplo: la infección de malware que sufrió la empresa Novartis en el año 2022, por parte de un grupo de cibercriminales (Bleeping computer, 2022). Además, en el sector farmacéutico, donde se maneja información sensible de pacientes y se lleva a cabo investigación y desarrollo de medicamentos, la seguridad de la información adquiere una importancia aún mayor. En este contexto, se plantea la necesidad de evaluar la seguridad informática de Acromax S.A, un laboratorio farmacéutico dedicado al desarrollo, fabricación y

comercialización de medicamentos de consumo humano, con presencia en tres ciudades dentro del Ecuador: Quito, Cuenca y Guayaquil (planta y oficina), y con una plantilla que supera los 250 empleados a nivel nacional. La evaluación se llevará a cabo mediante pruebas de intrusión de hacking ético debido que se posiciona como una estrategia efectiva para reducir vulnerabilidades de los sistemas informáticos dentro de las organizaciones. Esta metodología, que combina la simulación de ataques desde el exterior o el interior de la red, ofrece una visión completa de la seguridad informática de la empresa, permitiendo identificar debilidades antes de que los cibercriminales las exploren y aprovechen de estas.

PLANTEAMIENTO DEL PROBLEMA

Actualmente, existe una creciente dependencia de los sistemas de información y las redes informáticas en este sector, lo que aumenta la importancia de salvaguardar los datos sensibles de los pacientes, la información estratégica y financiera, así como los resultados de investigación y desarrollo de medicamentos. Sin embargo, se requiere una evaluación exhaustiva y/o preventiva de la seguridad de la infraestructura tecnológica y la implementación de medidas adecuadas para prevenir accesos no autorizados, y la protección de la integridad de la información. Hasta ahora, se han realizado diversas investigaciones sobre la seguridad informática y las pruebas de intrusión en diferentes industrias, incluida la farmacéutica. Estos estudios han proporcionado información valiosa sobre los métodos y herramientas utilizados para evaluar la seguridad de los sistemas informáticos y las buenas prácticas para fortalecer las defensas cibernéticas. Sin embargo, los sistemas informáticos de Acromax S.A, y los de todas las empresas farmacéuticas del Ecuador, deben cumplir con varias regulaciones impuestas por entidades de control como ARCSA “La Agencia Nacional de Regulación, Control y Vigilancia Sanitaria (Arcsa), que es la entidad pública adscrita al Ministerio de Salud Pública (MSP) que se encarga de controlar y vigilar las condiciones higiénico – sanitarias de los productos de uso y consumo humano, además de brindar servicios que facilitan la obtención de permisos de funcionamiento y Notificaciones Sanitarias” (Arcsa, 2023). Debido a las normativas legales que

debe cumplir la empresa Acromax S.A, se realizara el análisis pertinente de su infraestructura tecnológica con finalidad de contribuir al cumplimiento de las normativas tecnológicas regularizadas por los organismos de control.

IDEA POR DEFENDER

El hacking ético de caja gris es una estrategia efectiva para reducir las vulnerabilidades de los sistemas informáticos en una empresa farmacéutica.

OBJETIVOS

Objetivo General

“Proporcionar información de valor que permita identificar vulnerabilidades de seguridad informática existentes dentro de la organización.”

Objetivos Específicos

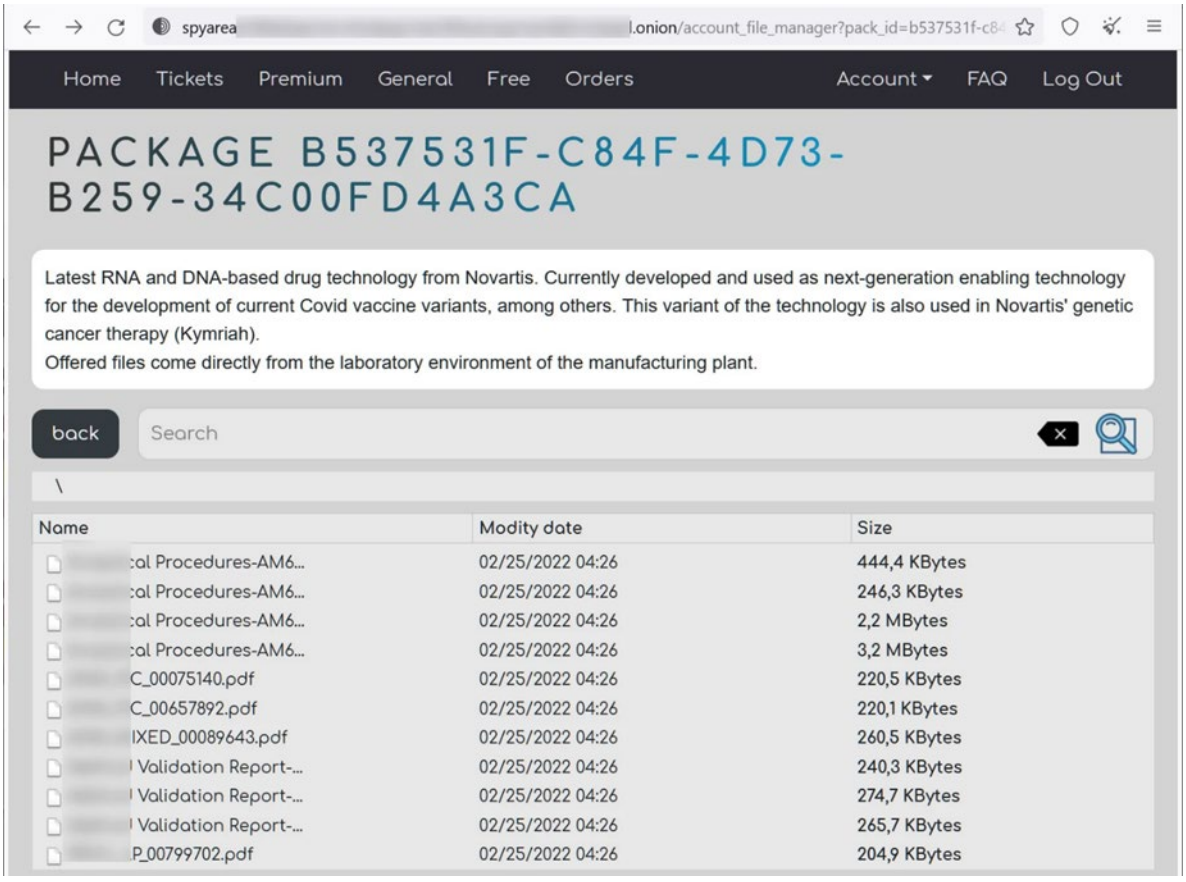
1) Recolectar información de interés de la empresa por medio de diversas técnicas de recolección de información
2) Analizar la información de los sistemas, puertos y servicios de la empresa mediante herramientas de escaneo certificadas.
3) Enumerar la información crítica recopilada por las herramientas de hacking ético.
4) Analizar las vulnerabilidades identificadas por las herramientas de hacking ético.
5) Generar un informe de auditoría que refleje los hallazgos del pentesting junto a sus recomendaciones de ciberseguridad.

JUSTIFICACIÓN

Actualmente en la era digital donde nos encontramos, donde las medianas y grandes empresas tienen una dependencia tecnológica relevante para sus diferentes actividades operativas, administrativas, financieras, entre otras altamente importantes. Es primordial reconocer los beneficios que las pruebas de hacking ético aportan a la seguridad informática de las empresas. Debido que estas pruebas, permiten evaluar la seguridad actual de los sistemas informáticos y redes de la empresa, al momento de implementarlo de manera

controlada y ética, se puede identificar posibles vulnerabilidades y riesgos de la ciberseguridad. La ausencia de estas pruebas de intrusión de manera continua puede acarrear graves desventajas para las empresas, tal como ser objetivo de un ataque cibercriminal, acarreando consecuencias como: pérdidas financieras, robo de información sensible, fraudes, entro otros delitos. Existen varios métodos usados por cibercriminales para atacar a las empresas, entre los más conocidos tenemos: phishing, ransomware, malware, ataques DDoS, entre otros. Los cibercriminales estudian a sus víctimas, no siempre usaran las mismas técnicas o ataques para realizar actos delictivos. Como por ejemplo la infección de malware que sufrió la empresa Novartis en el año 2022, por parte de un grupo de cibercriminales (Bleeping computer, 2022).

Figura 1. *Datos de Novartis vendidos en el mercado de extorsión Industrial Spy.*



Nota. La imagen muestra una lista de los archivos sustraidos con un peso total de 7.7 MB de archivos PDFs de la empresa Novartis , y posteriormente vendidos en un mercado negro del internet. Tomada de (BleepingComputer, 2022).

En vista, que hasta la más grande empresa puede ser víctima de un ataque, este trabajo de tesis busca aportar la mayor cantidad de sugerencias y recomendaciones para contribuir con la seguridad informática de la empresa Acromax S.A.

CAPÍTULO 1: MARCO TEÓRICO

La seguridad informática es un tema crucial en la actualidad, ya que los ataques cibernéticos pueden tener consecuencias catastróficas para las empresas y organizaciones que implementen soluciones informáticas. La información que se maneja en el sector farmacéutico es altamente sensible y muy apetecible para el mercado negro de la ciberdelincuencia, ya que es de las más valiosas y mejor pagadas hasta la actualidad (Lilliam Valenzuela, 2020)

El pasado 6 de febrero del 2022, existió el caso de un ataque informático mediante malware de tipo “ramsomware”, que ataco a los servidores y sistemas tecnológicos de INVIMA (“Instituto Nacional de Vigilancia de Medicamentos y Alimentos”), trayendo como consecuencia la indisponibilidad de información, sistemas, aplicativos webs, aplicativos de correo, entre otros. Por lo cual, como respuesta a este ataque, con el apoyo de equipos gubernamentales de respuesta a ataques informáticos, decidieron deshabilitar el portal web de la institución regulatoria colombiana, con la finalidad de salvaguardar la información. En todas las decisiones que se tomen a cualquier nivel dentro de las empresas del sector, la ciberseguridad debe estar siempre presente para poder implementar las medidas adecuadas que eviten vulnerabilidades y mantengan datos y sistemas bien protegidos (Ambit Team, 2022). Es por esto por lo que expertos en materia de ciberseguridad afirman que el correcto uso de planes en materia de ciberseguridad, tendrían como resultado la evasión y control de ataques cibernéticos (CERCAL group, 2022).

1.1 SEGURIDAD

La seguridad en su amplio espectro, se la considera como un concepto vital que está presente en múltiples aspectos de la sociedad y organizaciones. Según INSPQ (“Institut national de santé publique du Québec, 2018”), nos define la seguridad como:” el estado en el que se gestionan los riesgos y las

circunstancias que pueden ocasionar daños físicos, psicológicos o materiales, con el propósito de preservar la salud y el bienestar tanto a nivel individual como comunitario (Institut national de santé publique du Québec, 2018)". Los diversos desafíos de la seguridad en la actualidad y más "significativos", debido a la constante evolución de las amenazas que enfrentan estos campos son:

1. Desigualdad
2. Inseguridad Social
3. Inseguridad ambiental
4. Ciberdelincuencia

1.2 SEGURIDAD INFORMÁTICA

A la seguridad informática la podemos definir como "La disciplina encargada a la protección general de la información y los sistemas de cómputo contra amenazas internas y externas (Fernández & Cifuentes, 2022). Esta disciplina abarca todas las medidas y controles que se implementan para salvaguardar los recursos informáticos de una organización, tales como: software, hardware, redes informáticas, datos y servicios."

Los principales objetivos de la seguridad informática son la confidencialidad, la integridad y la disponibilidad de la información. Esto implica proteger los datos sensibles y restringir el acceso no autorizado, prevenir la alteración o destrucción no autorizada de la información y asegurar que los sistemas y servicios estén disponibles y funcionando correctamente cuando sean requeridos. En resumen, la seguridad informática abarca diversos aspectos relacionados con la protección de los sistemas de información y la prevención de amenazas cibernéticas. Asimismo, es importante implementar medidas de seguridad adecuadas y estar al tanto de las mejores prácticas y estándares en el campo de la seguridad informática.

1.3 SEGURIDAD INFORMÁTICA EN LA INDUSTRIA FARMACÉUTICA

La seguridad informática en la industria farmacéutica se ha vuelto un componente crítico debido a la creciente dependencia de la tecnología en las operaciones, almacenamiento y manejo de información sensible. La importancia de salvaguardar datos confidenciales, información financiera, investigación y otros activos se ha incrementado sustancialmente, dada a la

proliferación de amenazas cibernéticas (Klishchenko & Kuznetsov, 2022). Sin embargo, con la inversión adecuada en recursos, la integración de principios de seguridad y una mejora en la validación de sistemas, las empresas farmacéuticas pueden fortalecer su postura de seguridad y proteger sus valiosos activos en la era digital. Y reforzar aspectos tales como:

1. Protección de los datos sensibles de la industria farmacéutica.
2. Satisfacción de estándares y principios de gestión de la calidad.
3. Validación de información de los SGI

1.4 RIESGOS Y VULNERABILIDADES

En la actual era digital, donde la tecnología desempeña un papel crucial en casi todos los aspectos de nuestras vidas, la seguridad informática se ha convertido en una preocupación primordial. A medida que la interconexión y la dependencia de los sistemas informáticos aumentan, también lo hacen los riesgos y vulnerabilidades que acechan a la seguridad de la información y los activos digitales. En este contexto, comprender los conceptos de riesgos y vulnerabilidades informáticas se vuelve esencial para abordar de manera efectiva los desafíos que enfrentamos en la protección de la información y la infraestructura tecnológica. Cuando mencionamos riesgos orientados al campo informático estamos hablando de “la probabilidad de que un usuario no autorizado afecte negativamente a la confidencialidad, integridad y disponibilidad de los datos que se recopilan, transmiten o almacenan” (Paredes, 2022). A continuación, definimos las vulnerabilidades en el sector informático como “un punto de ruptura o brecha que identifica errores o problemas relacionados con la seguridad que pueden existir en el código del programa y los marcos de seguridad” (Redacción KeepCoding , 2022). Teniendo en cuenta que el riesgo es una probabilidad latente, el desconocimiento o inadecuada gestión de riesgos puede derivar una vulnerabilidad que puede ser explotada por personas no autorizadas o ajenas a la organización.

1.5 RIESGOS Y VULNERABILIDADES INFORMÁTICOS EN LA INDUSTRIA FARMACÉUTICA

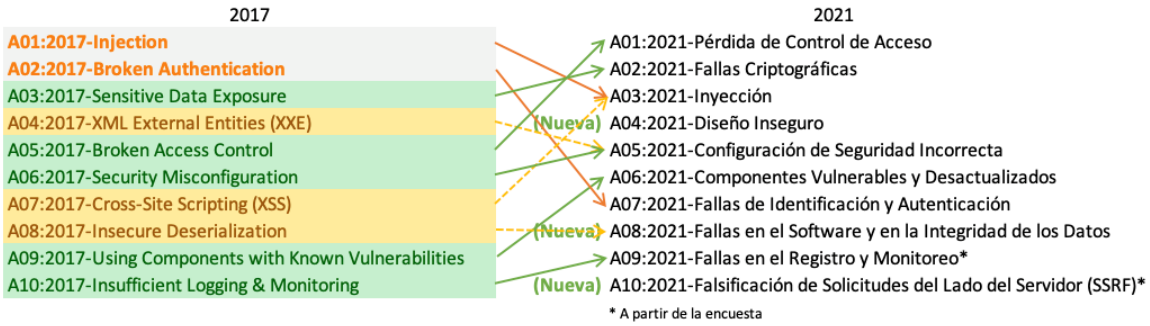
La industria farmacéutica se encuentra en un constante enfrentamiento con las amenazas de la ciberdelincuencia, un desafío particularmente intrincado debido al auge de la falsificación de productos farmacéuticos. Estos ataques no solo se perpetran por ganancias financieras, sino también por motivos de fama o incluso motivaciones políticas. La ciberdelincuencia posee el potencial de causar estragos en la marca y la reputación de las empresas farmacéuticas. Una vez que una organización es expuesta en los medios por violaciones de datos, la reconstrucción de la confianza pública se torna una tarea ardua. Los ciberdelincuentes pueden comprometer historiales de pacientes y solicitar rescates, creando una urgente necesidad de asegurar tanto las recetas médicas como los datos de investigación, ya que estas empresas están repletas de valiosa propiedad intelectual. En este complejo escenario, la dispersión de datos en fuentes no estructuradas resalta la importancia de procesos y procedimientos para la identificación, notificación y remediación de estos datos. Reducir el intercambio de información a través de historiales médicos electrónicos, portales de seguros y sitios de prescripción es esencial para salvaguardar información personal y sensible, además de recetas médicas y datos de investigación. No solo la ciberdelincuencia amenaza la industria farmacéutica, sino también la corrupción de datos, que puede desencadenar consecuencias catastróficas, incluida la pérdida de vidas. (Elazeem & El-Araby, 2020) (Sharma, Kumar, & Arora, 2022)

1.6 ATAQUE INFORMÁTICO

Mientras hacemos uso de la internet, ya sea para trabajar, estudiar, o navegar por algún sitio de nuestro interés, somos un posible objetivo de ataques informáticos. Un ataque informático según NetSoft Consulting lo define como: “un acto malicioso perpetrado por personas malintencionadas que utilizan virus informáticos o malware para infiltrarse en el servidor de un dispositivo, comprometer la seguridad, robar información confidencial y alterar el rendimiento del equipo” (Netsoft consulting, 2023).

Asimismo, IBM (International Business Machines Corporation), siendo una de las compañías tecnológicas más influyentes y respetadas a nivel global, realiza su aporte enfocado en el mundo de la ciberseguridad y nos define un ataque informático como: “intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas” (IBM, 2023). Con una visión más clara, acerca de la definición de ataques informáticos y sus consecuencias, gracias a OWASP, una entidad sin fines de lucro, reconocida mundialmente por sus aportes a la ciberseguridad, en su último entregable del OWASP top 10 correspondientes al año 2021. OWASP Top 10 cobra un papel crucial en el mundo de la seguridad informática, al identificar y categorizar los ataques más comunes que afectan las aplicaciones y servicios web que comúnmente son usados desde grandes corporaciones hasta servicios que llegan a ser usados por cualquier usuario que use la internet. Este listado proporciona una perspectiva valiosa sobre los riesgos cibernéticos inminentes.

Figura 2. *Comparativa de vulnerabilidades a partir de la encuesta de OWASP top 10.*



Nota. La imagen lista el orden de los ataques mas comunes en el periodo 2017-2021, y fueron reordenados según sus concurrencia en comparacion a los años anteriores. Tomada de (OWASP [fotografía], 2021).

Ahora que conocemos un listado de las amenazas mas frecuentes en la internet, se procede a describir brevemente las amenazas que en mi opinion personal son las mas relevantes para este trabajo de tesis. Las definicion sera descritas según OWASP (OWASP, 2021):

1. Perdida de Control de Acceso: “El control de acceso implementa el cumplimiento de política de modo que los usuarios no pueden actuar fuera de los permisos que le fueron asignados. Las fallas generalmente conducen a la divulgación de información no autorizada, la modificación o la destrucción de todos los datos o la ejecución de una función de negocio fuera de los límites del usuario”.

2. Fallas Criptograficas:” se refiere a debilidades o errores en la implementación o uso de algoritmos criptográficos, lo que puede resultar en la exposición de datos sensibles o la disminución de la efectividad de la seguridad criptográfica. Estas fallas pueden incluir el uso de algoritmos de cifrado obsoletos, problemas en la generación de claves, implementaciones incorrectas de cifrado, entre otros”.

3. Inyeccion: “una vulnerabilidad de seguridad que se produce cuando los datos no confiables son insertados en comandos o consultas de forma inadecuada en aplicaciones web. Estos ataques de inyección pueden aprovecharse para ejecutar comandos no deseados o manipular el comportamiento de la aplicación de manera maliciosa. Las formas comunes de inyección incluyen la Inyección SQL, la Inyección de Comandos y la Inyección de Código”.

4. Diseño Inseguro: “vulnerabilidad de seguridad que surge cuando las decisiones arquitectónicas y de diseño de una aplicación web no consideran adecuadamente los principios de seguridad. Un diseño inseguro puede permitir que los atacantes exploten vulnerabilidades en la aplicación de manera más efectiva, comprometiendo la confidencialidad, integridad y disponibilidad de los datos y servicios”.

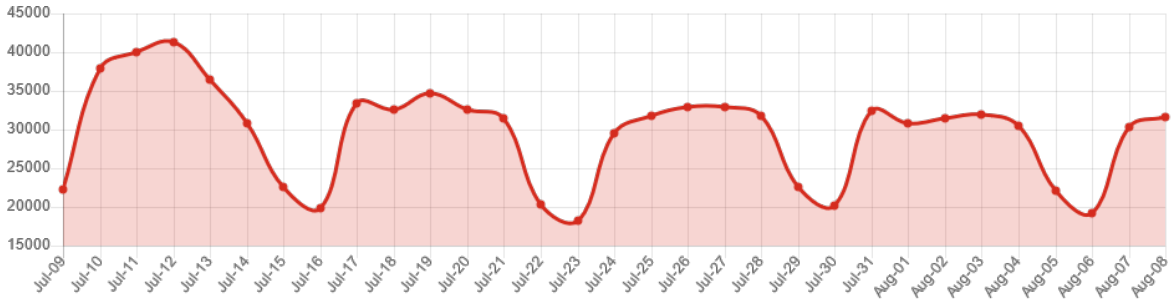
5. Configuración de Seguridad Incorrecta: “vulnerabilidad que surge cuando la configuración de sistemas, plataformas, aplicaciones o servicios web no se realiza de manera adecuada y segura. Esta falta de configuración adecuada puede exponer brechas de seguridad y debilidades que podrían ser aprovechadas por atacantes maliciosos”.

Con la nocion de un conocimiento general de los ataques mas comunes efectuados a nivel global, procederemos a conocer sobre la situacion actual de ciberataques en el Ecuador, según kaspersky con su herramienta web https://cybermap.kaspersky.com/es , que nos permite visualizar en tiempo real, los ciberataques efectuados por pais. En el caso del pais Ecuador, este se encuentra situado en el puesto #51 según Kaspersky (AO Kaspersky Lab, 2021). Mediante diferentes herramienta de analisis y evaluacion de amenazas como:

- OAS (On-Access Scan): muestra el flujo de detección de malware durante el escaneo On- Access, por ejemplo, cuando los objetos son accesados durante las operaciones abrir, copiar, ejecutar o guardar operaciones.
- ODS (On Demand Scanner): muesta el flujo de detección de malware durante el análisis bajo pedido, cuando el usuario selecciona manualmente la opción "Buscar virus" en el menú de contexto.
- MAV (Mail Anti-Virus): muestra el flujo de detección de malware durante el escaneo MAV cuando aparecen nuevos objetos en una aplicación de email (Outlook, The Bat, Thunderbird).MAV escanea los mensajes entrantes y llama a OAS cuando guarda los adjuntos a un disco.
- WAV (Web Anti-Virus): muestra el flujo de detección de malware durante el análisis de Web Anti-Virus cuando se abre la página html de un sitio web o se descarga un archivo.
- IDS (Intrusion Detection Scan): muestra el flujo de detección de los ataques a las redes.
- VUL (Vulnerability Scan): muestra el flujo de la detección de vulnerabilidades.
- KAS (Kaspersky Anti-Spam): muestra el tráfico sospechoso y no deseado descubierto por las tecnologías de filtrado de reputación de Kaspersky.
- BAD (Botnet Activity Detection): muestra estadísticas sobre direcciones IP de víctimas de ataques DDoS y servidores botnet.

Las modalidades de ataque y recoleccion de informacion se han detectado en modalidad OAS y ODS, lo cual observamos a continuacion mediante graficos:

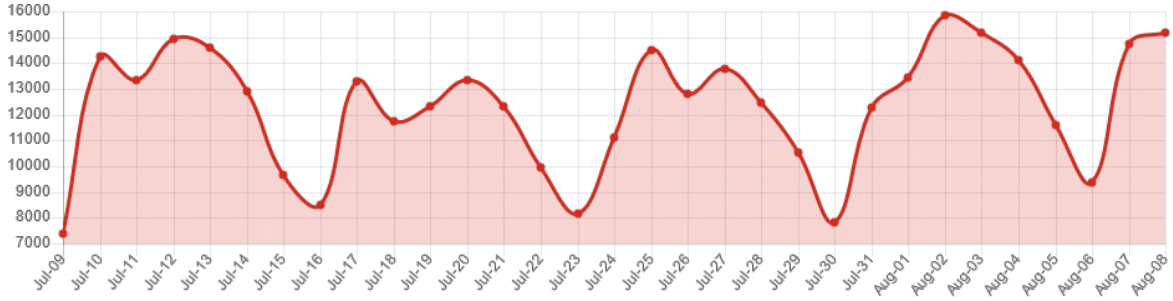
Figura 3. *Detección de ciberataques durante julio-09 hasta agosto-08 del año 2023.*



Nota. El día 12 de julio de 2023 se detectó la mayor cantidad de ciberataques mediante la modalidad de OAS con una cifra de 41257 ciberataques. Tomada de (AO Kaspersky Lab, 2023).

Por otro lado, tenemos estadisticas de deteccion bajo la modalidad ODS, que nos muestra:

Figura 4. *Estadísticas de ciberataques realizados durante julio-09 hasta agosto-08 del año 2023.*



Nota. El dia 2 de agosto de 2023 se detecto la mayor cantidad de ciberataques mediante la modalidad de ODS con una cifra de 15855 ciberataques. Tomada de (AO Kaspersky lab, 2023).

La seguridad informática en el Ecuador enfrenta una serie de riesgos y vulnerabilidades que requieren una atención y capacitación continua. La colaboración entre el gobierno, las empresas y la sociedad en general es

esencial para fortalecer las defensas cibernéticas, fomentar la educación en ciberseguridad y garantizar un entorno en línea más seguro y resiliente para todos.

1.7 CIBERSEGURIDAD

La ciberseguridad, como una rama esencial de la seguridad informática, adquiere una relevancia ineludible en la protección de los recursos digitales y la preservación de la privacidad en la era de la información. Conforme la sociedad y las empresas depositan una confianza creciente en la tecnología para sus operaciones a diario, asimismo se vuelven más susceptibles ante una gama diversa de amenazas cibernéticas que pueden poner en peligro la confidencialidad, integridad y disponibilidad de la información. Según CISA (Cybersecurity & Infrastructure Security Agency) define la ciberseguridad como: “La ciberseguridad es la práctica de proteger sistemas, redes y programas informáticos de ataques digitales. Estos ataques a menudo tienen como objetivo acceder, cambiar o destruir información valiosa; extorsionar dinero de los usuarios; o interrumpir los procesos normales de negocio (Cybersecurity & Infrastructure Security Agency , 2023)”. Teniendo en cuenta que, la ciberseguridad no puede pasar por alto como una responsabilidad para las empresas, existen normativas de ciberseguridad por cumplir para así poder garantizar los principios fundamentales de la información, si bien es cierto que, no existe ley global de ciberseguridad a la cual todas las empresas deban acogerse. Existen leyes por países que deben aplicarse con responsabilidad con un enfoque en la ciberseguridad, como, por ejemplo: “La ley de protección de datos”, esta ya es una realidad en el Ecuador y en muchos países del mundo. Gracias a la globalización de la internet y sus componentes, existen estándares por cumplir para tener una correcta ciberseguridad implementada en las empresas.

1.8 CERTIFICACIONES DE CIBERSEGURIDAD

Debido a la importancia que adquiere tener buenas prácticas de ciberseguridad en el mundo corporativo, para realizar contratos, negociaciones o prestaciones de servicio, no basta con implementar medidas correctas de ciberseguridad, sino tener un respaldo o alguna evidencia que dichas prácticas están siendo

implementadas mediante algún medio certificador, es allí donde las certificaciones de seguridad adquirir un rol importante en el mundo corporativo, que según ESIC define la certificaciones de ciberseguridad como: ”fundamentalmente, se trata de un archivo o registro que certifica que un individuo posee conocimientos específicos en el campo de la ciberseguridad y la tecnología, validando su capacidad para llevar a cabo diversas tareas dentro de este dominio (ESIC business, 2022)”. Actualmente, existen muchas certificaciones de ciberseguridad, que van desde un nivel inicial hasta certificaciones para niveles avanzados, cabe recalcar que las certificaciones no se miden en relación si una es mejor que otra. Si no más bien, el modelo de negocio que gire en torno a la empresa o al interesado en adquirir la certificación. Entre las certificaciones más demandadas según Coursera se listan las siguientes:

a. CompTIA Security+.

b. GIAC Security Essentials (GSEC).

c. Offensive Security Certified Professional (OSCP).

d. CISSP (Certified Information Systems Security Professional).

Estas certificaciones no solo validan las capacidades técnicas y estratégicas de la empresa en la protección de sus activos digitales, sino que también demuestran un compromiso inquebrantable con la integridad, la confidencialidad y la privacidad de los datos confiados a su cuidado. Al adoptar y aplicar los estándares y prácticas validados por estas certificaciones, las empresas no solo se protegen a sí mismas contra amenazas internas y externas, sino que también fortalecen la confianza de sus clientes y socios.

1.9 HACKING ÉTICO

A principios del siglo XXI, el hacking ético emergió como una respuesta a la creciente sofisticación de los ataques cibernéticos. Las organizaciones comenzaron a reconocer la necesidad de identificar vulnerabilidades antes de que fueran explotadas por atacantes maliciosos. Esto condujo a la popularización de las pruebas de penetración, donde profesionales capacitados intentan acceder a sistemas con el permiso del propietario, para identificar y

corregir debilidades. Según CompTIA (Computing Technology Industry Association), empresa certificadora de implementaciones TI a nivel mundial, define el hacking ético como: “la práctica de simular ataques cibernéticos con el objetivo de identificar vulnerabilidades en sistemas y redes. A diferencia de los hackers maliciosos, los hackers éticos operan con permiso y con el propósito de fortalecer la seguridad, en lugar de explotarla, también llamado como pentesting o pruebas de penetración (CompTIA, 2022)”. La implementación del hacking ético dentro de las corporaciones es crucial en un panorama digital cada vez más hostil. Existen múltiples razones por lo cual implementar esta práctica beneficiaria a las empresas, tales como:

1. Identificación Proactiva de Vulnerabilidades
2. Mejora de la Ciberdefensa
3. Cumplimiento Normativo
4. Protección de la reputación
5. Aprendizaje y capacitación continua

1.10 METODOLOGÍA DE EVALUACIÓN DE VULNERABILIDADES

Es importante utilizar metodologías de evaluación de vulnerabilidades informáticas debido que la necesidad de fortalecer la postura de seguridad cibernética de las organizaciones en un entorno digital cada vez más complejo y amenazante. Estas metodologías, diseñadas para identificar y analizar debilidades en sistemas y redes, desempeñan un papel fundamental en la prevención de ataques cibernéticos y la protección de datos sensibles proporcionando una estandarización de procesos para así garantizar resultados de las pruebas. Según Dale Gartner en su informe Magic Quadrant for Application Security Testing nos mencione que: “la implementación de metodologías de evaluación de vulnerabilidades es esencial para anticipar posibles puntos de acceso para los atacantes y remediarlos de manera proactiva (Gartner, Inc, 2021)”. La aplicación constante de estas medidas de seguridad como las pruebas de intrusión con las metodologías pertinentes permiten a las organizaciones identificar vulnerabilidades ocultas y resolverlas antes de que puedan ser explotadas por amenazas cibernéticas. Existen varias

metodologías de código abierto para implementar evaluaciones de vulnerabilidades entre las cuales se encuentran:

1. Metodología OWASP (“Open Web Application Security Project”): esta metodología se centra en la seguridad de los aplicativos webs, y tiene como objetivo identificar y mitigar vulnerabilidades. Dentro del marco de trabajo de esta metodología se analiza vulnerabilidades y ataques cibernéticos, muy recurrentes en periodos de 5 años, lo cual permite que en este tiempo se pueda analizar y estudiar los ciberataques más frecuentes. Asimismo, OWASP proporciona varios entregables para garantizar un trabajo de análisis exhaustivo, entre los cuales tenemos:

- OWASP top 10: entregable realizado mediante diferentes aportes de la comunidad activa relacionada con la seguridad informática, esta entregable lista las 10 principales vulnerabilidades de seguridad en aplicaciones web y su frecuencia.
- OWASP Web Security Testing Guide Checklist: es una lista de verificación que forma parte del proyecto OWASP, esta es una guía que proporciona orientación detallada sobre cómo realizar pruebas de seguridad dentro de los aplicativos webs. Dentro de la misma, encontramos técnicas, consejos y herramientas para cada fase de las pruebas de manera sistemática y completa.

2. Metodología OSSTMM (“Open-Source Security Testing Methodology Manual”): esta metodología de seguridad tiene un enfoque más amplio debido que puede aplicarse a diversos aspectos de la seguridad informática dentro de las organizaciones, tener como referencia esta metodología es un aspecto complementario al implementar un análisis de vulnerabilidades.

Debemos tener en cuenta que cada metodología tiene sus propias ventajas y enfoques. La elección de la metodología dependerá de los objetivos de la prueba, el tipo de sistema o red que se esté evaluando y la experiencia del profesional de seguridad.

CAPÍTULO 2: METODOLOGÍA

Para la elección de la metodología adecuada en base a las necesidades de la empresa Acromax, se llevó un análisis exhaustivo de las metodologías existentes en la actualidad. Por lo cual, la metodología OWASP 4.2, fue la metodología escogida para seguir en este trabajo de tesis, ya que ofrece beneficios de acorde a las exigencias de la organización. La elección de esta metodología permitió que durante las pruebas de intrusión se adquiriera diferentes beneficios como un enfoque integral, métodos y herramientas actualizadas, recursos gratuitos y documentados, y una comunidad activa en las pruebas de intrusión de hacking ético. Cabe recalcar que OWASP proporciono un marco sólido y confiable para evaluar y mejorar la seguridad de los aplicativos de la organización. El alcance de este pentesting fue de caja gris, debido que este responde a una colaboración con el objetivo y un nivel de intrusión moderado y acordado con el departamento a cargo de la seguridad informática de la organización.

Para este trabajo de tesis, se ha escogido un enfoque cuantitativo, debido a que la evaluación de hacking ético implico evaluaciones técnicas y análisis exhaustivos, que como resultados de estos procedimientos se pudo recolectar:

1. Datos cuantitativos: se obtuvo un número de vulnerabilidades identificadas, nivel de riesgos asociados a las vulnerabilidades e impacto potencial en los sistemas implicados.
2. Resultados medibles: cantidad de vulnerabilidades con medidas de mitigación y porcentaje de riesgos de las vulnerabilidades.
3. Métricas de seguridad: las pruebas de intrusión usaron métricas de seguridad específico para evaluar el nivel de riesgo y efectividad de las medidas de seguridad implementadas en la infraestructura de TI de la organización.

Previo a la inicialización del pentesting, se debe implementar un entorno de trabajo al cual se lo denominara “laboratorio de hacking ético”.
Este laboratorio debe cumplir con varios componentes, los cuales permitan realizan las pruebas de intrusión sin limitaciones por hardware o software. Por

lo cual para este trabajo de tesis de implemento el siguiente laboratorio, el cual se observa mediante la siguiente tabla:

Tabla 1. *Entorno de trabajo para hacking ético de caja gris para este trabajo de tesis.*

Tipo de herramienta	Nombre de la herramienta	Versión
Hardware	Laptop Hasee i9	FX
Sistema Operativo	Windows 11 Pro	22H2
Virtualizador	VMware® Workstation 17 Pro	17.0.2 build-21581411
Distribución Linux	Kali GNU/Linux	2023.3

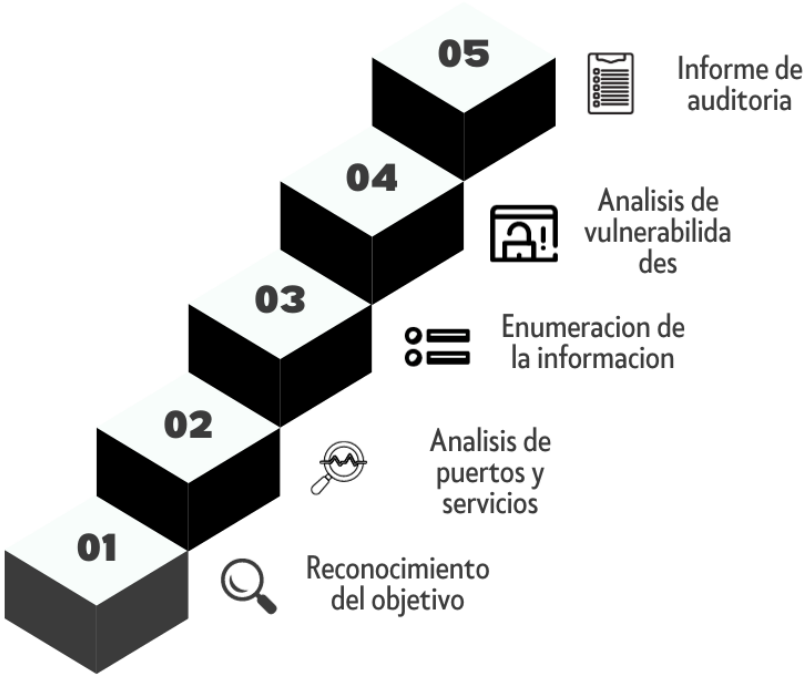
Nota. Las herramientas listadas fueron usadas para realizar cada fase del proceso de hacking ético, estas herramientas fueron actualizadas a su última versión estable. Elaborado por: Autor.

Gracias a la colaboración del departamento TI de Acromax, el pentesting que se escogió en base a las necesidades de la organización, fue el pentesting de caja gris, ya que este implico una previa colaboración de información de la infraestructura TI. El cual consistió en un listado de IPs expuestas al internet, el cual se evidencia a continuación:

1. 190.12.27.138
2. 186.47.208.179
3. 190.154.255.178
4. 186.69.165.4

De acorde a lo recomendado por la metodología OWASP, los pasos realizados durante este pentesting, se los evidencia mediante el siguiente grafico:

Figura 5. *Pasos definidos para realizar el pentesting de caja gris*



Nota. Los pasos para realizar un pentesting van de acorde al tipo de pentesting y lo acordado con la empresa. En este caso se omitió la explotación de las vulnerabilidades. Elaborado por: Autor.

A continuación, se describe en que consistió cada fase del pentesting:

2.1 RECONOCIMIENTO DEL OBJETIVO

Para la etapa inicial de este trabajo de pentesting, la etapa de reconocimiento desempeño un papel crucial para establecer bases sólidas de información debido que ayudo a comprender el escenario de evaluación mediante distintas técnicas y herramientas recomendadas por la metodología OWASP a través de su entregable OWASP Web Security Testing Guide Checklist, debido que este entregable es una guía robusta para realizar pruebas exhaustivas de los aplicativos y servicios web. Cabe recalcar que se realizó dos tipos de reconocimiento: reconocimiento pasivo y reconocimiento activo. Una vez preparado el entorno se procedió con las técnicas y herramientas de reconocimiento según OWASP_WSTG_Checklist. Se uso aplicativos de reconocimiento web haciendo uso del navegador Mozilla Firefox con motor de búsqueda Google. Dentro de este se usó herramientas como: Google Dorking,

Wappalyzer y Shodan, WayBackMachine, etc. A continuación, mediante una tabla informativa se detallará las herramientas y sus respectivos enlaces en internet. Mediante una tabla informativa, se lista las distintas herramientas usadas para el reconocimiento del objetivo, el uso de varias herramientas se debe a que la implementación de varias podía recoger más información valiosa o a su vez corroborar la información encontrada.

Tabla 2. *Herramientas usadas para el reconocimiento de la empresa*

HERRAMIENTA	URL
Google Dorking	*https://www.exploit-db.com/google-hacking-database*
Wappalyzer	*https://www.wappalyzer.com/*
Shodan	https://www.shodan.io/
Wayback Machine	https://archive.org/web/

Nota. La tabla se muestra como evidencia las diversas herramientas al alcance del usuario común junto a su URL correspondiente. Elaborado por: Autor.

El uso de estas herramientas permitió buscar información en relación con los diferentes aplicativos, servicios, dominios y otros datos de interés del objetivo. Después del reconocimiento mediante herramientas web, se realizó reconocimiento con herramientas en Kali Linux, con el propósito de recoger la mayor cantidad de información existente en la internet. Se ejecuto instrucciones de reconocimiento y enumeración de escáner CGI Nikto v2.5.0, la cual nos permite realizar intercambios de datos entre los servidores y aplicaciones externas de una manera estandarizadas para detectar información importante como IPs y subdominios asociados. Asimismo, se procedió a usar el framework llamado recon-ng, diseñado para elaborar un entorno de reconocimiento exhaustivo y rápido basado en la información web. Una vez realizado el pertinente proceso de reconocimiento, se procedió a realizar un análisis de la información recolectada mediante las distintas herramientas usadas. Para así realizar una planificación adecuada para las fases posteriores del hacking ético.

A continuación, se explica en qué consisten los diferentes tipos de reconocimiento realizados durante esta evaluación de hacking ético.

2.1.1 RECONOCIMIENTO PASIVO

Durante esta fase de la evaluación se enfocó en la recopilación de información sin realizar una interacción directa con el objetivo. Es decir que las técnicas y herramientas actuaron de manera pasiva para recopilar la información, sin escaneos intrusivos o alguna acción que pueda generar una alarma para la infraestructura TI. El objetivo principal de este tipo de reconocimiento fue obtener información valiosa sobre los aplicativos de la organización expuesta en la internet, al alcance del usuario común. Para esta fase se enumeró actividades como:

1. Enumeración de hosts y servicios: consistió en identificar los sistemas y servicios que están en funcionamiento y/o disponibles en el entorno de los aplicativos webs. Estos incluyeron la identificación de las direcciones IP, puertos abiertos y servicios activos.
2. Mapeo de la arquitectura de la aplicación: consistió en obtener información que ayudo a comprender la estructura y arquitectura de la aplicación web. La cual incluyo identificación de servidores web, bases de datos o aplicaciones de terceros usadas por el aplicativo web.
3. Enumeración de tecnologías utilizadas: durante este procedimiento se identificó las tecnologías y plataformas asociadas directa e indirectamente con el aplicativo web, como el lenguaje de programación, sistema gestor de base de datos, marcos de desarollo, etc.
4. Recopilación de información sobre miembros de la organización: mediante el uso de búsquedas avanzadas en la internet, se logró obtener información como correos y usuarios de miembros activos e inactivos de la organización.
5. Recopilación de información pública: la búsqueda de información pública en fuentes como motores de búsqueda, registros públicos, sitios web y redes sociales, permitió identificar patrones e información de utilidad para el análisis de esta.

2.1.2 RECONOCIMIENTO ACTIVO

Para esta fase de reconocimiento activo, se implementó medidas que implico una interacción directa con los aplicativos descubiertos en la fase de reconocimiento pasivo, con la finalidad de recopilar información más detallada sobre configuraciones, vulnerabilidades expuestas y posibles puntos de entrada. A diferencia del reconocimiento pasivo, este reconocimiento implico acciones proactivas que generaron tráfico y alertas a la infraestructura de la organización. Los puntos que a tomar en cuenta sobre este tipo de reconocimiento son:

1. Riesgo de detección: durante este reconocimiento se realizó técnicas para la implementación adecuada de las herramientas de reconocimiento para que estas no fueran intrusivas al momento de recopilar información.

2. Recopilación de información más detallada: Es reconocimiento activo logro obtener información más detallada acerca de la estructura de la aplicación.

3. Identificación de brechas de seguridad: durante este reconocimiento se pudo encontrar vulnerabilidades, configuraciones indebidas y puntos de referencia para la planificación de ataques informáticos.

La implementación sistemática de ambos tipos de reconocimiento permitió una planificación efectiva para realizar las siguientes fases del pentesting, partiendo de una robusta comprensión de la información adquirida sobre la infraestructura de los aplicativos identificados durante esta fase inicial.

2.2 ANÁLISIS DE PUERTOS Y SERVICIOS

Posterior a la etapa de reconocimiento, en beneficio a la información recolectada. Durante esta etapa se realizó un análisis exhaustivo en función a la información obtenida, ya que la metodología OWASP nos indica razones claves por la cual realizar este análisis, aspectos claves como:

1. Identificación de superficie de ataque: el análisis de puertos y servicios permitió identificar puntos de entrada dentro lo los aplicativos usados por el objetivo.

2. Detección de servicios externos: se identificó tanto servicios como aplicaciones de terceros usadas por el objetivo y expuestas al internet. Esto con la finalidad de evaluar los riesgos asociados con la dependencia de terceros.
3. Identificación de vulnerabilidades potenciales: durante la identificación de servicios y puertos se pudo evidenciar vulnerabilidades potenciales que podría ser aprovechadas por atacantes.
4. Priorización de actividades de prueba: el análisis de puertos y servicios proporciono información valiosa para priorizar las actividades de pruebas en áreas críticas identificadas.

Durante el desarrollo de esta fase se implementó técnicas y herramientas para el análisis de puertos y servicios, entre las que se destaca: análisis automatizado con programadas dedicados y pruebas manuales de acorde a los servicios y puertos identificados. La etapa del escaneo de vulnerabilidades dentro de este pentesting fue una fase crítica en el proceso de evaluación, ya que permitió identificar los servicios y puertos en uso por parte del objetivo existentes dentro de la infraestructura. Esta fase permitió al autor del pentesting comprender mejor la infraestructura de la organización para diseñar un plan de posibles ataques en base a la información obtenida. A continuación, se describe mediante una tabla, las herramientas usadas para el análisis de la infraestructura:

Tabla 3. *Listado de herramientas usadas para los diferentes escaneos realizados.*

Tipo de escaneo	Herramienta
Escaneo de puertos y servicios	Nmap v7.94
Escaneo de dominios	DiG 9.19.17-1-Debian
Escaneo automatizado de puertos y servicios con scripts	Bash versión 5.2.15 y Python 3.11.6

Nota. La tabla contiene el listado de herramientas usadas para los diferentes escaneos realizados en este trabajo de hacking ético junto a las versiones de cada herramienta. Elaborado por: Autor.

Esta fase permitió comprender y abordar amenazas y riesgos que puedan afectar a la seguridad informática de los aplicativos asociados a la organización, y para tomar decisiones informadas sobre la implementación de medidas de seguridad adecuadas.

2.3 ENUMERACIÓN DE LA INFORMACIÓN

La fase de enumeración de la información durante este trabajo de pentesting permitió:

1. Identificación integral de la superficie de ataque: durante la fase de enumeración se realizó una identificación exhaustiva de los activos, recursos, y servicios asociados e identificados durante fases previas a la enumeración. Lo cual ayudo a planificar la superficie de ataque en su totalidad, ya que esta fue esencial para una evaluación completa de la seguridad informática.
2. Detección de posibles puntos de entrada: al enumerar la información recolectada sobre la infraestructura del objetivo, se logró identificar varios posibles puntos de entradas susceptibles a ataques informáticos. Esto abarco desde rutas de acceso a datos sensibles, hasta interfaces de usuarios vulnerables, lo que ayudo a determinar áreas de alto riesgo.
3. Evaluación de riesgos y amenazas: esta fase de enumeración ayudo a priorizar actividades durante el pentesting, debido que, al identificar los componentes y áreas más críticas, se logró asignar recursos y tiempo de manera eficiente.

Es importante destacar que la enumeración se llevó a cabo de manera ética y dentro de los límites legales y acuerdos establecidos con Acromax S.A.

La herramienta usada para el análisis de la información fue CherryTree 1.0.1: “Una aplicación jerárquica para tomar notas, con texto enriquecido y resaltado de sintaxis, que almacena datos en un solo archivo (XML o sqlite) o en varios archivos y directorios”. Debido que esta herramienta es multiplataforma y fue usada dentro de un entorno Linux como Windows debido a la versatilidad que esta brinda al ser multiplataforma.

2.4 ANÁLISIS DE VULNERABILIDADES

Esta fase de análisis de vulnerabilidades, de acorde a la metodología OWASP se la considera critica, debido que identificar amenazas y debilidades existentes dentro la infraestructura es fundamental. Por lo cual se destaca razones claves de esta fase como lo fueron:

1. Identificación de amenazas y debilidades: esta fase permitió realizar una evaluación profunda de las aplicaciones asociadas al objetivo, en busca de amenazas y debilidades de seguridad. Este incluyó las mencionadas en el entregable OWASP TOP 10.
2. Descubrimiento de vulnerabilidades únicas: esta fase de análisis permitió descubrir vulnerabilidades específicas de los aplicativos que no son evidente mediante un análisis superficial. Estas vulnerabilidades únicas incluyen fallos de lógica o problemas de seguridad.
3. Planificación de medidas correctivas: la identificación adecuada de las vulnerabilidades proporcionó una base sólida para planificar medidas correctivas de seguridad.
4. Priorización de acciones correctivas: este análisis permitió ayudar a priorizar las acciones correctivas en función a la gravedad y probabilidad de explotación de las vulnerabilidades identificadas.

En esta fase, se buscó de manera sistemática y automatizada cualquier debilidad, error o fallo dentro de los aplicativos expuestos a la internet, debido que estos podrían ser aprovechados por un atacante para comprometer la seguridad informática de la organización. La metodología de análisis de vulnerabilidades en base a lo recomendado por la metodología OWASP, ofrece diversos puntos de evaluación como:

1. Escaneo de vulnerabilidades por tipo de escaneo.
2. Revisión de código en busca de vulnerabilidades
3. Pruebas de penetración controladas en vulnerabilidades

En la etapa de análisis de las vulnerabilidades dentro de los aplicativos de la empresa, se usó la herramienta recomendada por la metodología OWASP, La herramienta OWASP ZAP 2.13 en modo ataque la cual realizo múltiples

pruebas de intrusión como:

1. Inyección de payloads: este tipo de intrusión introduce campos de entradas para poder evaluar la resistencia de la aplicación frente ataques como inyección SQL, XSS, entre otros.

2. Fuzzing automatizado: esta técnica sirve para enviar datos de prueba en masa con el fin de detectar posibles deficiencias en la gestión de datos y errores.

3. Man in the Middle (MITM): este tipo de ataque permite evaluar la seguridad de la comunicación entre el cliente y el servidor, identificando posibles vectores de ataque durante el análisis.

4. Escaneo de seguridad avanzada: consiste en la búsqueda de vulnerabilidades conocidas por el OWASP TOP 10 o desconocidas, incluyendo la identificación de configuraciones susceptibles a vulnerarse.

Se hizo uso de la herramienta JoomScan v 0.0.7 (“Un proyecto en lenguaje de programación Perl para detectar vulnerabilidades del CMS Joomla y analizarlas”), el uso de esta herramienta es de uso especifico, debido que en la etapa de reconocimiento se evidencio que el gestor de contenidos de la página web es la herramienta Joomla, y mediante esta herramienta podremos encontrar datos asociados a la misma.

2.5 INFORME DE AUDITORIA

Para fase final de este pentesting, la elaboración del informe de auditoría consistió en la documentación pertinentes de los hallazgos y recomendaciones para mejorar la seguridad de los sistemas usados por la organización en sus operaciones cotidianas. En función, a lo recomendado por la metodología OWASP, esta proporciono una estructura clara para la elaboración de este informe de auditoría, en donde se detallan aspectos métricos fundamentales para la comprensión del cuerpo del informe. El informe de auditoría tuvo como objetivo proporcionar una visión clara de las vulnerabilidades y riesgos de seguridad existentes, para que de esta manera los encargados de la infraestructura TI, puedan tomar decisiones en base a información del pentesting realizado hacia la organización. Haciendo uso de herramientas

como OWASP WSTG Checklist, se logró adjuntar dentro del informe entregado a la organización de manera implícita los hallazgos relevantes para la mejora de la seguridad informática. Para el desglose de los resultados del impacto de los riesgos se categorizo bajo parámetros los cuales se definen de la siguiente manera:

TABLA 1. *Tipo de severidad de vulnerabilidades y definición.*

Severidad	Definición
Alto	El riesgo de explotación por vulnerabilidad detectada podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad operación.
Medio	En este contexto, las vulnerabilidades existen, pero no son explotables, sin un ataque previo como: ataques de phishing o ingeniería social. Sin embargo, puede llegar a convertirse en una severidad alta, si los ataques previos se realizan con efectividad.
Bajo	Las vulnerabilidades detectadas no son explotables, pero reducir las mismas, reduce una superficie de ataque para la organización.
Informativo	No existe una vulnerabilidad, pero se otorga información adicional sobre los elementos analizados durante las pruebas, y se aconseja controles y documentaciones adicional.

Elaborado por autor.

CAPÍTULO 3: RESULTADOS DE LA EVALUACIÓN DE HACKING ÉTICO

En este capítulo de tesis, se presentarán los resultados del pentesting de caja gris realizado, en donde se utilizó la metodología OWASP. Se describirá las fases correspondientes a la metodología implementada, así como los hallazgos resultantes de la prueba de intrusión.

3.1 RECONOCIMIENTO DEL OBJETO: ACROMAX S.A

Para esta fase inicial, el primer objetivo de análisis fueron las IPs entregadas por el departamento TI de Acromax. Cabe recalcar que las IPs fueron listadas por medio de un correo eléctrico, sin ningún tipo de información adicional. Por lo cual mediante técnicas y herramientas de reconocimiento se pudo recolectar información relacionada a estas IPs.

Tabla 4. *Reconocimiento pasivo a las IPs entregadas por Acromax.*

IP	Subred	ASN	Proveedor
190.12.27.138	190.12.27.0/24	22724	PUNTONET
186.47.208.179	186.47.208.0/22	28006	CNT EP
190.154.255.178	190.154.0.0/16	14522	Satnet
186.69.165.4	186.69.160.0/19	14522	Satnet

Nota. Esta tabla contiene la información recopilada por las herramientas web a partir de las IPs entregas por la organización. Elaborado por: Autor.

Es importante resaltar que identificar la subred y/o número del sistema autónomo, de ahora en adelante denominado ASN, permite realizar ataques o campañas de ingeniería social o phishing.

Al finalizar el reconocimiento de las IPs entregadas, se procedió a realizar un reconocimiento pasivo del aplicativo web de la organización publicado en internet, con la URL: https://www.acromax.com.ec/. Mediante técnicas y herramientas disponible en la internet, se evidencia mediante una tabla lo recopilado:

Tabla 5. *Reconocimiento pasivo de la página web de la organización*

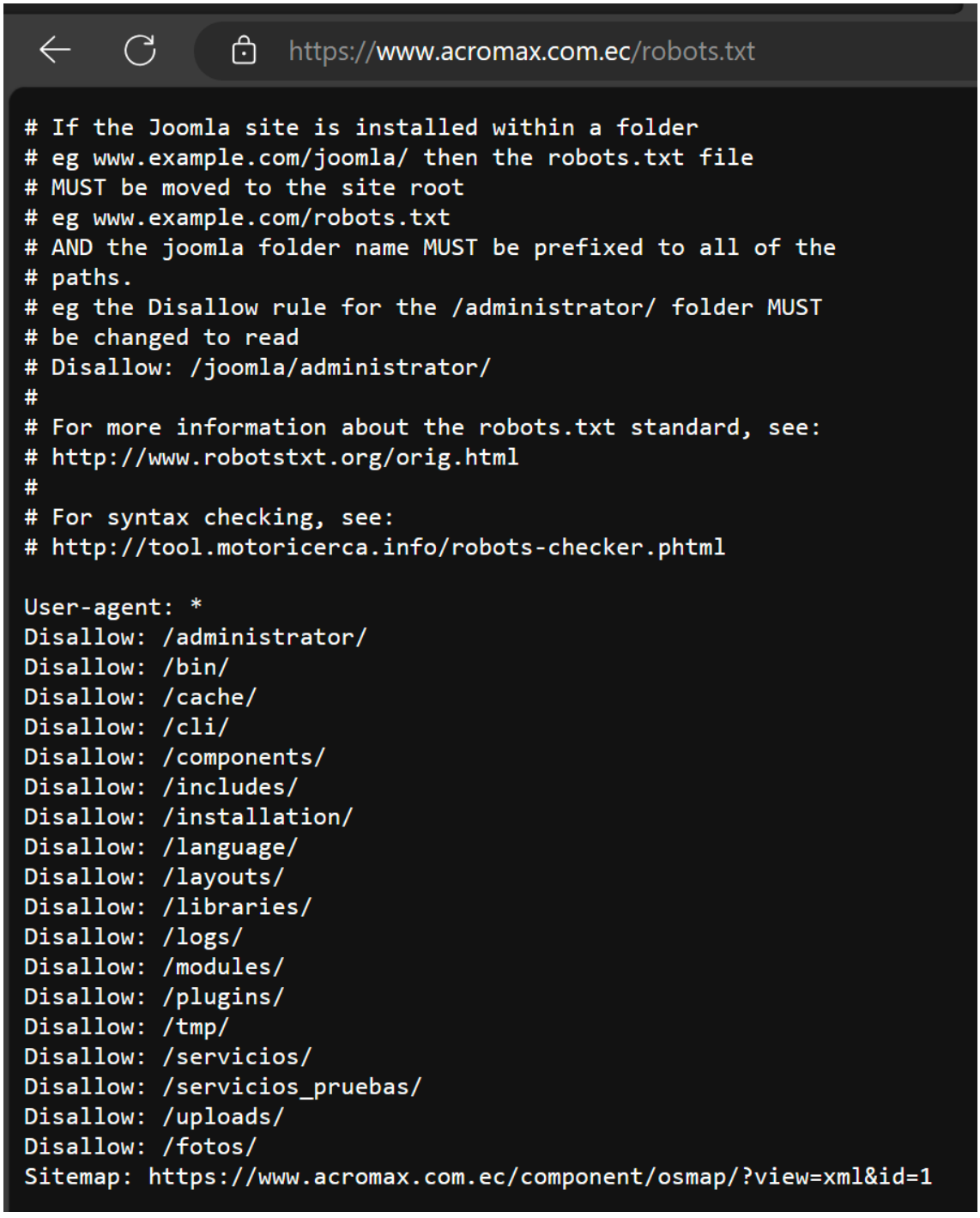
IP	Subred	ASN	Proveedor
104.21.59.233	104.21.59.233/12	13335	Cloudflare
172.67.185.26	172.67.185.26/13	13335	Cloudflare

Nota. Esta tabla contiene 2 IPs asociadas a la página web de la organización.
Elaborado por: Autor.

1. Usualmente las páginas web se sirven desde una única dirección IP. Sin embargo, usar más de una IP podría tener varias razones asociadas como: Balanceo de carga: implementar este escenario puede beneficiar los tiempos de mejora en velocidad y disponibilidad del sitio web.
2. Redes de entrega de contenido (CDN): este enfoque permite alojar el contenido de la página web en diferentes servidores con direcciones distintas, en este caso servidores de Cloudflare, ubicados en distintas partes del mundo.
3. Redundancia y tolerancia a fallos: Este escenario permite respaldar y garantizar la disponibilidad del sitio antes fallas como caída del servidor.

Si bien es cierto se mencionas varias ventajas sobre usar más de una IP en una página web, pero para este trabajo de pentesting, se obtuvo un objetivo más de análisis. Dentro de la página web, se evidencio el acceso a la ruta del archivo robots.txt.

Figura 6. *Captura del acceso al archivo robots.txt en la página web del objetivo.*

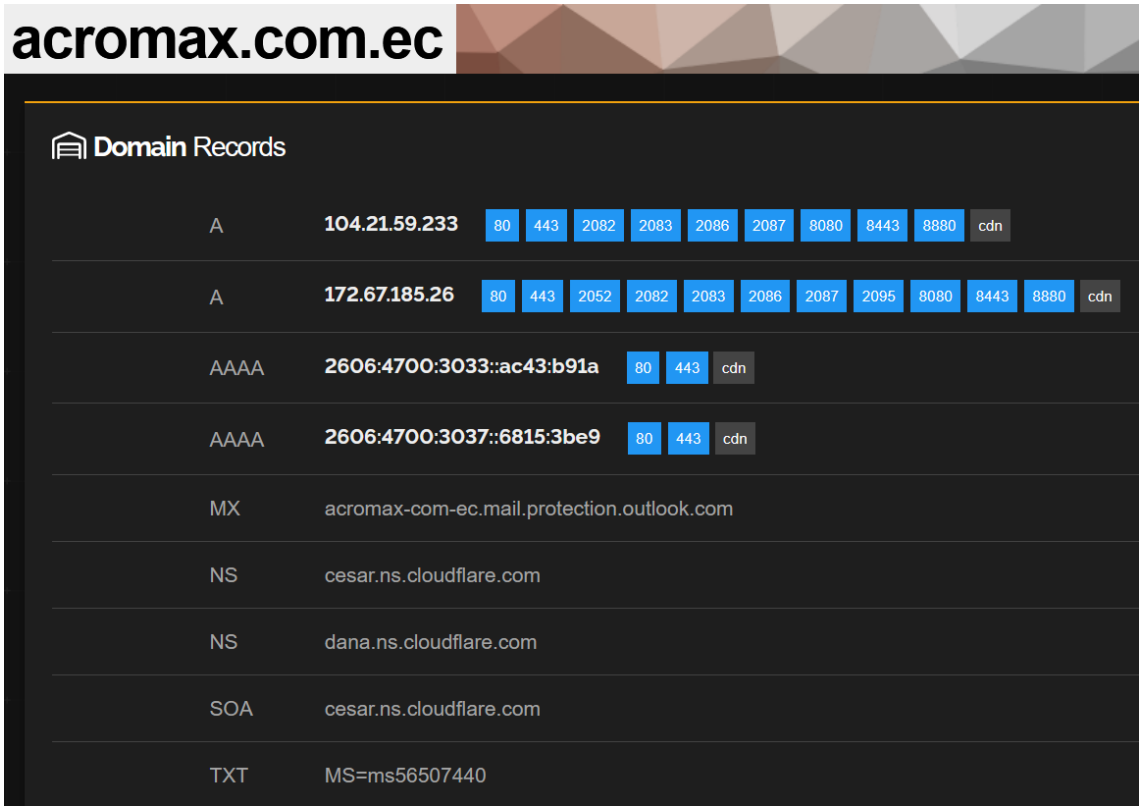


Nota. La revisión y análisis del archivo robots.txt logro proporcionar información valiosa acerca de la estructura y posibles áreas de interés del sitio web.

Elaborado por: Autor.

Después del análisis del archivo robots, se realizó un reconocimiento con el motor de búsqueda disponible de Shodan. Motor que entrego información como puertos, servidores de correo e información de interés, la cual se evidencia mediante la siguiente imagen:

Figura 7. *Resultado del reconocimiento mediante el motor de búsqueda de Shodan.*



Nota. El motor de búsqueda de Shodan, realizo una búsqueda exhaustiva sobre puertos, servidores de correo y dominio, IPs v4 y v6. Elaborado por: (Shodan, 2023).

La información descubierta mediante las herramientas de reconocimiento, permitieron proceder a la fase de análisis de puertos y servicios de las IPs, descubiertas.

3.2 ANÁLISIS DE PUERTOS Y SERVICIOS

Para la fase de análisis de puertos y servicios se usó la herramienta Dig y Nmap en sus últimas versiones estables, descritas previamente. La optimización y ejecución de los scripts realizados con Nmap, en su mayoría fueron automatizados bajo la modalidad: Bash y Python scripting. Con la

finalidad de mejorar tiempos de respuestas y niveles de intrusión menos invasivos.

Resultados con Nmap

Scripts ejecutados:

1. nmap -sS -p1-65535 -v -n --min-rate 5000 -oA puertos 104.21.59.233
2. nmap -sS -p1-65535 -v -n --min-rate 5000 -oA puertos 172.67.185.26
3. *nmap -sV --script vuln -p80,443,587,8080 -v -n -oA vulnerabilidades 104.21.59.233*

Tabla 6. *Resultado de los puertos y servicios del escaneo externo de la organización.*

Puertos descubiertos	Estado de los puertos	Servicios ejecutados
80	open	http
443	open	https
587	open	Submission
8080	open	Cloudflare http-proxy

Elaborado por autor.

Una vez identificado los puertos abiertos dentro de la infraestructura de Acromax, se procedió a realizar un análisis DNS con la herramienta DIG.

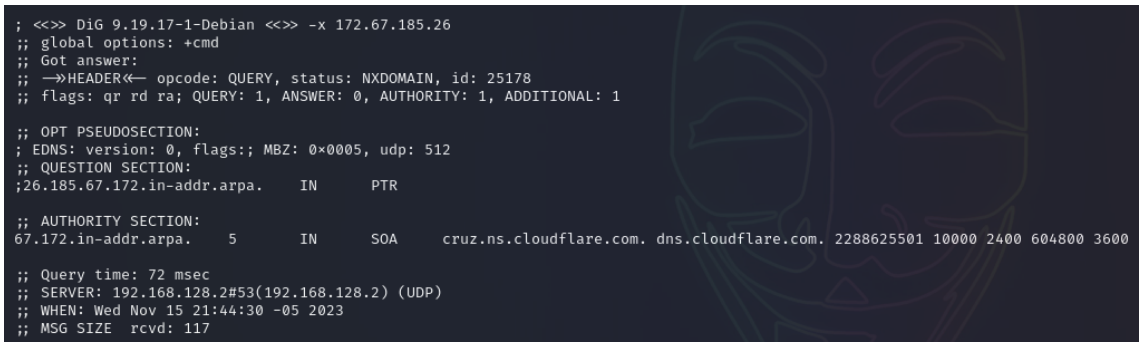
Resultados con DiG

El propósito principal del uso de la herramienta DiG fue una búsqueda inversa DNS, la cual se realizó a las IPs asociadas a la página web.

Figura 8. *Escaneo DNS con la herramienta DiG a la IP 104.21.59.233*

Nota. el escaneo DNS nos dio como resultado, el encargado de las conexiones DNS, la empresa Cloudflare. Elaborado por: Autor.

Figura 9. *Escaneo DNS a la segunda IP asociada a la página web de la organización.*



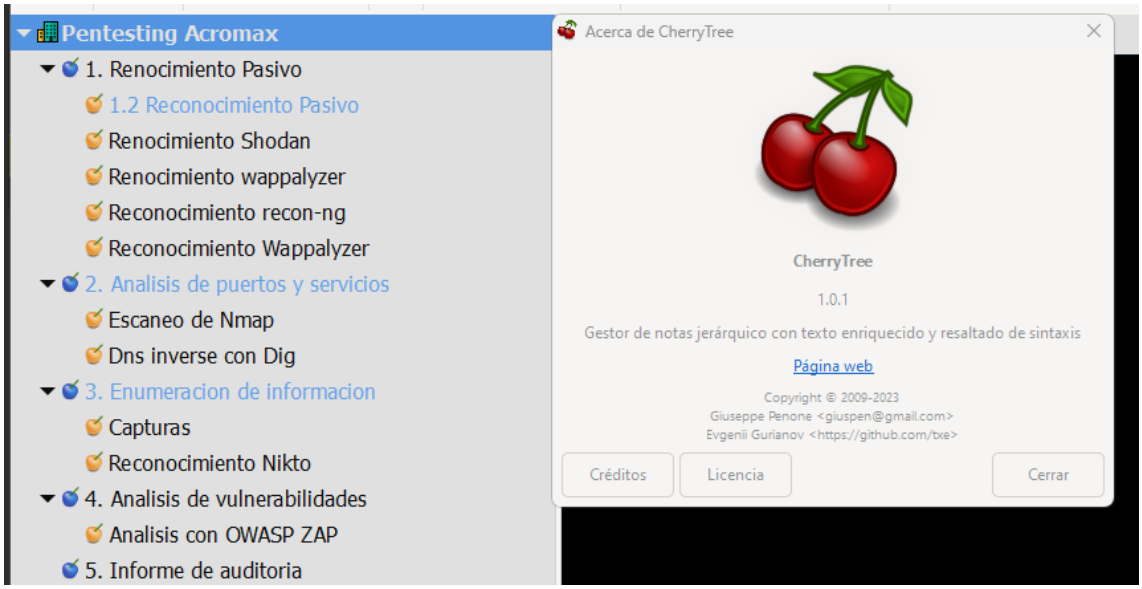
Nota. el segundo escaneo DNS nos dio como resultado, el encargado de las conexiones DNS, la empresa Cloudflare limitando la enumeracion adicional. Elaborado por: Autor.

Como se logro evidenciar en ambas instrucciones ejecutadas se buscó realizar una búsqueda inversa del DNS. Y esta no arrojo información adicional de la página web. Pero si entrego la información del proveedor encargado de la resolución DNS este alojado en los servidores de Cloudflare. Por lo cual la respuesta de estos análisis se ven limitadas, a lo que el servidor este configurado a mostrar.

3.3 ENUMERACIÓN DE LA INFORMACIÓN ENCONTRADA

La etapa de enumeración es un componente critico dentro de las pruebas de hacking ético, así como lo dicta la metodología OWASP. Por lo cual, dentro de este trabajo de tesis, se llevó a cabo la recopilación de información de manera estructurada a través del software CherryTree e imágenes de resultados de los comandos ejecutados, el cual se evidencia en el siguiente grafico:

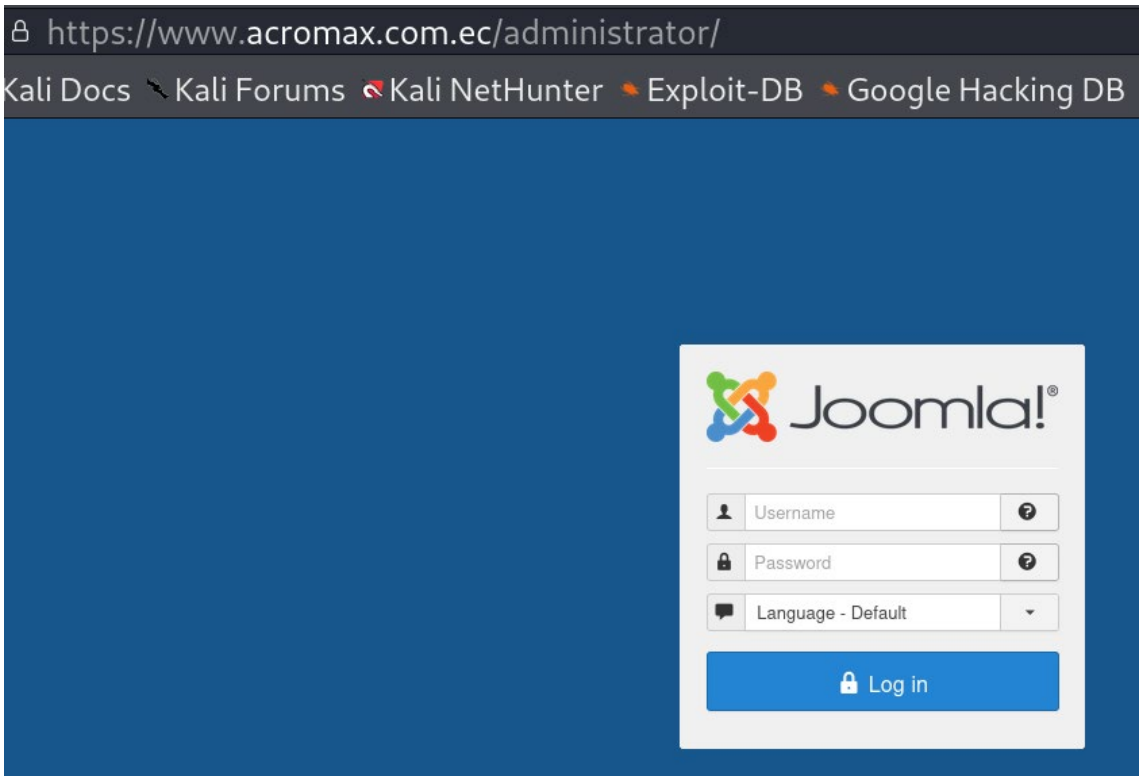
Figura 10. *Enumeración de la información de cada paso del pentesting mediante el software CherryTree.*



Nota. Como se evidencia en la imagen, mediante CherryTree se logró almacenar de forma encriptada y asegurada la información de los resultados obtenidos durante cada etapa del pentesting. Elaborado por: Autor.

Dentro de la etapa de enumeración detallaremos la información relevante de las etapas realizadas. Como se logró visualizar en la etapa de reconocimiento en la ruta del archivo robots.txt, se evidencia algunas rutas de interés, en las cuales mediante el proxy de OWASP ZAP. Se logro acceder a estas rutas, no disponibles para el usuario común.

Figura 11. *Acceso al portal Joomla administrador de la empresa Acromax.*

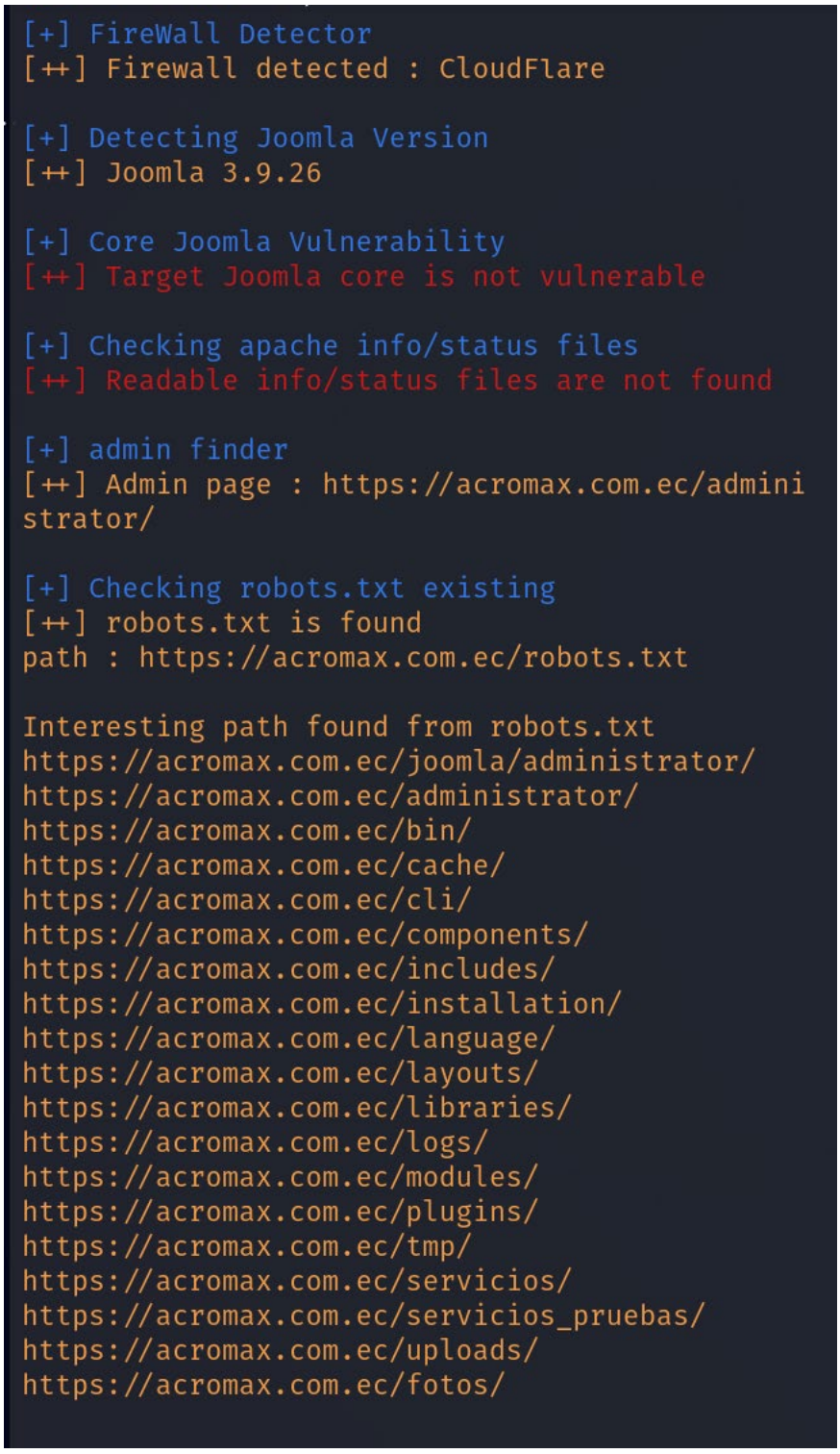


Nota. Esta ruta fue mostrada por el archivo robots.txt, por lo cual, al momento de acceder a la misma mediante un proxy, nos muestra un portal de acceso.

Elaborado por: Autor.

La ruta /administrador logro confirmar que el sistema gestor de contenidos, de ahora en adelante llamado CMS, de Acromax es Joomla, el cual hasta este punto se desconoce la versión o más detalles de esta. En este punto de la evaluación la herramienta de JoomScan desempeño un rol importante, debido al análisis enfocado al CMS Joomla, se logró enumerar información de la página web de Acromax acerca del CMS.

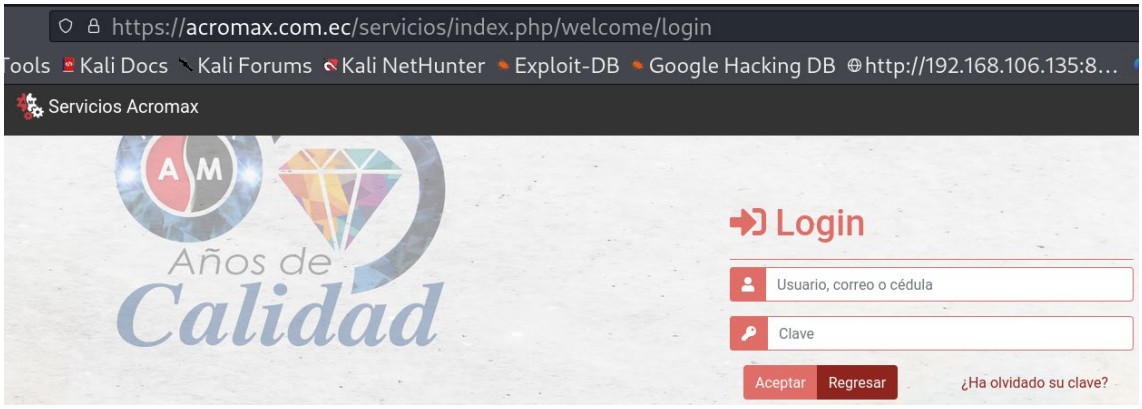
Figura 12. *Enumeración del cms Joomla mediante JoomScan*



Nota. El escáner arrojo la versión en uso del Joomla es 3.9.26 en la cual se encuentra alojada la página web de Acromax, y la última versión disponible es la 5.0.0. Elaborado por: (OWASP , 2022).

Otra ruta de interés que se logró acceder fue la ruta /servicios, la cual redirige a un portal de ingreso programa en PHP:

Figura 13. *Acceso a la ruta de servicio de la organización.*



Nota. El acceso a esta ruta de /servicios, nos revela un dato importante, como lo es el lenguaje de programación PHP, debido a la extensión que se visualiza en la ruta /servicios/index.php. Elaborada por: Autor.

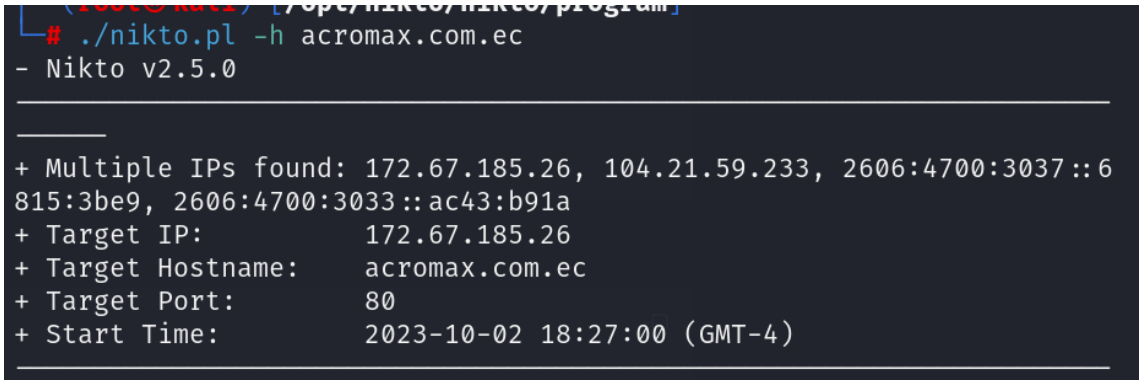
Como resultado de una búsqueda exhaustiva de portales de ingreso dentro de la organización, se logró acceder a la ruta del acceso de usuarios internos, lo cual se evidencia a continuación:

Figura 14. *Acceso al portal de usuarios internos de la organización.*

Nota. El acceso a la ruta del portal de usuarios internos podría ser crítico, si es que se tiene una credencial validad para acceder. Elaborado por: Autor.

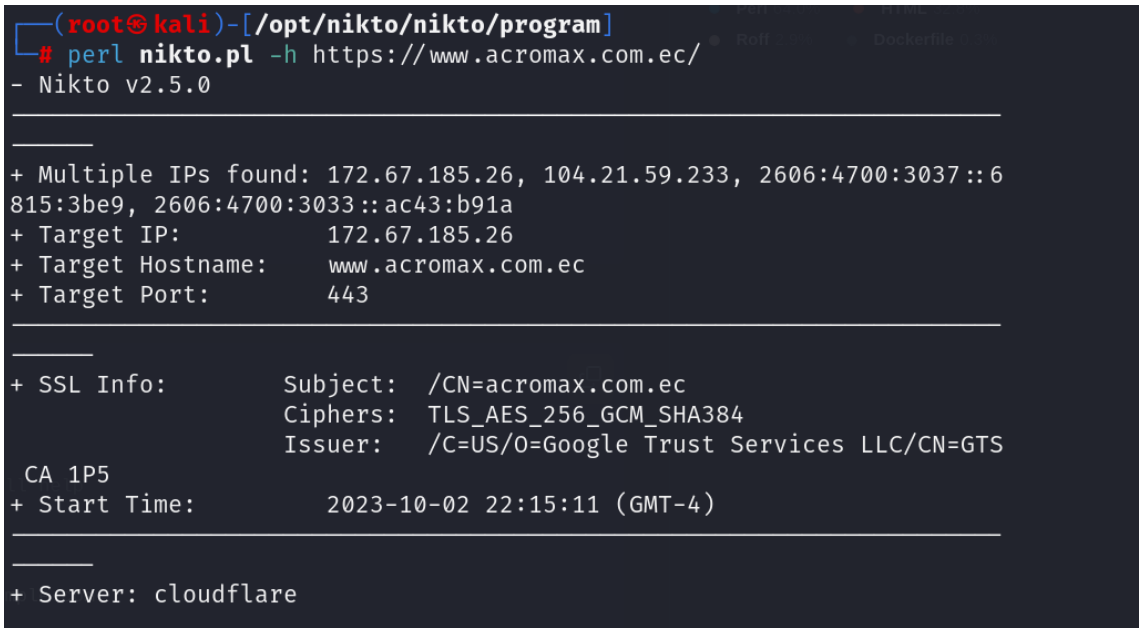
Una vez finalizada la búsqueda de directorios, se realizó una enumeración de la página de web de la organización mediante la herramienta Nikto v2.5.0. La cual permitió corroborar información del análisis de puertos y servicios realizado con Nmap.

Figura 15. *Enumeración del puerto 80 de la página web de la organización.*



Nota. Esta herramienta de enumeración, lista detalles de infraestructura encontrada en relación con la URL Acromax.com.ec. Elaborado por: Autor

Figura 16. *Enumeración del puerto 443 de la página web de la organización.*



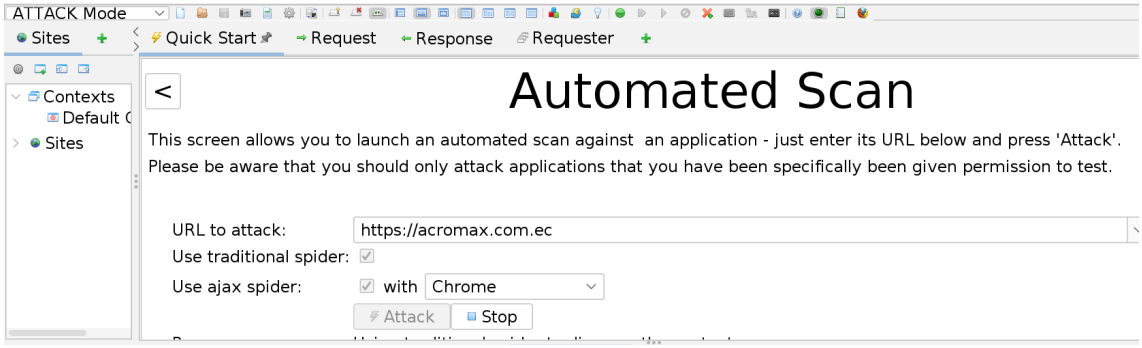
Nota. Esta herramienta de enumeración, lista detalles de infraestructura encontrada en relación con la URL Acromax.com.ec. Elaborado por: Autor

Los resultados entregados por la herramienta de enumeración Nikto, fueron de suma importancia para corroborar información encontrada por diferentes herramientas de reconocimiento previamente observadas. Se logro evidenciar varias IPs como proveedores informáticos.

3.4 ANÁLISIS DE VULNERABILIDADES

El análisis realizado por la herramienta de OWASP ZAP, realiza varias pruebas de intrusión de manera ética y legal. Este análisis fue realizado en Modo ataque, el cual es un modo más intrusivo el cual solo se puede utilizar cuando se tiene autorización de la organización para poder evaluar su infraestructura.

Figura 17. *Preparación del entorno previo al escáner en modo ataque por owasp zap.*

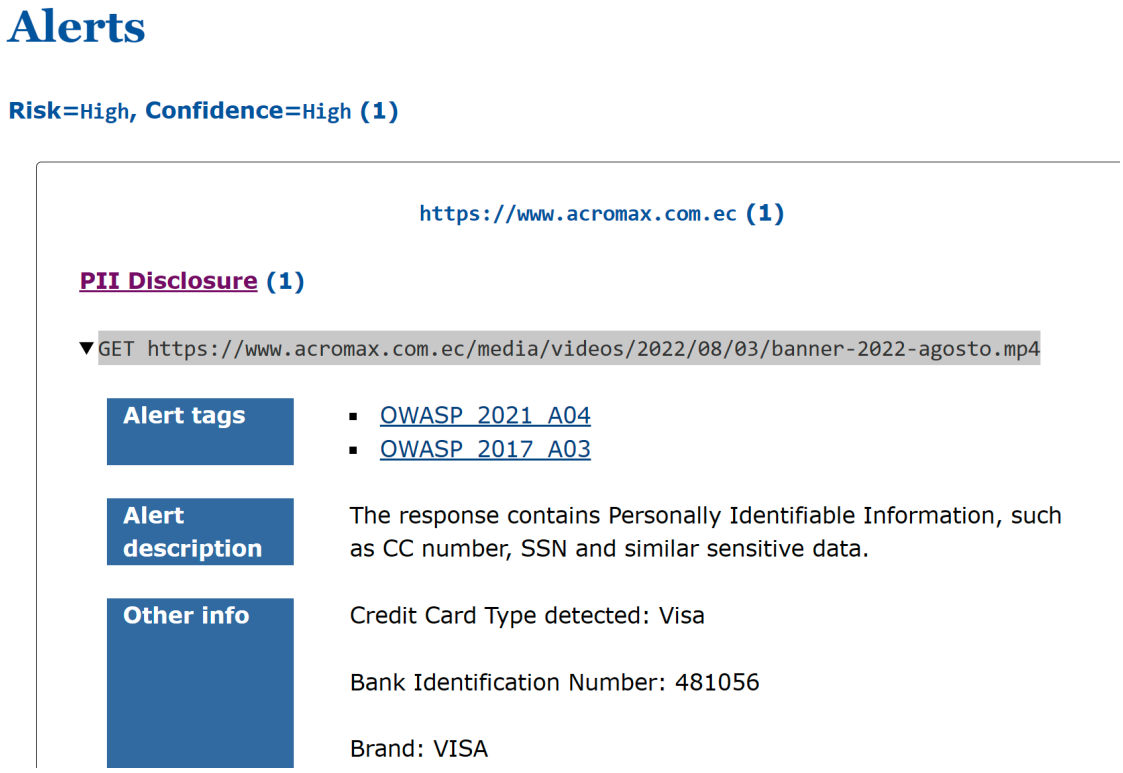


Nota. La herramienta ZAP permite, realizar distintas configuraciones previo al escáner, para no realizar nada que será considerado ilegal o dañino durante el escáner. Elaborado por: Autor.

Al finalizar este escáner la herramienta ZAP genera un reporte con varios parámetros e información relacionada a las vulnerabilidades encontradas. A continuación, podremos evidenciar los riesgos de mayor relevancia detectado durante el escáner automatizado por ZAP:

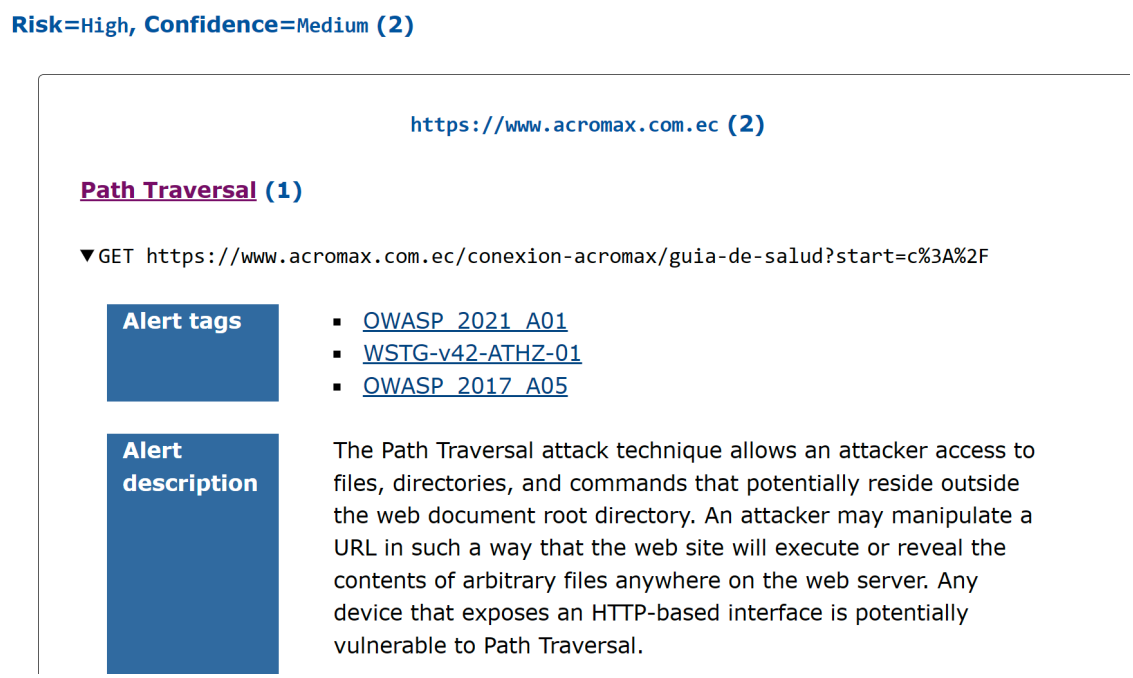
Figura 18. *Alerta por PII Disclosure durante el escáner.*

IDS (Intrusion Detection Scan):



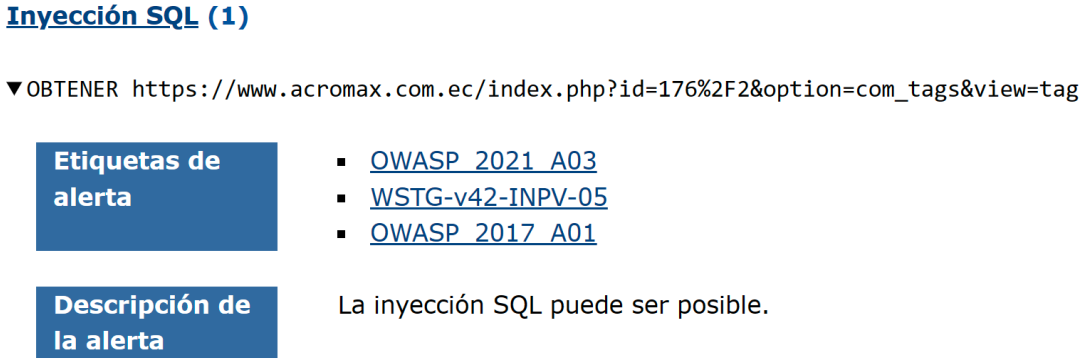
Nota. Esta alerta es de alto riesgo, debido que en la URL del archivo con extensión .mp4 se detectó una tarjeta VISA, originaria de un banco norteamericano. Elaborado por: (ZAP , 2023).

Figura 19. *Alerta por riesgo de Path Traversal.*



Nota. La tecnica de ataque de Path Traversal puede ser aprovechada por un atacante para acceder a archivos, directorios y/o comandos del directorio raiz, debido que la URL es manipulable. Elaborado por: (ZAP , 2023).

Figura 20. *Alerta por riesgo de inyección SQL.*



Nota. Al ser posible la inyeccion SQL dentro de alguna URL esta puede ser vulnerada desde lado del usuario interno como externo, lo cual traeria consecuencias fatales para la organización. Elaborado por: (ZAP , 2023).

Figura 21. *Alerta por biblioteca JQUERY desactualizada.*

https://www.acromax.com.ec (1)

Biblioteca JS vulnerable (1)

▼OBTENER
https://www.acromax.com.ec/cache/com_templates/templates/shaper_helix3/aef959b10b0919e412903a0fc0624e55.js

Etiquetas de alerta	▪ CVE-2020-11023 ▪ OWASP_2017_A09 ▪ CVE-2020-11022 ▪ OWASP_2021_A06 ▪ CVE-2015-9251 ▪ CVE-2019-11358
Descripción de la alerta	La biblioteca jquery identificada, versión 1.12.4 es vulnerable.
Información adicional	CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358

Nota. La ultima version de jquery descargable es 3.7.1 Elaborado por: (ZAP , 2023).

Después de conocer la versión del CMS, la herramienta whatweb nos ayudó a identificar el lenguaje de programación de la página web, cual se identificó que se encuentra en una versión desactualizada y vulnerable.

FIGURA 1. *Evidencia del lenguaje de programación mediante whatweb.*

```
└─$ whatweb https://www.acromax.com.ec
https://www.acromax.com.ec [200 OK] Adobe-Flash, Bootstrap, Cookies[fb0bf998fe80d741f665d3b333aecaaa], Country[RESERVED][ZZ], HTML5, HTTPSe
rver[cloudflare], HttpOnly[fb0bf998fe80d741f665d3b333aecaaa], IP[172.67.185.26], JQuery, MetaGenerator[Joomla! - Open Source Content Manage
ment], Object, Open-Graph-Protocol[website], OpenSearch[https://www.acromax.com.ec/component/search/?id=367&amp;Itemid=101&amp;format=opens
earch], PHP[7.4.1,], Script[66102b410d32d22bc31f2f26-text/javascript,application/json,application/ld+json,text/javascript], Title[Acromax :
: Laboratorio Químico Farmacéutico], UncommonHeaders[x-content-type-options,x-forwarded-port,cf-cache-status,report-to,nel,cf-ray,alt-svc],
 X-Powered-By[PHP/7.4.1, ASP.NET]
```

Nota. La página web está programada con PHP v7.4.1 y la última versión es 8.2.12. Elaborado por: Autor.

Como última instancia se plantea la importancia de actualizar el CMS Joomla que se encuentra en la versión 3.9.26 y la última versión estable a descargar es la 5.0.0. Debido a esta desactualización podría existir una vulnerabilidad critica como Cross Site Scripting, a continuación, se muestra una URL, que habla de la vulnerabilidad existente en la versión del Joomla usado por la organización: https://www.exploit-db.com/exploits/43488

3.5 INFORME DE AUDITORIA

En esta fase final del pentesting se mostrará las vulnerabilidades más relevantes de acorde a su nivel de criticidad. Con sus respectiva documentación y recomendaciones de acorde a la metodología OWASP.

Parámetros del reporte

Niveles de riesgo: Alto, Medio Bajo, Informativo.

Figura 22. *Recuento de alertas por vulnerabilidades encontradas.*

		Confirmado por el usuario	Alto	Medio	Bajo	Total
Riesgo	Alto	0 (0.0%)	1 (2,9%)	2 (5,7%)	0 (0.0%)	3 (8,6%)
	Medio	0 (0.0%)	6 (17,1%)	3 (8,6%)	1 (2,9%)	10 (28,6%)
	Bajo	0 (0.0%)	2 (5,7%)	9 (25,7%)	1 (2,9%)	12 (34,3%)
	Informativo	0 (0.0%)	2 (5,7%)	3 (8,6%)	5 (14,3%)	10 (28,6%)
	Total	0 (0.0%)	11 (31,4 %)	17 (48,6%)	7 (20,0%)	35 (100%)

Nota. El escáner para el análisis de vulnerabilidades dentro de la organización, duro más de 12 horas, y como resultado encontramos un total de 35 riesgos de diferentes tipos. Elaborado por: (ZAP , 2023).

Descripcion de los riesgos detectados

3.5.1 PI DISCLOSURE

Tipo de riesgo: Alto

URL de la documentación del reporte por vulnerabilidad:
https://www.zaproxy.org/docs/alerts/10062/

Descripción de la alerta: La respuesta contiene información personal identificable, como el número de CC, el SSN y otros datos sensibles similares, relacionado a una tarjeta VISA 481XXXX

3.5.2 PATH TRAVERSAL

Tipo de riesgo: Alto

URL de la documentación del reporte por vulnerabilidad: http://projects.webappsec.org/w/page/13246952/Path%20Traversal.

Descripción de la alerta:
La técnica de ataque Path Traversal permite a un atacante acceder a archivos, directorios y comandos que potencialmente residen fuera del directorio raíz del documento web. Un atacante puede manipular una URL de tal manera que el sitio web ejecute o revele el contenido de archivos arbitrarios en cualquier parte del servidor web. Incluso si el servidor web restringe adecuadamente los intentos de Path Traversal en la ruta URL, una aplicación web en sí misma puede seguir siendo vulnerable debido a un manejo inadecuado de la entrada proporcionada por el usuario. Este es un problema común de las aplicaciones web que utilizan mecanismos de plantillas o cargan texto estático desde archivos.

3.5.3 INYECCIÓN SQL

Tipo de riesgo: Alto

URL de la documentación del reporte por vulnerabilidad: https://cwe.mitre.org/data/definitions/89.html.

Descripción de la alerta:

Es posible la inyección SQL por medio de la URL: https://www.acromax.com.ec/index.php?id=152%2F2&option=com_tags&view=tag.

Como consecuencias de que los aplicativos dentro de una organización sean vulnerables ante ataques de tipo inyección SQL podría acarrear como consecuencias como:

1. Robo de bases de datos
2. Robo de credenciales

3. Daño de los aplicativos
4. Obtención de privilegios

3.5.4 AUSENCIA DE TOKEN ANTI-CSRF

Tipo de riesgo: Medio

URL de la documentación por vulnerabilidad:
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery

Descripción de la alerta:

No se encontraron tokens Anti-CSRF en un formulario de envío HTML.
Una falsificación de solicitud de sitio cruzado es un ataque que implica forzar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención con el fin de realizar una acción como la víctima. La causa subyacente es la funcionalidad de la aplicación que utiliza acciones predecibles de URL/formulario de forma repetitiva.

3.5.5 LIBRERÍA JS VULNERABLE

Tipo de riesgo: Medio
URL de la documentación del reporte por vulnerabilidad:
https://cwe.mitre.org/data/definitions/829.html.
Descripción de la alerta:
Se identifico la librería jquery v 1.12.4-joomla, la cual es vulnerable.

CAPITULO 4: PROPUESTA

El presente trabajo de tesis propuso una solución enfocada en un análisis exhaustivo de la seguridad informática de la empresa Acromax mediante técnicas de hacking ético, las cuales siguieron directrices de la metodología de código abierto y gran respaldo de la comunidad informática denominada OWASP. Durante este capítulo se deja como evidencia la metodología implementada junto a sus herramientas, procesos y aportes a la seguridad informática de la organización, en base al análisis realizado por medio de las pruebas de intrusión realizadas. De acorde con lo conversado con la organización, se destaca la entrega de información por la organización, la cual fue un listado de IPs expuestas al internet:

1. 190.12.27.138

2. 186.47.208.179
3. 190.154.255.178
4. 186.69.165.4

4.1 PREPARACIÓN DEL ENTORNO DE TRABAJO PARA HACKING ÉTICO

Una vez acordado el alcance y limitaciones dentro de las pruebas de intrusión, se acordó:

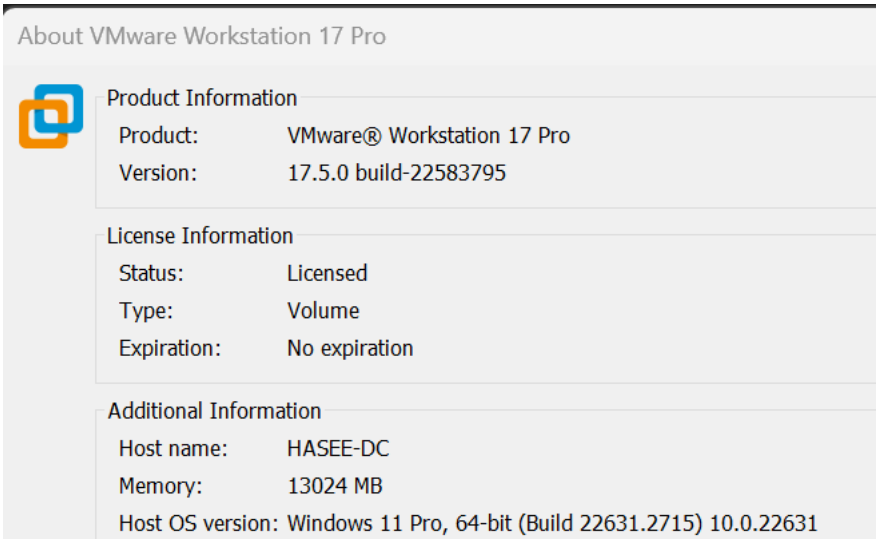
a. No limitaciones de peticiones durante el escáner de vulnerabilidades.

b. No explotación manual ni automatizada.

c. No divulgación de información no autorizada.

Para la preparación del entorno de hacking ético, se preparó un laboratorio de hacking ético y/o entorno controlado para las pruebas, los cuales permitieron realizar el análisis de manera íntegra y controlada. Este laboratorio incluyo herramientas open-source y de pago. Las cuales se deja en evidencia a continuación:

Figura 23. *Licencia VMware Workstation 17 Pro, con un valor de 99USD.*



Nota. Adquirir una licencia profesional del virtualizador permitió instalar versiones estables de Linux, así como mejores resultados de rendimiento.

Una vez que el virtualizador fue adquirido, se realizó la descarga e instalación del sistema operativo especializado en ciberseguridad Kali Linux, el cual dentro

de su aplicativo web contiene la opción de maquina preconstruida para el virtualizador VMware Workstation.

Figura 24. *Opción de descarga para el sistema operativo Kali Linux*

Nota. Se recomienda el uso de esta opción para maquinas virtuales, debido que no requiere mayor complejidad de instalación mas que opciones de personalización.

Una vez instalado el virtualizador y el sistema operativo Kali Linux, el cual fue escogido para realizar la auditoria de ciberseguridad, debido que este sistema opera contiene múltiples herramientas estables y legales para realizar diferentes pruebas enfocadas a la seguridad informática, tales como:

1. Escaneos de puertos, servicios, documentos, etc.

2. Herramientas de diversos ataques como ataques de fuerza bruta, diccionarios, entre otros.

Para poder haber obtenido los resultados más íntegros y concretos dentro de la evaluación se ejecutó dentro del entorno de Kali Linux, varios comandos previos al uso de las herramientas que este trae por defecto.

Los comandos usados fueron:

1. sudo apt update: este comando sirve para actualizar la lista de paquetes instalados por defecto en Kali Linux, dentro de este proceso de actualización el

comando busca y compara las versiones existentes instaladas y las disponibles en la internet.

2. sudo apt upgrade: este comando se ejecutó después del apt update, debido que con este comando confirmamos que deseamos actualizar los paquetes desactualizados y obsoletos instalados por defecto.

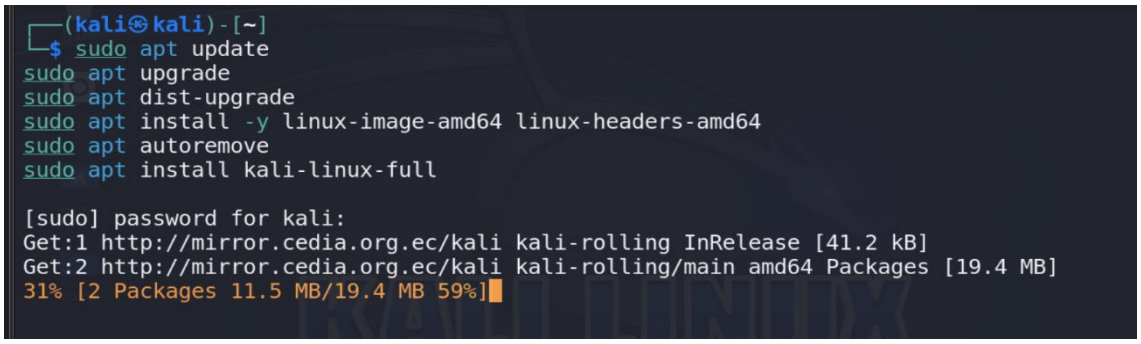
3. sudo apt dist-upgrade: este comando nos permitió actualizar la distribución de Kali Linux, hacia su última versión estable.

4. sudo apt install -y linux-image-amd64 linux-headers-amd64: este comando nos permitió actualizar los paquetes relacionados al kernel, fue de suma importancia para garantizar: seguridad, rendimiento y compatibilidad dentro del análisis.

5. sudo apt autoremove: este comando permitió eliminar los paquetes obsoletos dentro del sistema, los cuales si es que no se eliminan puede generar errores de rendimiento dentro de los procesos realizados en Kali Linux.

6. sudo apt install kali-linux-full: este comando permitió actualizar todas las herramientas instaladas dentro del sistema operativo.

Figura 25. *Ejecución de comando de preparación del sistema operativo Kali Linux.*



Elaborado por autor.

4.2 TECNICAS Y HERRAMIENTAS DURANTE EL PENTESTING DE CAJA GRIS

De las herramientas por defecto y las usadas en esta evaluación informática, en Kali Linux encontramos:

1. Nikto: una potente herramienta de escáner web, que, como objetivo de sus análisis, busca información de servidores, proxy, DNS y toda la información existe de un aplicativo relacionado a su interfaz de comunicación.

Tabla 7. *Información de interés encontrada con Nikto*

IPs encontradas	Puertos en uso	Servidor en uso
172.67.185.26	80	Cloudflare
104.21.59.233	8080	Cloudflare
2606:4700:3033::ac43:b91a	443	Cloudflare http-proxy
2606:4700:3037::6815:3be9	587	Submission

Nota. El comando usado para obtener estos resultados fue Nikto.pl -h.

Elaborado por autor.

3. Nmap: una potente herramienta de escáner de red, que permite descubrir equipos, puertos y servicios, hasta con sus versiones para poder recopilar información en busca de vulnerabilidades asociadas.

Figura 26. *Información de interés encontrada con Nmap*

Puertos descubiertos	Estado de los puertos	Servicios ejecutados
80	open	http
443	open	https
587	open	Submission
8080	open	Cloudflare http-proxy

Elaborado por autor.

3. Whatweb: herramienta que permitió realizar un análisis exhaustivo de lo que contiene un sitio web, información como CMS, IPs, plugin, lenguaje de

programación, errores SQL entre otra información de valor para una auditoria de seguridad informática.

El comando usado fue: whatweb https://www.acromax.com.ec/

Figura 27. *Información de interés encontrada con Whatweb*

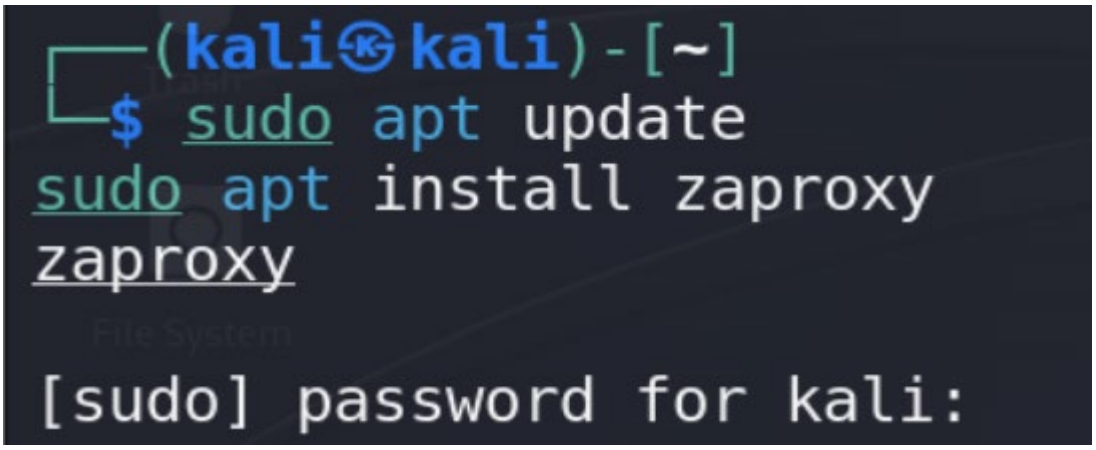
CMS	Lenguaje de programación	CDN
Joomla v8.2.12	PHP v7.4.1	Cloudflare

Elaborado por autor.

Al finalizar los procesos y tecnicas de recopilacion de informacion, se procedio a realizar la instalacion de la herramienta de analisis de vulnerabilidaes recomendada por OWASP y esta fue la herramienta ZAP. Para la cual se ejecuto 3 comandos, los cuales fueron:

1. sudo apt update
3. sudo apt install zaproxy
3. zaproxy

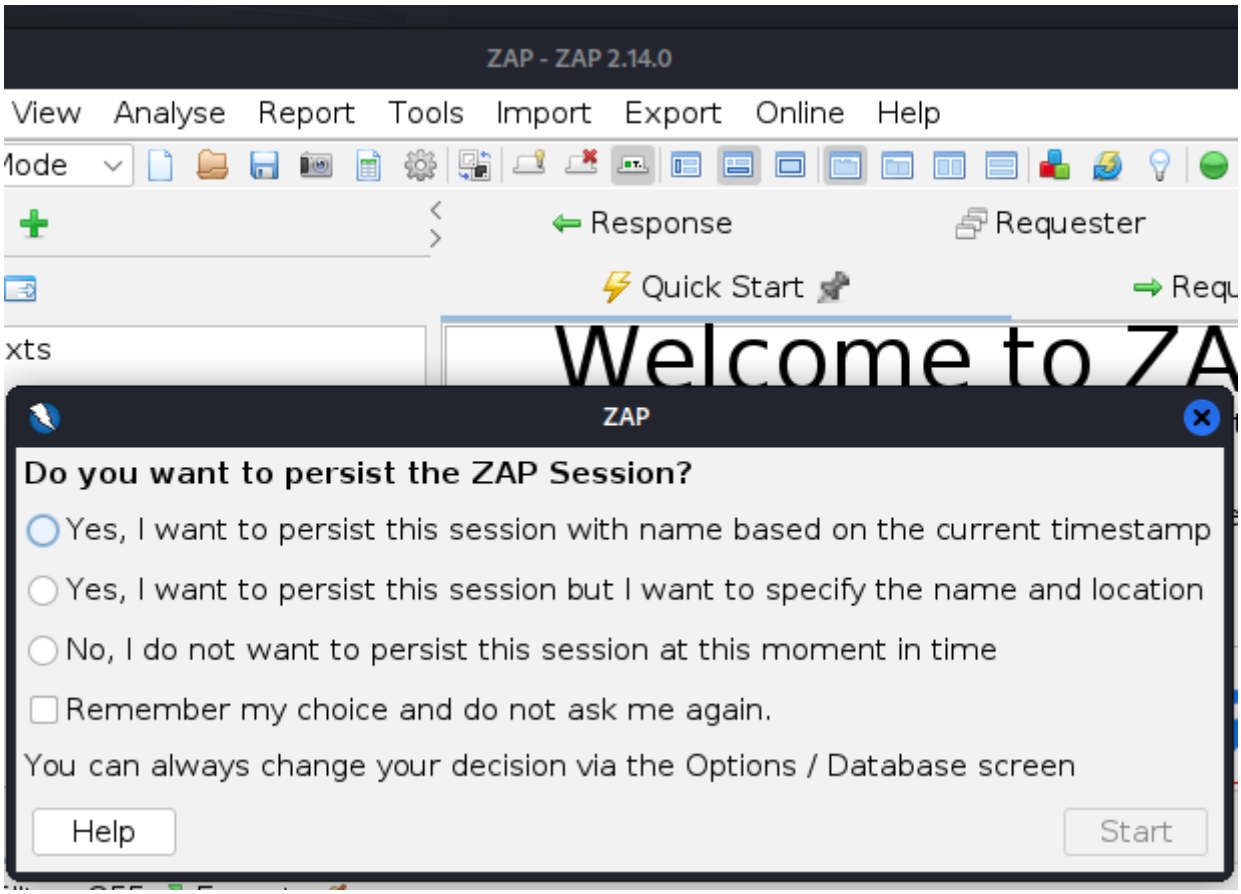
Figura 28. *Ejecucion de comandos para instalar ZAP en Kali Linux*



Elaborado por autor.

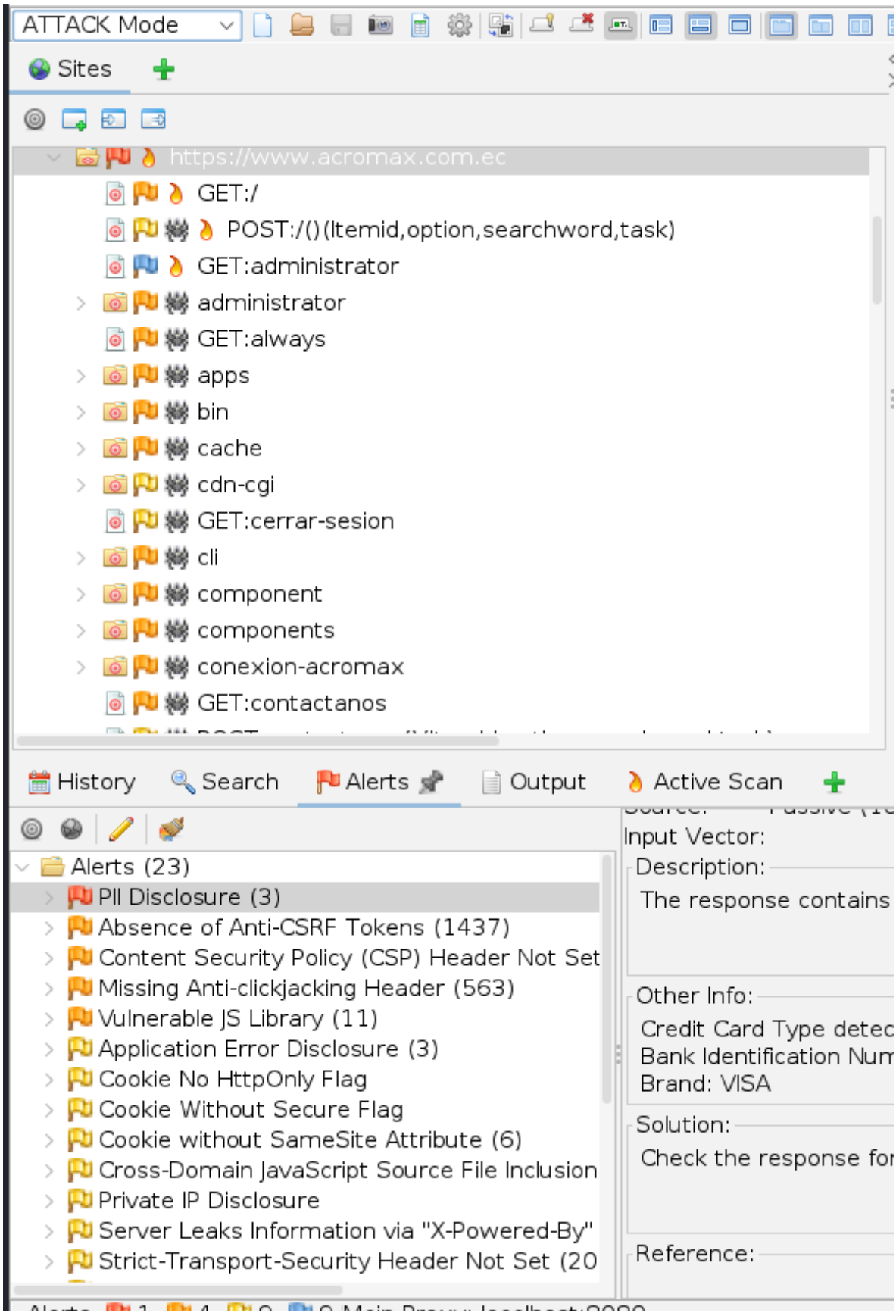
La ejecucion de los comandos se realizado de manera exitosa por lo cual, al finalizar la instalacion se evidenciara la herramienta que se apertura gracias al comando zaproxy.

Figura 29. *Instalacion de ZAP de forma exitosa*



El uso de la herramienta ZAP, permitió identificar vulnerabilidades dentro de la organización, mediante un escáner automatizado enfocado en la información recolectada previamente, se encontró 23 vulnerabilidades enfocadas dentro de la URL: https://www.acromax.com.ec/

Figura 30. *Evidencia de las vulnerabilidades encontradas en modo ataque*



4.3 MEDIDAS DE MITIGACIÓN PARA LAS VULNERABILIDADES IDENTIFICADAS DENTRO DE LA ORGANIZACIÓN

Mitigación para PI DISCLOSURE

Consecuencias:

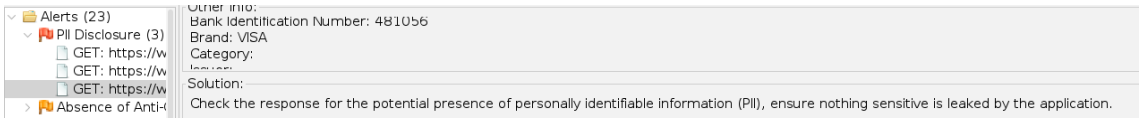
1. Violación de la privacidad: la divulgación de información personal no autorizada viola la privacidad de los individuos.

1. Riesgo de robo de identidad: los datos personales que sean expuestos podrían ser utilizados por cibercriminales para llevar a cabo acciones ilegales como fraudes, robo de identidad, entre otros delitos.
2. Daño a la reputación: las organizaciones que son víctimas de violaciones de seguridad que resultan en la divulgación de información personal, a menudo experimentan un daño significativo de la reputación organizacional.
3. Sanciones legales y multas: la divulgación no autorizada de datos de clientes, socios de las organizaciones, acarrea sanciones financieras y pérdida de credibilidad de los usuarios.

   Mitigación:

- Implementar prácticas de desarrollo seguro.
- Limitar el consumo de recursos por usuario o servicio.
- Validar pruebas unitarias de integración para validar que todos los flujos críticos son resistentes al modelado de amenazas.
- Comprobar la posible presencia en la respuesta de información personal identificable (PII), se debe asegurar de que la aplicación no filtra nada sensible por medio de alguna petición.

Figura 31. *Evidencia de la solución recomendada por OWASP*



URL de documentaciones soluciones expuestas

https://cheatsheetseries.owasp.org/cheatsheets/Secure_Product_Design_Cheat_Sheet.html

https://owasp.org/Top10/A04_2021-Insecure_Design/

https://owaspsamm.org/model/design/security-architecture/

https://www.zaproxy.org/docs/alerts/10062/

Mitigación para PATH TRAVERSAL

Consecuencias:

1. Ejecución de código malicioso: esta vulnerabilidad permite la escritura o ejecución de archivos, un atacante podría cargar y ejecutar código malicioso dentro de los sistemas.

2. Manipulación de datos: un atacante podría manipular y corromper datos críticos al acceder o modificar archivos fuera de las rutas permitidas.

3. Ataques de denegación de servicio: Un atacante podría realizar ataques de DoS accediendo a archivos críticos o sobrecargando el sistema con operaciones de lectura y escritura no autorizadas.

Mitigación:

- Validación de entradas: implementar una estricta validación de todas las entradas de usuario para garantizar que no contengan secuencias de exploración de rutas.
- Sanitización de rutas: limpiar y normalizar las rutas de acceso proporcionadas al usuario antes de utilizarlas. Eliminar caracteres especiales y asegurarse de que las rutas estén en un formato seguro y predecible.
- Restricciones de acceso: configurar las adecuadas restricciones de acceso para archivos y directorios.
- Implementación de WAF (Web Application Firewall): configurar un WAF para filtrar y bloquear solicitudes maliciosas que intentan explotar la travesía de rutas.

URL de documentación de soluciones expuestas

https://sucuri.net/website-firewall/

https://blog.infranetworking.com/10-tips-para-prevenir-malware-en-joomla/

Mitigación para inyección SQL

Consecuencias:

1. Acceso no autorizado: un atacante podría utilizar inyección SQL para acceder a datos sensibles almacenado en bases de datos, como usuarios y contraseñas, u otra información confidencial.

2. Alteración de datos: la inyección SQL puede permitir la ejecución de comandos maliciosos en la base de datos, esto podría incluir creación de cuentas, instalación de malware o manipulación de la estructura de la base de datos.

3. Ataques de fuera bruta: la obtención sobre contraseñas o hashes almacenados en la base de datos, un cibercriminal podría realizar ataques de fuera bruta para descifrar contraseñas débiles o predecibles.

Mitigación:

- Validación y sanitización de entradas: realizar una validación rigurosa y sanitización adecuada de todas las entradas de usuario antes de ser utilizadas en consultas SQL dentro de los formularios web, parámetros de URL y cualquier otro dato ingresado por el usuario.
- Implementación de procedimientos almacenados: utilizar procedimientos almacenados en lugar de consultas SQL directas siempre que sea posible, debido que estos pueden ayudar a reducir el riesgo de inyección SQL.
- Cifrado de datos sensibles: implementar el cifrado de datos sensibles almacenados en la base de datos, debido que esto ayudara a proteger la información incluso si se produce una brecha de seguridad.

URL de documentación de soluciones expuestas

https://owasp.org/www-project-proactive-controls/v3/en/c3-secure-database

https://owasp.org/Top10/A03_2021-Injection/

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Mitigación para ausencia de ANTI-CRSF tokens

Consecuencias:

1. Ejecución de acciones no autorizadas: un atacante podría engañar a un usuario autenticado para que realice acciones no autorizadas en la aplicación en su nombre, por ejemplo: cambios de configuración, eliminación de datos o realización de transacciones sin el consentimiento del usuario.

2. Robo de sesiones y suplantación de identidad: al explotar una vulnerabilidad CSRF, un atacante podría secuestrar la sesión de un usuario autenticado, permitiendo la autenticación dentro de los aplicativos de la organización.

3. Perdida de privacidad: si un aplicativo maneja información privada o confidencial, la falta de protección CSRF podría exponer información, que un atacante podría inducir acciones que comprometan la privacidad.

Mitigación:

- Implementación de Tokens Anti-CSRF: implementar los tokens para que estos puedan ser únicos por sesión y generados de manera segura.
- Almacenamiento seguro de tokens: asegurarse de que los tokens anti-CSRF se almacenen de manera segura en el lado del cliente, preferiblemente en cookies con atributos seguros y HTTPOnly.
- Políticas de contenido: implementar políticas de seguridad de contenido para limitar dominios desde los cuales se pueden cargar dentro de los aplicativos.
- Implementar métodos seguros: utilizar métodos HTTP seguros según su propósito como: GET, POST, etc.

URL de documentación de soluciones expuestas

https://docs.joomla.org/How_to_add_CSRF_anti-spoofing_to_forms#Recommended_Security_Procedures

https://www.zaproxy.org/docs/alerts/10202/

http://projects.webappsec.org/w/page/13246919/Cross%20Site%20Request%20Forgery

Mitigación para librería JS vulnerable

Mitigación:

- Actualizar a una versión 3.5.0 o superior.

Figura 32. *Evidencia de la solución recomendada por OWASP por librería vulnerable*

URL de documentación de soluciones expuestas

https://jquery.com/download/

https://security.snyk.io/
https://security.stackexchange.com/questions/205864/is-there-a-way-to-exploit-jquery-1-12-4-vulnerabilitypackage/npm/jquery/1.12.4

Mitigación para lenguaje de programación y CMS desactualizado

Mitigación:

PHP versión 7.4.1: actualizar a la versión 7.4.21 o posterior de PHP.

Joomla versión 3.9.26: actualizar a una versión 4.3.3 o posterior.

URL de documentación de soluciones expuestas

https://www.php.net/releases/7_4_21.php

https://www.tenable.com/plugins/was/112882

https://downloads.joomla.org/co/latest

CAPÍTULO 5: CONCLUSIÓN

El presente trabajo de tesis se propuso abordar el desafío crítico de fortalecer la seguridad informática en una empresa farmacéutica a través de la implementación de pruebas de intrusión. El objetivo general de este estudio fue claro: reducir las vulnerabilidades en los sistemas informáticos para garantizar la integridad, confidencialidad y disponibilidad de la información en un entorno altamente sensible como los que se manejan dentro de organizaciones de suma importancia como las farmacéuticas. Durante el desarrollo de este proyecto, se llevó a cabo un minucioso proceso de hacking ético de caja gris, revelando un panorama detallado de las vulnerabilidades existentes en la infraestructura TI de la empresa farmacéutica. La identificación de estas vulnerabilidades no solo proporcionó una comprensión profunda de las posibles amenazas, sino que también sirvió como punto de partida para la implementación de medidas correctivas. Las recomendaciones y soluciones propuestas como resultado de las pruebas de intrusión no solo se limitaron a la mitigación de las vulnerabilidades identificadas, sino que también ofrecieron una visión estratégica para mejorar continuamente la postura de seguridad de la organización. Se abordaron áreas críticas, desde la actualización de sistemas y la aplicación de parches hasta la implementación de políticas robustas de acceso. La efectividad del enfoque de hacking ético de caja gris en este contexto específico se hizo evidente a medida que se lograron avances tangibles en la protección de los activos digitales de la empresa farmacéutica. Los resultados no solo se traducen en una mayor resistencia a posibles amenazas, sino también en la construcción de una cultura de seguridad sólida dentro de la organización. En conclusión, la implementación correcta de pruebas de intrusión éticas, particularmente el hacking ético se revela como una estrategia efectiva y proactiva para identificar y abordar las vulnerabilidades en los sistemas informáticos de una empresa farmacéutica. Este enfoque no solo responde a los desafíos actuales en materia de ciberseguridad, sino que también establece un marco para la mejora continua y la adaptación a las evoluciones constantes en el panorama de amenazas cibernéticas.

RECOMENDACIONES

Las recomendaciones establecidas en este capítulo están basadas en opiniones del autor, en base a los resultados del estudio implementado dentro de este trabajo de tesis. Implementar buenas prácticas de seguridad a nivel corporativo, puede marcar un valor agregado dentro de las organizaciones, a continuación, se lista buenas prácticas que en opinión del autor se puede implementar dentro de distintos sectores comerciales, incluyendo al sector farmacéutico:

1. Políticas de seguridad documentadas: el desarrollo e implementación de políticas claras y específicas que aborden aspecto como acceso a los sistemas, uso de contraseñas, gestión de activos y respuesta a incidentes. Asegura que el personal este capacitado y apto para seguir buenas prácticas de ciberseguridad.

2. Auditorias de seguridad: realizar evaluaciones de manera regular para identificar posibles vulnerabilidades en la infraestructura. Esta medida puede demostrar la situación informática actual de las organizaciones.

3. Concientización del personal: realizar campañas regulares de concientización y formación de ciberseguridad para el personal.

En cuanto a las recomendaciones específicas para la organización evaluada en este trabajo de tesis, se recomienda lo siguiente:
1. Realizar un pentesting desde una perspectiva interna: la evaluación realizada en este trabajo de tesis se realizó desde una perspectiva externa, y pese a ser realizada de esa manera se encontraron vulnerabilidades que pueden ser fácilmente explotables desde un usuario interno de la organización.

2. Implementar campañas de desarrollo seguro: las vulnerabilidades que sobresalieron durante el análisis de este trabajo están relacionadas a brechas de seguridad por código inseguro.

Las recomendaciones brindadas en este capítulo pueden ser implementadas en cualquier sector que haga uso de soluciones informáticas.

BIBLIOGRAFÍA

Accuracy. (01 de junio de 2023). *An industry under attack – cybercriminals target our well-being.* Obtenido de https://www.accuracy.com/wp-content/uploads/2023/06/Article-Cybersecurity-and-pharma-EN.pdf

Acromax S.A. (15 de agosto de 2020). *Acromax: Inicio*. Recuperado el 14 de 07 de 2023, de https://www.acromax.com.ec/

Ambit Team. (08 de noviembre de 2022). *5 riesgos de seguridad de las compañías farmacéuticas*. Obtenido de https://www.ambit-bst.com/blog/5-riesgos-de-seguridad-de-las-compa%C3%B1%C3%ADas-farmac%C3%A9uticas

Andrade Vintimilla, J. F. (2023). *Ciberseguridad y salud.* Obtenido de https://www.itscs-cicc.com/ojs/index.php/inndev/article/view/47

AO Kaspersky Lab. (18 de julio de 2021). *CYBERTHREAT REAL-TIME MAP*. Obtenido de https://cybermap.kaspersky.com/stats#country=35&type=OAS&period=w

AO Kaspersky lab. (01 de agosto de 2021). *OAS- On Access Scan.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (09 de agosto de 2023). *Arriba - On Demand Scanner en el ultimo mes.* Obtenido de https://cybermap.kaspersky.com/es/stats#country=35&type=ODS&period=m

AO Kaspersky Lab. (09 de agosto de 2023). *Arriba - On-Access Scan EN EL ÚLTIMO MES.* Obtenido de https://cybermap.kaspersky.com/es/stats#country=35&type=OAS&period=m

AO Kaspersky Lab. (01 de agosto de 2023). *BAD - botnet activity detection.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (2023 de agosto de 2023). *IDS- Intrusion Detection Scan.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (02 de agosto de 2023). *KAS - Kaspersky Anti-Spam.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (01 de agosto de 2023). *MAV- Mail Anti-Virus.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (01 de agosto de 2023). *ODS- On Demand Scanner.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (01 de agosto de 2023). *VUL- Vulnerability Scan.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

AO Kaspersky lab. (01 de agosto de 2023). *WAV- Web Anti-Virus.* Obtenido de https://cybermap.kaspersky.com/es/subsystems

Arcsa. (2023). *Arcsa, una institución que mejora continuamente su servicio de atención al usuario.* Obtenido de https://www.controlsanitario.gob.ec/arcsa-una-institucion-que-mejora-continuamente-su-servicio-de-atencion-al-usuario/

Asamblea nacional del Ecuador. (13 de JULIO de 2023). *Ley Orgánica de Protección de Datos Personales.* Obtenido de Medidas correctivas, Infracciones y Régimen Sancionatorio: https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf

Astudillo, K. (2016). *Hacking Etico 101 - Cómo hackear profesionalmente en 21 días o menos* (segunda ed.). CreateSpace Independent Publishing Platform.

Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities.* Apress. doi:https://doi.org/10.1007/978-1-4842-2155-6

Bejtlich, R., & Almeida, B. (2013). *The practice of network security monitoring: understanding incident detection and response.* No Starch Press.

Bleeping computer. (03 de junio de 2022). *Novartis says no sensitive data was compromised in cyberattack*. Obtenido de BLEEPINGCOMPUTER.com: https://www.bleepingcomputer.com/news/security/novartis-says-no-sensitive-data-was-compromised-in-cyberattack/

BleepingComputer. (03 de junio de 2022). *Novartis says no sensitive data was compromised in cyberattack [fotografía]*. Obtenido de BleepingComputer.com : https://www.bleepingcomputer.com/news/security/novartis-says-no-sensitive-data-was-compromised-in-cyberattack/

Cbinsights. (22 de abril de 2019). *Healthcare Data Is Becoming More Vulnerable To Cyber Attacks. Here's How Startups Are Fighting Back.* Obtenido de Cybersecurity startups are working to defend patient data from hackers and to secure the future of healthcare.: https://www.cbinsights.com/research/healthcare-data-cyber-attacks/

CERCAL group. (24 de mayo de 2022). *Ciberseguridad en la Industria farmacéutica: ¿Por qué debe ser una prioridad?* Obtenido de https://es.linkedin.com/pulse/ciberseguridad-en-la-industria-farmac%C3%A9utica-por-qu%C3%A9-claudia

Chang, J. E. (2020). *Análisis de ataques cibernéticos hacia el Ecuador.* (Vol. IV). Sangolqui, Ecuador: Editora Adjunta. Obtenido de http://geo1.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf

CompTIA. (29 de julio de 2022). *What Is Ethical Hacking?* Obtenido de https://www.comptia.org/content/articles/what-is-ethical-hacking

Coursera. (15 de junio de 2023). *10 certificaciones y cursos de ciberseguridad populares.* Obtenido de https://www.coursera.org/mx/articles/popular-cybersecurity-certifications

Cybersecurity & Infrastructure Security Agency . (23 de febrero de 2023). *Cybersecurity & Infrastructure Security Agency* .

Delta exponential technologies. (18 de julio de 2023). *¿Qué es el pentesting? tipos y cómo utilizarlo para prevenir ciberataques[fotografía]*. Obtenido de https://www.deltaprotect.com/blog/que-es-pentesting

Elazeem, A., & El-Araby, N. (2020). *Effect of cybercrime on the pharmaceutical industry. .* Journal of Intellectual Property and Innovation Management.

ESET. (22 de diciembre de 2022). *Qué es un exploit: la llave para aprovechar una vulnerabilidad*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2022/12/22/exploits-que-son-como-funcionan/

ESIC business. (1 de junio de 2022). *Principales certificaciones en Ciberseguridad.* Obtenido de https://www.esic.edu/rethink/tecnologia/5-certificaciones-en-ciberseguridad#:~:text=Una%20certificaci%C3%B3n%20en%20ciberseguridad%20es%2C%20b%C3%A1sicamente%2C%20un%20fichero,desempe%C3%B1ar%20una%20serie%20de%20funciones%20en%20este%20%C3%A1mbito.

Fernández, R., & Cifuentes, Q. (2022). *La seguridad informática para la toma de decisiones en el distrito de educación 12d03.* Mocache-Ecuador.: CIENCIAMATRIA.

Gartner, Inc. (27 de mayo de 2021). *Gartner Magic Quadrant for Application Security Testing.* Obtenido de https://www.gartner.com/en/documents/4001946

Google. (2019). *Acotar las búsquedas web.* Obtenido de https://support.google.com/websearch/answer/2466433

Google. (11 de noviembre de 2019). *Hacer una búsqueda avanzada en Google.* Obtenido de https://support.google.com/websearch/answer/35890?hl=es&co=GENIE.Platform%3DAndroid&sjid=15068984974981903472-NA

IBM. (25 de junio de 2023). *Por qué ocurren los ciberataques*. Obtenido de https://www.ibm.com/es-es/topics/cyber-attack

Institut national de santé publique du Québec. (17 de agosto de 2018). *Definición del concepto de seguridad*. Obtenido de

https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad#:~:text=La%20seguridad%20es%20un%20estado%20en%20el%20cual,bienestar%20de%20los%20individuos%2

Klishchenko, M., & Kuznetsov, D. (2022). *Information technologies in the analysis of pharmaceutical personnel security.* Pharmacy Formulas.

Lilliam Valenzuela. (16 de junio de 2020). *La importancia de la ciberseguridad en el sector farmacéutico*. Obtenido de https://www.farmaindustrial.com/articulos-online/la-importancia-de-la-ciberseguridad-en-el-sector-farmaceutico-GBS2h

Lyon, G. F. (2009). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning.* Nmap Project.

MedProGroup. (30 de diciembre de 2020). *Cybersecurity in healthcare.* Obtenido de Landscape and Threats: https://www.medpro.com/documents/10502/2836433/Cybersecurity+in+Healthcare+Landscape+and+Threats+CME-CDE.pdf

Netsoft consulting. (15 de julio de 2023). *Ataques informáticos y virus comunes, identifícalos*. Obtenido de https://tienda.eset.com.ec/ataques-informaticos-virus-comunes

Orebaugh, A., & Pinkard, B. (2008). *Nmap in the enterprise: your guide to network scanning.* Syngress. Obtenido de https://theswissbay.ch/pdf/Gentoomen%20Library/Programming/Networking/Nmap%20in%20the%20Enterprise%20Your%20Guide%20to%20Network%20Scanning~tqw~_darksiderg.pdf

OWASP . (05 de agosto de 2022). *OWASP Joomla Vulnerability Scanner Project*. Obtenido de https://www.kali.org/tools/joomscan/

OWASP [fotografía]. (15 de septiembre de 2021). *OWASP Top 10:2021*. Obtenido de https://owasp.org/Top10/es/#como-se-estructuran-las-categorias

OWASP. (03 de diciembre de 2020). Obtenido de https://owasp.org/www-project-web-security-testing-guide/stable/

OWASP. (15 de septiembre de 2021). *A01:2021 – Pérdida de control de acceso*. Obtenido de https://owasp.org/Top10/es/A01_2021-Broken_Access_Control/

OWASP. (15 de septiembre de 2021). *A02:2021 – Fallas criptográficas*. Obtenido de https://owasp.org/Top10/es/A02_2021-Cryptographic_Failures/

OWASP. (15 de septiembre de 2021). *A05:2021 – Configuración de seguridad incorrecta*. Obtenido de https://owasp.org/Top10/es/A05_2021-Security_Misconfiguration/

OWASP. (15 de septiembre de 2021). *https://owasp.org/Top10/es/A03_2021-Injection/*. Obtenido de https://owasp.org/Top10/es/A03_2021-Injection/

OWASP. (15 de septiembre de 2021). *https://owasp.org/Top10/es/A04_2021-Insecure_Design/*. Obtenido de https://owasp.org/Top10/es/A04_2021-Insecure_Design/

OWASP. (24 de septiembre de 2021). *OWASP top 10*. Obtenido de https://owasp.org/Top10/

OWASP. (27 de septiembre de 2021). *OWASP Top 10:2021.* Obtenido de https://owasp.org/Top10/

OWASP Foundation. (2013). *Penetration testing a way for improving our cyber security.* Obtenido de https://owasp.org/www-pdf-archive/OWASP_EU_Tour_2013_Bucharest_AdrianFurtuna.pdf

OWASP Joomla vulnerability scanner project. (16 de agosto de 2019). *JoomScan: Tool Documentation*. Obtenido de https://www.kali.org/tools/joomscan/

Paredes, F. (25 de mayo de 2022). *¿Cuales son las fases para la adecuada gestion de riesgos informaticos TI?.* Obtenido de https://www.magnetmex.com/tecnologia/gestion-de-riesgos-informaticos/

Penone, G. (29 de agosto de 2023). *CherryTree*. Obtenido de https://github.com/giuspen/cherrytree

Philpot james. (14 de abril de 2021). *Security incidents in healthcare infrastructure during COVID-19 Crisis.* Obtenido de https://www.safecare-project.eu/?p=588

Redacción KeepCoding . (26 de septiembre de 2022). *¿Qué es una vulnerabilidad informática?* Obtenido de https://keepcoding.io/blog/que-es-una-vulnerabilidad-informatica/

Sharma, A., Kumar, D., & Arora, N. (2022). *Supply chain risk factor assessment of Indian pharmaceutical industry for performance improvement.* International Journal of Productivity and Performance Management.

Shodan. (18 de septiembre de 2023). *acromax.com.ec*. Obtenido de https://www.shodan.io/domain/www.acromax.com.ec

Singular solutions. (24 de julio de 2023). *Servicio pentesting de webs, apps y sistemas*. Obtenido de EXEVI Singular Solutions: https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/

Spinelli Riso, A. (2018). *Ciberseguridad en pymes de la industria de retail farmacéutico: estudio de los casos zona vital y farma Belén.* Obtenido de https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16720/1/%5BP%5D%5BW%5D%20T.%20G.%20A.%20y%20C.%20Spinelli%20Riso,%20Agustín.pdf

Statcounter globalstats. (24 de julio de 2023). *Browser market share worldwide - june 2023[fotografía]*. Obtenido de https://gs.statcounter.com/browser-market-share

ZAP . (17 de octubre de 2023). *ZAP attack mode Scanning Report acromax*. Obtenido de https://www.zaproxy.org/