UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS:

Análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023

Para optar el título profesional de:
INGENIERO DE SISTEMAS

PRESENTADO POR:
Bach. Ramiro NUÑEZ PEREZ

ASESOR:
Dr. Ing. Manuel Avelino LAGOS BARZOLA

AYACUCHO - PERÚ

2025

Dedicatoria

A nuestro Creador, Dios, fuente de fortaleza y guía, cuya presencia ha sido un refugio constante, especialmente en tiempos de adversidad. Su protección y amor han sido nuestro sostén en cada momento de dificultad.

A mis queridos padres, quienes con su amor incondicional y su constante apoyo han sido la fuente que ha impulsado mi deseo de superación. Gracias por enseñarme a perseverar y por estar a mi lado en cada etapa de este camino. Sin su sacrificio, aliento y dedicación, no habría sido posible alcanzar este logro. Ustedes son mi mayor inspiración y el pilar sobre el que he edificado mis sueños.

Agradecimientos

Deseo expresar mi más profundo agradecimiento a la Universidad Nacional de San Cristóbal de Huamanga, así como a su distinguida facultad de Ingeniería de Sistemas, cuyos docentes, con su enfoque crítico y vocación académica, han sido pilares fundamentales en mi formación profesional, brindándome siempre la orientación necesaria para alcanzar mis objetivos.

Agradezco de manera especial a mi asesor, el Dr. Manuel Avelino Lagos Barzola, por su invaluable dedicación, por el tiempo que me brindó y por su orientación experta durante el desarrollo de este proyecto, lo cual ha sido fundamental para su culminación exitosa.

Asimismo, quiero extender mi gratitud a mis amigos, quienes con su apoyo y colaboración contribuyeron de manera significativa al avance de este trabajo.

Resumen

En la actualidad, la seguridad informática constituye un aspecto crítico para las instituciones públicas y privadas debido al incremento sostenido de ciberataques a nivel mundial. En el contexto peruano, diversos estudios han evidenciado deficiencias significativas en la protección de los sistemas informáticos, lo que posiciona al país en un nivel de alto riesgo dentro de la región. La Municipalidad Distrital de San Juan Bautista no es ajena a esta problemática, lo que evidencia la necesidad de evaluar el estado de seguridad de sus sistemas a través de un análisis de vulnerabilidades. El presente estudio tuvo como objetivo identificar y analizar las vulnerabilidades en la infraestructura informática de la municipalidad, con el propósito de evaluar su nivel de exposición y proponer medidas de mitigación. Para ello, se adoptó un enfoque de investigación aplicada, con un diseño no experimental y de nivel descriptivo. El análisis de vulnerabilidades se llevó a cabo mediante la metodología NIST SP 800-115, conjuntamente con herramientas y técnicas de hacking ético, como Sistema Operativo principal Kali Linux y aplicaciones como Shodan, BuiltWith, Google dorks, Nmap, Nslookup, Netcraft, BeEF, OWASP ZAP, Nikto, Burp Suite, con el fin de detectar vulnerabilidades en aplicaciones web y redes. El enfoque de hacking ético permitió simular escenarios de ataque controlados, evaluando la seguridad del sistema desde la perspectiva de un atacante con el objetivo de identificar brechas de seguridad y fortalecer la protección de la infraestructura digital. En conclusión, los hallazgos de este estudio evidencian la necesidad crítica de implementar auditorías de seguridad periódicas para garantizar la integridad, disponibilidad y confidencialidad de la información en instituciones públicas.

Palabras clave: Hacking Ético, Seguridad Informática, Análisis de Vulnerabilidades, Sistemas Informáticos y NIST SP 800-115.

Abstract

Currently, cybersecurity is a critical aspect for public and private institutions due to the sustained increase in cyberattacks worldwide. In Peru, various studies have revealed significant deficiencies in the protection of IT systems, placing the country at high risk within the region. The District Municipality of San Juan Bautista is no stranger to this problem, highlighting the need to assess the security status of its systems through a vulnerability analysis. The present study aimed to identify and analyze vulnerabilities in the municipality's IT infrastructure, with the goal of assessing its level of exposure and proposing mitigation measures. To this end, an applied research approach was adopted, with a non-experimental, descriptive design. The vulnerability analysis was conducted using the NIST SP 800-115 methodology, in conjunction with ethical hacking tools and techniques, such as the Kali Linux operating system and applications such as Shodan, BuiltWith, Google dorks, Nmap, Nslookup, Netcraft, BeEF, OWASP ZAP, Nikto, and Burp Suite, to detect vulnerabilities in web applications and networks. The ethical hacking approach allowed for the simulation of controlled attack scenarios, assessing system security from an attacker's perspective with the goal of identifying security breaches and strengthening the protection of digital infrastructure. In conclusion, the findings of this study highlight the critical need to implement periodic security audits to ensure the integrity, availability, and confidentiality of information in public institutions.

Keywords: Ethical Hacking, Computer Security, Vulnerability Analysis, Computer Systems, and NIST SP 800-115.

índice

Lista de tablas

Lista de figuras

Introducción

En la actualidad, la seguridad informática se ha convertido en un pilar fundamental para la protección de la información en instituciones públicas y privadas. El creciente número de ciberataques ha evidenciado la vulnerabilidad de los sistemas, comprometiendo la confidencialidad, integridad y disponibilidad de los datos. En el contexto peruano, diversos estudios han señalado deficiencias significativas en la seguridad digital, posicionando al país en una situación de alto riesgo dentro de la región. De acuerdo con El Peruano (2020), Perú es el segundo país de América Latina con los niveles más bajos de seguridad en línea, lo que resalta la necesidad de fortalecer las estrategias de protección de la información en el ámbito institucional.

En particular, la Municipalidad Distrital de San Juan Bautista no es ajena a esta problemática, ya que sus sistemas informáticos pueden ser blanco de amenazas cibernéticas debido a la falta de controles de seguridad adecuados. La ausencia de auditorías de seguridad periódicas y configuraciones de red insuficientes podrían facilitar ataques dirigidos contra su infraestructura tecnológica. Dado este panorama, resulta crucial realizar un análisis de vulnerabilidades para identificar los riesgos existentes y desarrollar estrategias de mitigación efectivas.

Este estudio tiene como objetivo identificar y analizar las vulnerabilidades en la infraestructura informática de la municipalidad, con el fin de evaluar su grado de exposición y proponer soluciones para fortalecer la ciberseguridad institucional. Para ello, se empleó un enfoque de investigación aplicada, con un diseño no experimental y descriptivo. La metodología se fundamenta en el NIST SP 800-115, complementada con herramientas avanzadas de hacking ético como OWASP ZAP, Nmap, y BeEF. Su propósito es evaluar la seguridad de los sistemas informáticos mediante pruebas de penetración, simulando ataques reales para identificar vulnerabilidades y establecer medidas de mitigación.

El hacking ético, como enfoque metodológico, ha demostrado ser una estrategia eficaz para la detección y mitigación de vulnerabilidades en infraestructuras informáticas. Esta técnica permite simular escenarios de ataque controlados, facilitando la identificación de brechas de seguridad y la formulación de estrategias preventivas. Además, posibilita la evaluación de la resiliencia de los sistemas frente a posibles ataques y la validación de las

medidas de seguridad implementadas.
Este estudio se estructura en los siguientes capítulos:

Capítulo I: Se presenta el planteamiento del problema, detallando el diagnóstico de la situación actual, la formulación del problema, los objetivos de la investigación y la justificación del estudio.

Capítulo II: Se aborda el marco teórico, proporcionando antecedentes nacionales e internacionales relevantes, así como conceptos fundamentales sobre seguridad informática, hacking ético y detección de vulnerabilidades.

Capítulo III: Se describe la metodología de investigación, especificando el tipo, nivel y diseño de estudio, así como las técnicas e instrumentos utilizados para la recolección de datos.

Capítulo IV: Se presentan los resultados y el análisis de datos, exponiendo los hallazgos obtenidos a través de las pruebas de seguridad realizadas en la infraestructura informática de la municipalidad.

Capítulo V: Se detallan las conclusiones y recomendaciones, enfatizando las medidas de seguridad propuestas para mitigar los riesgos detectados y fortalecer la resiliencia informática de la institución.

Este trabajo busca contribuir al fortalecimiento de la seguridad informática en el sector público, resaltando la importancia de realizar auditorías de seguridad periódicas, implementar soluciones tecnológicas avanzadas y promover el uso de hacking ético como una estrategia efectiva para la protección de los activos digitales.

Capítulo I

Planteamiento del Problema

1.1.Diagnóstico y enunciado del problema

En la actualidad, las instituciones en Perú enfrentan una escasa conciencia sobre los peligros asociados a los ciberataques, los cuales afectan negativamente sus transacciones, productividad y reputación corporativa. La seguridad en las redes ha dejado de ser un aspecto secundario, convirtiéndose en un factor fundamental para agregar valor a los servicios empresariales. No obstante, una mentalidad conservadora y la falta de interés por actualizar normas y procedimientos han retrasado la implementación de estándares modernos en control, gestión y seguridad informática en el país (Albújar, 2015).

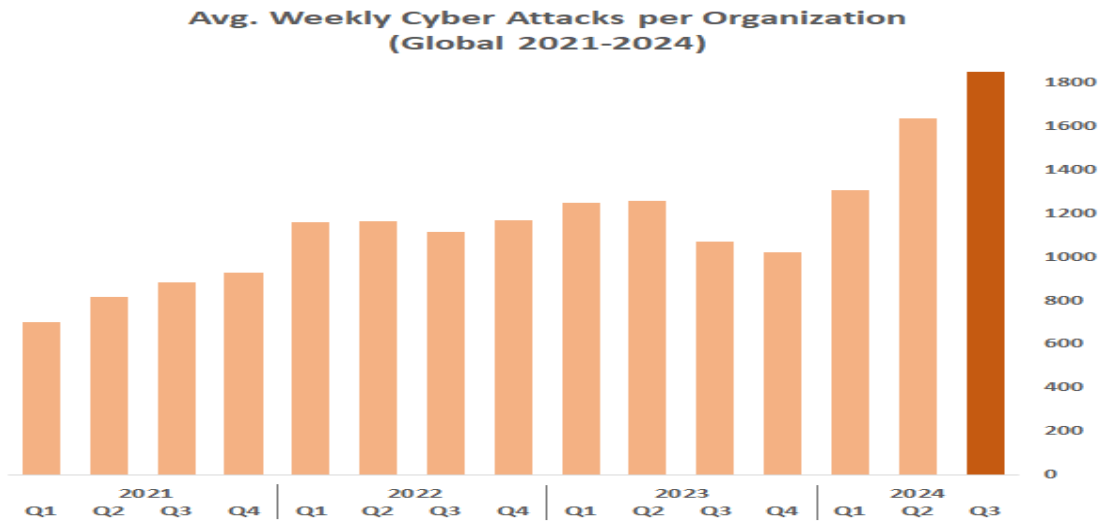
Esta falta de estándares no solo limita el progreso interno de Perú, sino que también perjudica su competitividad internacional. De acuerdo con el Diario El Peruano (2020), Perú es el segundo país de América Latina con los peores niveles de seguridad en línea, después de Brasil, y ocupa el puesto 17 a nivel globa l. Este ranking se basa en factores como infecciones por malware móvil, ciberataques financieros, infecciones informáticas, ataques telnet, criptominería y preparación ante ciberataques. Como resultado, Perú es visto como un país con deficiencias en la protección de la información personal, lo que restringe su acceso a los beneficios derivados del intercambio internacional de datos y tecnologías (Ruiz, 2020).

A su vez, la falta de medidas de seguridad en redes continúa siendo un problema creciente, exacerbado por el incremento de ciberatacantes organizados con habilidades especializadas, quienes sacan provecho de estas vulnerabilidades (Joyanes, 2015). Las aplicaciones web, consideradas una de las principales vías para los ciberataques, suelen ser vulnerables debido a la carencia de herramientas adecuadas, como antivirus, firewalls y sistemas de detección de intrusiones (González & Montesino, 2018).

Este panorama se ve reflejado en hechos concretos que han evidenciado la vulnerabilidad de las entidades gubernamentales. Un caso relevante es el de la Municipalidad Distrital de San Juan Bautista, cuya página web fue hackeada en dos ocasiones, los días 15 de junio de 2021 y 20 de diciembre de 2023. los ciberataques informáticos en los últimos tres años.

Figura 1

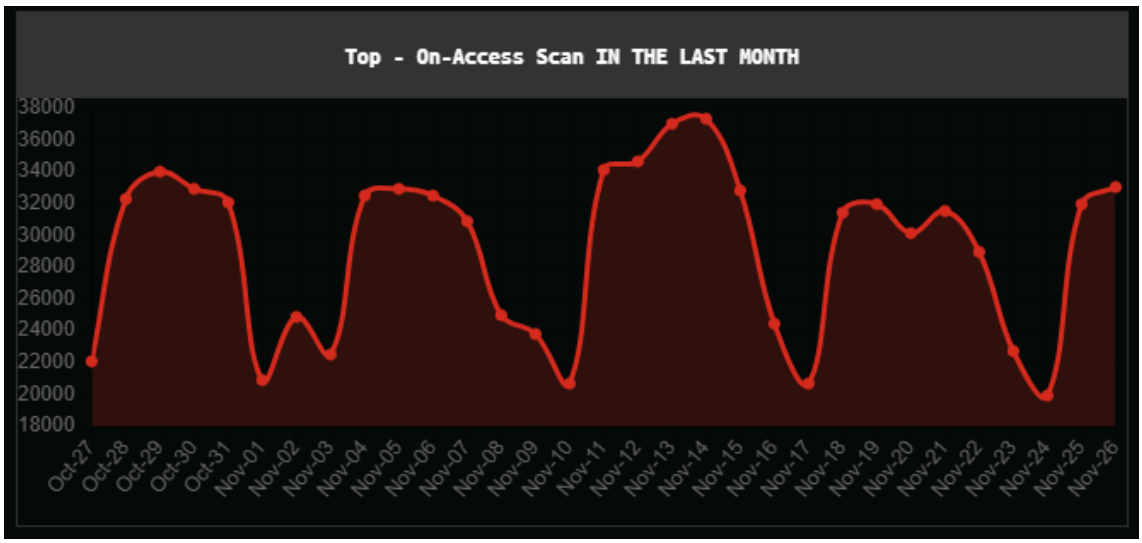
Estadística de los ciberataques informáticos en los últimos tres años.



Nota. En la imagen muestra que, en el tercer trimestre de 202, Tomado de (https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/, 2024).

Figura 2

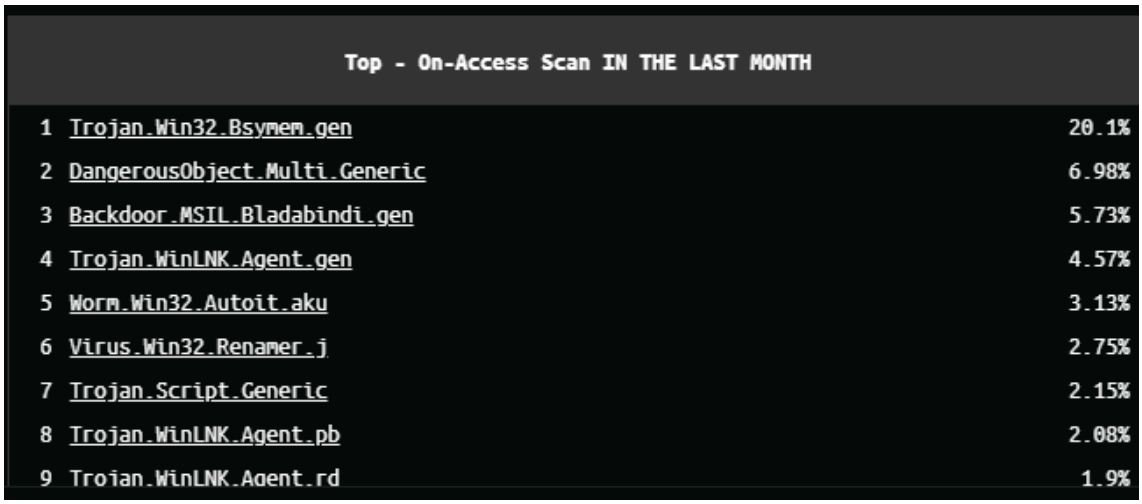
Estadística de los ciberataques informáticos en tiempo real en Perú en el 2024



Nota. El gráfico muestra los ataques de red registrados en el Perú entre el 27 de octubre y el 26 de noviembre de 2024. Tomado de (https://cybermap.kaspersky.com/, 2024).

Figura 3

Estadística de los tipos de ataques más frecuentes a redes en Perú.



Top - On-Access Scan IN THE LAST MONTH		
1	Trojan.Win32.Bsymem.gen	20.1%
2	DangerousObject.Multi.Generic	6.98%
3	Backdoor.MSIL.Bladabindi.gen	5.73%
4	Trojan.WinLNK.Agent.gen	4.57%
5	Worm.Win32.Autoit.aku	3.13%
6	Virus.Win32.Renamer.j	2.75%
7	Trojan.Script.Generic	2.15%
8	Trojan.WinLNK.Agent.pb	2.08%
9	Trojan.WinLNK.Agent.rd	1.9%

*Nota***.** La figura muestra los tipos de ataques más comunes registrados entre el 27 de octubre y el 26 de noviembre de 2024. Tomado de Kaspersky Cybermap (https://cybermap.kaspersky.com/), 2024.

Ahora enfocándonos en un plano local, al realizar un análisis de vulnerabilidades en una institución se pueden identificar y evaluar los riesgos de seguridad de los sistemas y servicios públicos, como redes de comunicaciones, sistemas de información y gestión de emergencias, cámaras de vigilancia, entre otros. De esta manera, se pueden detectar posibles vulnerabilidades y brechas de seguridad, y se pueden desarrollar estrategias y soluciones para mitigar estos riesgos y proteger los sistemas y servicios públicos.

Por ello el proceso de análisis de vulnerabilidades a realizar en el municipio de San Juan Bautista, para asegurar la integridad, disponibilidad de los sistemas y servicios públicos. También puede ayudar a mejorar la conciencia y la educación en seguridad cibernética de los empleados y funcionarios públicos, y a promover una cultura de seguridad en todo el municipio.

1.2.Formulación del problema

1.2.1. Problema principal

¿Cuáles son los resultados del proceso de análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023?

1.2.2. Problemas específicos

a. ¿Cuál es la información relevante de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023?

b. ¿Cuáles son las vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023?

c. ¿Cuáles son las medidas de seguridad informática para mitigar las vulnerabilidades en los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Desarrollar el proceso de análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023. Utilizando la metodología NIST SP 800-115., herramientas y técnicas de Hacking Ético, con el propósito, de identificar, evaluar, las vulnerabilidades y proponer medidas de seguridad; y la finalidad de establecer normativas y regulaciones en materia de seguridad informática y minimizar los riesgos.

1.3.2. Objetivos específicos

a. Determinar la información relevante de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023.

b. Identificar y analizar las vulnerabilidades de los sistemas informáticos en la Municipalidad Distrital de San Juan Bautista, 2023.

c. Plantear medidas de seguridad informática para la mitigación de vulnerabilidades en los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023.

1.4. Justificación y delimitación de la investigación

1.4.1. Justificación

La falta de recursos y la capacitación limitada en seguridad informática son factores comunes en muchas entidades públicas, como la Municipalidad Distrital de San Juan Bautista. Esta situación dificulta la implementación de mecanismos de seguridad actualizados y efectivos en sus sistemas informáticos. A menudo, se depende únicamente de herramientas tradicionales como firewalls y antivirus, que, si no se configuran adecuadamente, pueden representar vulnerabilidades críticas. Asimismo, la ausencia de procesos sistemáticos de análisis y evaluación de seguridad incrementa la exposición a amenazas externas e internas.

Esta investigación tiene como finalidad realizar un análisis exhaustivo de las vulnerabilidades presentes en los sistemas informáticos de la municipalidad, con el propósito de identificar y evaluar los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad de la información institucional. Para ello, se emplearán metodologías reconocidas en la industria, como las directrices de la NIST SP 800-115 y las recomendaciones del OWASP Top 10, apoyadas en el uso de herramientas de Hacking Ético, que permitirán detectar fallos de seguridad relevantes y valorar su impacto en la infraestructura tecnológica.

Con base en los hallazgos obtenidos, se propondrán soluciones concretas y adaptadas a las necesidades específicas de la municipalidad, orientadas a fortalecer la protección de sus sistemas informáticos. Este enfoque busca mitigar los riesgos de incidentes de seguridad informática y proteger uno de los activos más valiosos de la entidad: la información.

Además, se plantearán medidas de seguridad que no solo permitan remediar las vulnerabilidades identificadas, sino que también mejoren las capacidades de prevención, detección y respuesta ante amenazas futuras, promoviendo así una cultura de seguridad informática dentro de la organización.

1.4.2. Delimitación

La investigación se centró en el análisis de vulnerabilidades de los sistemas informáticos la Municipalidad Distrital de San Juan Bautista en 2023. El enfoque principal fue examinar la seguridad de la infraestructura web pública, evaluando posibles

fallas en la configuración, vulnerabilidades en los componentes utilizados, y posibles brechas de seguridad en la plataforma.

El análisis se centró en identificar vulnerabilidades críticas que pudieran comprometer la integridad de la página web y la protección de los datos de los usuarios, tales como la exposición de datos sensibles, inyecciones de código, fallos en el control de acceso y posibles configuraciones incorrectas en el servidor web. Se utilizaron herramientas de escaneo y metodologías de seguridad como NIST SP 800-115. y técnicas de hacking ético para identificar riesgos y proponer medidas correctivas.

Capítulo II
Marco Teórico

2.1. Antecedentes de la investigación

2.1.1. A nivel internacional

Wang y Yang (2017), en su investigación titulada "Hacking ético y defensa de la red: elija su mejor herramienta de escaneo de vulnerabilidades de red", desarrollaron un proyecto cuyo objetivo fue realizar prácticas en laboratorio relacionadas con el escaneo de vulnerabilidades en redes. En su estudio, utilizaron herramientas como OpenVAS y Nmap para identificar vulnerabilidades en la infraestructura de red. Este enfoque resulta relevante para el análisis de la seguridad de los sistemas informáticos de la municipalidad, ya que demuestra la efectividad de estas herramientas en la detección de puntos débiles en las redes.

Por otro lado, Ushmani (2018), en su estudio titulado "Hacking ético", exploró las fases del proceso de hacking ético, que incluyen reconocimiento, exploración, obtención de acceso, mantenimiento del acceso y cobertura de huellas. Estas fases ofrecen un marco claro y estructurado para el análisis de vulnerabilidades de los sistemas informáticos de la municipalidad, proporcionando una guía útil para identificar los riesgos y puntos débiles en la seguridad. Según Ushmani, el uso del hacking ético resulta fundamental para mitigar riesgos y mejorar la seguridad de los sistemas de comunicación e información.

De manera similar, Macías (2021) aplicó el concepto de hacking ético en la red wifi de la Universidad Estatal del Sur de Manabí. Su estudio reveló que un hacker logró acceder al sistema principal de la institución al explotar una vulnerabilidad en el software utilizado. Este hallazgo subraya la importancia de realizar pruebas de seguridad periódicas en las redes de las organizaciones, lo cual es crucial para tu investigación sobre la seguridad de las redes y sistemas informáticos de la municipalidad.

2.1.2. A nivel nacional

Según Tovar (2017): El propósito de la investigación desarrollada para su tesis fue implementar el hacking ético como una estrategia para mejorar la seguridad en la infraestructura informática del Grupo Electrodata. Este estudio, de tipo aplicado, permitió evaluar el estado real de la tecnología utilizada por la empresa. A través del proyecto, se

logró identificar con éxito la mayoría de las vulnerabilidades presentes en los dispositivos informáticos del Grupo Electrodata. Esta identificación permitió a la empresa comprender el nivel de exposición ante posibles amenazas y eventos perjudiciales. Además, el análisis de las vulnerabilidades permitió evaluar su viabilidad de explotación y brindar a la organización una mejor perspectiva sobre estas debilidades, facilitando así un análisis de riesgos más detallado y la formulación de medidas de mitigación. Se evidenció que la explotación de ciertas vulnerabilidades podría comprometer de manera crítica información sensible de la empresa. Como resultado, Grupo Electrodata obtuvo información clave para tomar acciones correctivas inmediatas y mitigar vulnerabilidades clasificadas como críticas.

De manera similar, López (2017): En su investigación titulada "Pentesting en aplicaciones web utilizando ética-hacking", se abordó como problemática principal la vulnerabilidad en el desarrollo de aplicaciones. El estudio describió pruebas y técnicas de penetración utilizando diversos métodos e instrumentos de software para detectar posibles vulnerabilidades en aplicaciones web específicas. Se emplearon metodologías como pruebas de penetración (pentesting), NIST SP 800-115., OSSTMM e ISSAF, junto con herramientas especializadas como Burp Suite, Acunetix, SQLMap, entre otras. Los resultados permitieron concluir que ninguna aplicación web es completamente segura o inmune a ataques. No obstante, mediante pruebas de intrusión, técnicas y herramientas de hacking ético, es posible identificar y mitigar vulnerabilidades, reduciendo significativamente la probabilidad de futuros ataques. López resaltó que en un mundo donde la comunicación y las operaciones dependen en gran medida de sistemas tecnológicos, las organizaciones deben priorizar la seguridad en el desarrollo de sus aplicaciones para protegerse contra amenazas emergentes.

2.2. Marco teórico

2.2.1. Análisis de vulnerabilidades.

Almeyda y colaboradores (2016) definen el análisis de vulnerabilidades como un proceso sistemático orientado a identificar debilidades y amenazas potenciales en sistemas, organizaciones o infraestructuras. Este análisis tiene como objetivo detectar áreas de riesgo y diseñar estrategias efectivas para prevenir o reducir su impacto. El proceso abarca diversos aspectos, como la seguridad física, la infraestructura de red, los sistemas operativos, las aplicaciones y los protocolos de comunicación. Para llevar a cabo

el análisis, se emplean diferentes técnicas que van desde pruebas manuales hasta el uso de herramientas automatizadas de escaneo y evaluación de vulnerabilidades.

2.2.2. Recopilación de información.

Según (Stallings & Brown, 2018). La recopilación de información en el ámbito de la seguridad informática es el proceso de identificar, recolectar y analizar datos sobre un sistema o red con el fin de evaluar su seguridad y detectar posibles vulnerabilidades. Este proceso es crucial para realizar una evaluación efectiva de la infraestructura informática y fortalecer su defensa contra ataques.

2.2.2.1 Identificar direcciones IP, nombres de dominio y redes

Según Kurose y Ross (2021), "una dirección IP es un identificador único asignado a cada dispositivo conectado a una red que utiliza el Protocolo de Internet para la comunicación" (p. 98).

Por otro lado, Tanenbaum y Wetherall (2019) “explican que los nombres de dominio facilitan la identificación de servidores y recursos en la web mediante nombres legibles para los humanos en lugar de direcciones numéricas."

2.2.2.2 Descubrir servicios y puertos activos

Según (Scarfone & Mell, 2009). Menciona, el descubrimiento de servicios y puertos activos es el proceso de escanear un sistema o red para identificar qué servicios están en ejecución y qué puertos están abiertos. Este procedimiento se realiza mediante herramientas como Nmap, que permite mapear la superficie de ataque de un sistema.

Según (Easttom , 2019), "el escaneo de puertos es una técnica utilizada para determinar qué servicios están activos en una máquina y evaluar posibles vulnerabilidades asociadas a ellos" (p. 125).

2.2.2.3 Identificar sistemas operativos y aplicaciones

Según (Stallings y Brown, 2018), "el reconocimiento del sistema operativo permite a un atacante o auditor de seguridad evaluar la superficie de ataque de un dispositivo en la red" (p. 210).

Esta información es crítica para evaluar la compatibilidad de parches de seguridad y estrategias de mitigación de vulnerabilidades. Determinar qué aplicaciones están instaladas en los dispositivos también permite identificar software obsoleto o inseguro.

2.2.2.4 Recopilar información sobre configuraciones

Según (Kurose y Ross, 2021), "una configuración segura implica establecer permisos adecuados, restringir accesos no autorizados y minimizar servicios innecesarios para reducir la exposición a ataques" (p. 275).

Este paso permite detectar configuraciones erróneas o inseguras que podrían ser explotadas por actores malintencionados. Incluye la revisión de políticas de acceso, permisos de usuario y configuraciones de firewall.

2.2.3. Identificación y análisis de vulnerabilidades

Según (Kizza, 2015) explica que este proceso consiste en evaluar sistemas y redes informáticos para detectar posibles vulnerabilidades y analizar su impacto potencial en la seguridad de la información. La identificación y el análisis de vulnerabilidades permiten determinar puntos débiles en los sistemas que podrían ser explotados por atacantes para comprometer la seguridad. Este procedimiento resulta fundamental para fortalecer la protección tecnológica, ya que ayuda a las organizaciones a identificar y mitigar amenazas antes de que sean aprovechadas por actores maliciosos. Entre los métodos empleados se incluyen las pruebas de penetración, el análisis de código, la revisión de configuraciones y las auditorías de seguridad. Dado que las amenazas a la seguridad de la información evolucionan constantemente, es crucial mantener un proceso continuo de detección y análisis de vulnerabilidades. Por ello, las empresas y organizaciones deben implementar medidas preventivas que garanticen la protección de sus sistemas y de la información que gestionan.

2.2.4. Medidas de seguridad informática

Según (Talib, Zaidan y Zaidan, 2018) describen la seguridad informática como un conjunto de métodos, herramientas y procesos diseñados para proteger la información almacenada o procesada en sistemas informáticos, evitando el acceso no autorizado, la alteración o la destrucción de los datos. Este enfoque incluye controles tecnológicos, físicos y administrativos que garantizan la disponibilidad, integridad y confidencialidad de la información. Entre las medidas más comunes se encuentran la autenticación de usuarios, el cifrado de datos, la implementación de cortafuegos, la realización de copias de seguridad periódicas y la capacitación y sensibilización de los usuarios. Además, resulta fundamental establecer normas y procedimientos de seguridad claros y asegurarse

de que todos los miembros de la organización estén informados sobre ellos. En general, aplicar medidas de seguridad informática es clave para prevenir y mitigar amenazas de ciberseguridad, así como para proteger los sistemas y datos de las empresas.

2.2.5. Sistemas informáticos

Según (Tanenbaum, 2015) en su obra Sistemas Operativos Modernos, los sistemas informáticos se componen de elementos físicos y lógicos que operan en conjunto para procesar y almacenar información. Estos sistemas tienen aplicaciones diversas, que van desde el manejo de datos empresariales hasta el desarrollo de videojuegos y aplicaciones móviles. Tanenbaum detalla el diseño y funcionamiento de los sistemas informáticos, abordando aspectos como la arquitectura de las computadoras, el software del sistema y la gestión de recursos. Además, examina su uso en contextos prácticos, incluyendo áreas como la computación en la nube y la inteligencia artificial.

2.2.6. Servidores

Según (Tanenbaum y van Steen, 2015), un servidor es un ordenador diseñado específicamente para proporcionar recursos y servicios a otros dispositivos dentro de una red. Entre los servicios que ofrece un servidor se encuentran el almacenamiento y compartición de archivos, la ejecución de aplicaciones, servicios web, correos electrónicos y mensajería, entre otros. Estos sistemas están equipados con software especializado para gestionar y controlar la información y servicios, así como con hardware de alta capacidad para garantizar una accesibilidad rápida y constante. Los servidores desempeñan un papel crucial en las redes corporativas de alto rendimiento, siendo responsables del mantenimiento de bases de datos, el soporte de aplicaciones empresariales y la transmisión de datos en tiempo real. Las organizaciones pueden mejorar la eficiencia y la seguridad de sus operaciones utilizando múltiples servidores, cada uno con funciones específicas adaptadas a sus necesidades.

2.2.7. Redes

De Según (Kurose y Ross, 2017), las redes consisten en un conjunto de dispositivos o sistemas informáticos, como ordenadores, servidores, enrutadores, conmutadores e impresoras, que están interconectados para compartir recursos y comunicarse entre sí. Estas conexiones permiten la transferencia de información, recursos y servicios en tiempo real, incluso entre dispositivos ubicados en diferentes partes del mundo. Las redes utilizan diversos medios físicos, como cables, fibra óptica, señales de

radio o infrarrojos, para establecer estas conexiones. Además, pueden clasificarse según su alcance, tamaño y topología, y tienen múltiples aplicaciones, como la colaboración en equipo, el acceso a recursos compartidos, el intercambio de archivos y la comunicación en tiempo real.

2.2.8. Plataformas web

Según (O'Reilly, 2005), las plataformas web son aplicaciones basadas en la web que, a través de un navegador, permiten a los usuarios acceder y utilizar una amplia variedad de servicios en línea. Estas plataformas abarcan desde herramientas simples de productividad y almacenamiento en la nube hasta complejos sistemas de gestión de contenidos y software de comercio electrónico. Se distinguen por ofrecer interfaces de programación de aplicaciones (API) y herramientas para desarrolladores. Su creciente popularidad en los últimos años se debe a su adaptabilidad, escalabilidad y accesibilidad desde cualquier dispositivo con conexión a Internet. Las plataformas web facilitan el almacenamiento de datos en la nube, el acceso a recursos compartidos, la colaboración entre usuarios y la integración con aplicaciones y servicios de terceros, destacándose por estas funcionalidades clave.

2.3. Haking ético

Según (Gómez, 2015), el hacking ético es una disciplina dentro de la seguridad de la tecnología de la información que se enfoca en evaluar de manera legal y aprobada los riesgos y vulnerabilidades de los sistemas o activos informáticos de una organización.

En este sentido, el hacking ético es una técnica esencial para cualquier organización preocupada por la protección de su información, ya que permite identificar fallos de seguridad, explotarlos de manera controlada y ofrecer recomendaciones para fortalecer la infraestructura y los sistemas de información de la organización (Medina Rojas, s.f., 2020).

De manera similar, el objetivo principal del hacking ético es identificar y explotar vulnerabilidades en los sistemas, utilizando pruebas de penetración para evaluar tanto la seguridad lógica como física de datos, aplicaciones web, servidores y redes. El servicio de hacking ético simula un ataque gestionado, lo cual proporciona a la empresa información valiosa para defenderse contra posibles ciberataques al implementar medidas preventivas (De la Torre, 2017).

Por otro lado, según (Hacking Ético s.f., 2021), este método consiste en utilizar conocimientos informáticos y de seguridad para evaluar redes, descubrir vulnerabilidades y reportarlas para que se tomen medidas correctivas sin causar daño. El propósito es identificar qué componentes de una red son vulnerables al robo de información y tomar medidas para parchearlos antes de que ocurra un ataque real.

Finalmente. (Informática, 2016) destaca que el análisis de programas informáticos es fundamental en el hacking ético, cuyo objetivo principal es evaluar la seguridad actual de la información. Es esencial obtener el permiso de la empresa, institución u organización antes de realizar un hacking ético, así como establecer un contrato que respete los derechos y normas de la organización, para luego proporcionar los resultados obtenidos.

2.3.1. Nist sp-800-115

La metodología NIST SP 800-115 establece directrices sobre cómo llevar a cabo una Evaluación de Seguridad de la Información (ESI), conceptualizándola como el proceso de determinar cuán efectivamente una entidad cumple con objetivos específicos de seguridad. En este contexto, se considera como elementos de evaluación tanto los activos como los objetos, tales como servidores, redes de datos, procedimientos y personas (Digital, 2017).

En el ámbito de la Evaluación de la Seguridad de la Información, se pueden utilizar tres enfoques diferentes de evaluación.

- **Pruebas:** Consiste en someter uno o varios elementos evaluados a condiciones controladas para comparar su comportamiento observado con las expectativas establecidas, lo que permite realizar un análisis comparativo de los resultados.
- **Escrutinio:** Este enfoque implica un examen detallado, inspección, revisión y observación minuciosa de los elementos evaluados, con el fin de profundizar en su comprensión, resolver dudas y recopilar información relevante que pueda servir como evidencia.
- **Entrevista:** Este método se basa en la comunicación directa con los grupos de personas involucradas o relacionadas con el objeto de evaluación, con el objetivo de obtener aclaraciones y testimonios que proporcionen evidencia significativa para el proceso de evaluación.

Figura 4

La figura ilustra las fases de Nist sp-800-115.

Nota. Fases de nist sp-800-115.

La NIST SP 800-115 establece un proceso de Evaluación de Seguridad de la Información (ESI) que incluye, al menos, tres fases principales.

Fase de planificación: En esta fase, se establecen las pautas que guiarán todo el proceso, se definen claramente los objetivos a alcanzar y se gestionan las aprobaciones necesarias para continuar. Al mismo tiempo, se preparan las condiciones técnicas y organizativas que asegurará el éxito de la prueba. Es importante señalar que durante esta etapa no se lleva a cabo ninguna evaluación de seguridad real; más bien, se dedica exclusivamente a la preparación y organización detallada de la prueba que se realizará (Digital, 2017)..

Fase de descubrimiento: En esta etapa, se lleva a cabo una investigación exhaustiva y recolección de información sobre la infraestructura tecnológica de la organización. También se realizan escaneos para identificar servicios y tecnologías activos; con los datos obtenidos, se procede a buscar posibles vulnerabilidades, consultando tanto bases de datos públicas como internas (Digital, 2017).

Fase de ejecución: Esta fase constituye el núcleo del proceso. Se ponen a prueba las vulnerabilidades identificadas previamente, intentando explotarlas. Cuando un ataque tiene éxito, se procede a aislar y documentar detalladamente la vulnerabilidad, además de proponer medidas correctivas. Las actividades en esta fase incluyen la obtención y

elevación de privilegios, así como la exploración interna del sistema. En algunos casos, puede ser necesario instalar herramientas adicionales para recopilar más información o obtener accesos de mayor nivel (Digital, 2017)..

Fase de documentación y reporte: Esta fase se lleva a cabo de manera paralela con las etapas anteriores y se encarga de recopilar la información necesaria para el informe final. En la fase de Planificación, se documentan las reglas de evaluación y las pautas de interacción. En la fase de descubrimiento, se guardan los informes generados por los escáneres de vulnerabilidades y otros datos relevantes obtenidos. Durante la fase de Ejecución, se archivan los informes creados por las herramientas de explotación de vulnerabilidades. Al concluir la prueba de intrusión, se elabora un informe que describe las vulnerabilidades identificadas, evalúa los riesgos y proporciona recomendaciones para mitigar las debilidades encontradas (Digital, 2017).

2.3.2. Fases del hacking ético

Según (Niño, 2019), se destaca que un modelo de referencia es crucial para guiar al hacker ético durante las pruebas de penetración, asegurando que sus acciones sean sistemáticas y bien estructuradas. En este contexto, se pueden identificar cinco etapas clave dentro del proceso de hacking ético. Aunque el hacker ético realiza acciones similares a las de un hacker malicioso, su enfoque es completamente legal y tiene como objetivo identificar y corregir vulnerabilidades para mejorar la seguridad de los sistemas.

Figura 5

La figura ilustra las fases del hacking ético.

Nota. En la imagen ilustra las 5 etapas de hacking ético.

2.3.1.1. Reconocimiento

Según (Niño, 2018), en esta etapa, el individuo se organiza para iniciar la recolección e investigación de datos esenciales necesarios para un objetivo específico, utilizando diversos recursos o técnicas. El autor resalta que este proceso de recopilación es clave, ya que permite al individuo obtener la información crucial para avanzar en el objetivo. Además, se hace necesario distinguir entre dos tipos de reconocimiento, los cuales se describen a continuación:

a. Reconocimiento pasivo.

Consiste en la recopilación y análisis de información sin establecer ninguna conexión directa con la organización objetivo. Este tipo de reconocimiento se realiza principalmente a distancia, utilizando métodos como la observación o vigilancia del objetivo. Sin embargo, es más común que se lleve a cabo a través de Internet, donde es más fácil acceder a los datos necesarios de forma precisa y sin alertar a la entidad objetivo.

b. Reconocimiento activo.

A diferencia del reconocimiento pasivo, el reconocimiento activo implica un contacto directo con la red de la organización objetivo. Este tipo de acción puede conllevar riesgos, ya que las personas que lo practican se exponen a ser descubiertas. Si el objetivo lo detecta, es probable que la empresa tome medidas inmediatas para identificar al intruso y localizar su origen.

Según (Bermeo, 2017), en la fase de reconocimiento, se recolecta toda la información necesaria sobre el objetivo, utilizando una variedad de estrategias, herramientas y técnicas. En este proceso, se pueden emplear tanto el reconocimiento pasivo como el activo para obtener los datos más relevantes y precisos.

El reconocimiento pasivo y activo son dos enfoques fundamentales en el proceso de recopilación de información durante el hacking ético. Ambos métodos ayudan a los hackers éticos a obtener información clave sobre un objetivo, pero se diferencian en cómo se obtiene esa información y el riesgo de ser detectado.

a. Pasivo.

En esta fase, el hacker obtiene información sobre un objetivo sin interactuar directamente con la red o el sistema. El objetivo es obtener datos de manera indirecta y sin alertar a la

organización objetivo. Algunos de los métodos comunes en el reconocimiento pasivo incluyen:

- Dumpster diving: Recuperación de información valiosa de los desechos físicos, como documentos tirados.
- Búsqueda en motores de búsqueda: Utilización de herramientas como Google para encontrar información pública.
- Búsqueda en bases de datos Whois: Obtener información sobre nombres de dominio y registros relacionados con las direcciones IP.
- Búsqueda de ubicación de servidores: Determinar la localización geográfica de los servidores mediante herramientas de geolocalización de IPs.
- Búsqueda de nombres de dominio: Investigar registros de dominios y las entidades asociadas.
- Recopilación de datos de DNS: Obtener información sobre servidores de nombres de dominio, que puede revelar más detalles sobre la infraestructura de la red.

b. Activo.

El reconocimiento activo implica interactuar directamente con la red o los sistemas del objetivo, lo que aumenta el riesgo de detección. A través de métodos activos, el hacker ético puede obtener detalles técnicos más precisos sobre la red y los dispositivos. Algunos métodos incluyen.

- **Manipulación social:** Engañar a las personas dentro de la organización para obtener acceso a información sensible.
- **Port Scanning:** Escaneo de puertos de red para identificar servicios activos.
- **Herramientas de escaneo de red**: Utilización de programas como Nmap para mapear y examinar la red.
- **Determinación de direcciones IP**: Identificar el rango de direcciones IP activas en la red.
- **Determinación del sistema operativo:** Identificar qué sistema operativo se está utilizando en los dispositivos de la red.
- **Identificación de dispositivos activos:** Determinar qué máquinas están en funcionamiento en la red.
- **Identificación de cuentas de usuario activas:** Obtener información sobre las cuentas que están en uso en la red.

- **Investigación de routers:** Determinar la ubicación y configuración de los routers en la red.

Según (FasesHackingEtico, 2019), ambos tipos de reconocimiento, tanto pasivo como activo, pueden ser fundamentales para descubrir puntos débiles en la infraestructura de una organización. Esta información recopilada puede ser utilizada para identificar vulnerabilidades específicas que, en combinación con otras técnicas, pueden ser explotadas para ganar acceso no autorizado o comprometer la seguridad del sistema.

2.3.1.2. Exploración

En esta fase, el profesional de Hacking Ético interactúa directamente con la empresa objetivo para identificar servidores, direcciones IP y otra información relevante para el análisis de vulnerabilidades. Aquí, el experto adopta un enfoque más agresivo en la recolección de datos, lo que le permite aumentar las posibilidades de encontrar fallos en la configuración o vulnerabilidades en el sistema. Como resultado, se mejora la probabilidad de detectar debilidades en la seguridad de la empresa que podrían ser aprovechadas para comprometer sus sistemas. (Tovar, 2020).

Según (Bermeo, 2017), antes de intentar atacar una red, el hacker pasa por esta fase, que se denomina exploración, donde usa toda la información adquirida durante la fase de reconocimiento para identificar vulnerabilidades específicas.

2.3.1.3. Obtener acceso

Según (Bermeo, 2017), esta fase es crucial para el hacker, ya que es el momento en el que se obtiene acceso al sistema vulnerable. Durante esta etapa, el hacker explota las vulnerabilidades identificadas en la fase anterior (fase de exploración), lo que la convierte en una de las fases más importantes en el proceso.

La explotación ocurre frecuentemente de forma:

- LAN (Local Area Network): Acceso a través de la red local de la organización.
- Offline (sin estar conectado): Realización de ataques sin conexión a la red, utilizando herramientas o dispositivos externos.
- Internet: Ataques a través de la red pública, aprovechando vulnerabilidades accesibles desde cualquier parte del mundo.

Según (Tovar, 2020), en esta fase se pone a prueba la habilidad del Hacker Ético, ya que será el encargado de intentar explotar personalmente las vulnerabilidades descubiertas en la fase anterior, la de Exploración de Vulnerabilidades. Dependiendo de los ataques ejecutados, el Hacker Ético puede llegar a tomar control total del sistema comprometido y aumentar sus privilegios.

El esfuerzo del intruso se justifica en este momento, pues es cuando se aprovechan las vulnerabilidades encontradas previamente para obtener acceso a la red. Si el infiltrado logra ingresar, podrá acceder a múltiples puntos de control dentro del sistema, lo que expondrá a todos los usuarios y recursos vinculados a la red a riesgos. (Plinio, 2012).

2.3.1.4. Mantener acceso

Una vez que el hacker ha logrado acceder al sistema, lo más importante es mantener ese acceso, ya que existen diversas formas en las que puede perderlo si es descubierto. Para asegurar el acceso, el hacker puede emplear métodos como puertas traseras, infecciones con troyanos y otros recursos que le permitan acceder al sistema cuando lo necesite en el futuro. Es vital que el hacker utilice herramientas como conexiones Telnet y FTP para mantener el acceso, al tiempo que trata de pasar desapercibido. Además, en esta fase, el hacker emplea sniffers para capturar el tráfico de red, lo cual le permite obtener información sobre los dispositivos que interactúan con su objetivo y crear una identidad falsa para suplantar una de las direcciones de confianza. Durante este proceso, es crucial que elimine cualquier rastro dejado por su intrusión, manteniendo el acceso mediante puertas traseras y troyanos, y utilizando estas herramientas para obtener privilegios elevados (como administrador) o robar información como contraseñas y datos bancarios (Fernández, 2017; Orlando, 2018).

Esta fase ocurre después de que se ha adquirido acceso al sistema. El hacker, en este momento, puede utilizar técnicas como puertas traseras, rootkits y troyanos para reforzar su control sobre el sistema comprometido. Además, el hacker puede usar el sistema vulnerable para lanzar ataques a otros sistemas, aprovechando tanto sus propios recursos como los del sistema comprometido. En esta etapa, también se emplean sniffers para interceptar el tráfico de la red, incluidas las sesiones Telnet y FTP, con el fin de obtener más información y continuar explotando las vulnerabilidades de otros sistemas dentro o fuera de la red (FasesDelHackingÉtico, 2014).

2.3.1.5. Cubrir los pasos

(FasesDelHackingÉtico, 2014), esta fase se refiere a los esfuerzos que realiza el hacker para descubrir y eliminar cualquier prueba de su presencia y de los actos ilegales cometidos. Los piratas informáticos intentan borrar todos los rastros de un ataque, como archivos de registro o advertencias generadas por sistemas de detección de intrusos (IDS), con el objetivo de ocultar su rastro o protegerse de consecuencias legales. Una de las razones principales para eliminar estas pruebas es seguir manteniendo el acceso al sistema comprometido. Al borrar sus huellas, los administradores de red no podrán detectar la intrusión, lo que facilita que el hacker conserve su acceso sin ser descubierto.

Según (Reyes, 2015) señala que, después de lograr entrar exitosamente en el sistema y cumplir sus objetivos, el infiltrado debe proceder a investigar y borrar cualquier evidencia de su actividad. Esto le permite mantener el acceso y continuar entrando al objetivo cuando lo desee.

Por su parte, (Bermeo, 2017) menciona que, en esta fase, el hacker se enfoca en eliminar toda prueba de su presencia y actividades ilegales. Esta acción se realiza con el fin de mantener el acceso al sistema comprometido, ya que, si se eliminan las huellas, los administradores no podrán encontrar evidencia clara de la intrusión. Además, borrar los rastros ayuda a evitar ser detectado por las autoridades de ciberseguridad.

2.3.3. Hacking ético

La información y los datos que una empresa posee son esenciales para su funcionamiento. Sin embargo, existe el riesgo de que los sistemas no sean tan seguros como parecen, lo que podría afectar gravemente las operaciones de la organización. En este contexto, es necesario realizar una revisión exhaustiva de la seguridad para asegurarse de que los problemas se resuelvan en la medida de lo posible. En este proceso, los técnicos especializados juegan un papel fundamental, y en ocasiones, se recurre a expertos en la materia para realizar un análisis más profundo y ejecutar diversas pruebas y ataques. El objetivo es determinar si el sistema es completamente seguro y puede resistir cualquier imprevisto, como los ataques cibernéticos (Sogeti, 2018).

De manera similar, (Sogeti, 2018) señala que la información obtenida y gestionada por los profesionales encargados de evaluar las vulnerabilidades se organiza siguiendo modelos establecidos de hacking ético. Estos modelos guían el trabajo para asegurar que todas las

áreas de la red sean evaluadas y que los datos obtenidos se presenten de manera precisa y completa. Entre los métodos más importantes se encuentran OSSTMM, ISSAF y NIST SP 800-115.

Por otro lado, (Durand, 2019) agrega que la metodología empleada en las pruebas de pentesting es crucial, ya que define cómo se llevará a cabo cada prueba. Para ello, se destacan tres enfoques fundamentales: OSSTMM, ISAAF y NIST SP 800-115., los cuales se explorarán en detalle a continuación.

2.3.2.1. Osstmm

Según (Cruz, 2017), el OSSTMM es un modelo que asegura la seguridad continua y validada del sistema, lo cual lo convierte en una función crucial. Esta estrategia comenzó a implementarse en el año 2000, con un enfoque progresivo aprobado por métodos de protección.

A lo largo de 2005, este enfoque empezó a ganar reconocimiento no solo por su capacidad para implementar procedimientos eficaces, sino también por garantizar la ausencia de riesgos. Debido a su éxito, en 2006, OSSTMM se consolidó como una de las herramientas más utilizadas (Sogeti, 2018).

Con la introducción de la comunicación a distancia en el mercado, el sector de redes dentro de las organizaciones experimentó transformaciones significativas que complicaron su funcionamiento, requiriendo una arquitectura distinta. Como los modelos de estudio de las regiones vulnerables debían adaptarse a estos nuevos requisitos, el OSSTMM introdujo modificaciones en sus versiones para ser más útil en la realización de pruebas en diversos lugares y medios (Sogeti, 2018).

De igual manera, (Cruz, 2017) sostiene que esta táctica es una de las mejores opciones disponibles, ya que permite ejecutar de manera eficaz las actividades necesarias. Esto significa que administradores, técnicos y expertos en seguridad pueden utilizarla para estudiar, probar y verificar que el sistema funcione adecuadamente en caso de que un hacker intente obtener información de forma inapropiada. En caso de que los resultados no sean satisfactorios, es crucial definir las acciones correctivas para mejorar y contrarrestar el problema.

El Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) se creó como un método científico para evaluar la seguridad de una empresa a través de

diversos controles, comenzando desde el exterior y avanzando hacia el interior. Este manual detalla las fases de las pruebas de seguridad operativa, abarcando aspectos como los canales humanos, inalámbricos, físicos, telecomunicaciones, redes de datos, y otros elementos derivados de métricas efectivas. También proporciona directrices para los asistentes del sistema con el fin de legalizar la empresa de acuerdo con las normas de ISECOM (Valencia, 2013).

2.3.2.2. Issaf

Según (Gontharet y Testing, 2015), el Marco de Evaluación de la Seguridad de los Sistemas de Información, también conocido como el marco de evaluación de la protección del sistema de datos, es uno de los marcos más reconocidos en el ámbito de la seguridad informática. Fue implementado por la OISSG con el objetivo de abordar los requisitos de seguridad de las empresas en un entorno donde la información se considera un activo valioso. Muchas organizaciones, sin embargo, no prestan la debida atención a la seguridad de la información, lo que puede comprometer sus datos y sistemas.

Este marco no solo proporciona procedimientos estandarizados para evaluar las prácticas de protección de los sistemas, sino que también va más allá al explicar cómo y por qué es necesario realizar una verificación de la seguridad. Esta característica distingue al Marco de Evaluación de la Seguridad de los Sistemas de Información de otros informes y manuales, ya que no se limita a ser un manual paso a paso, sino que también ofrece una justificación integral de la importancia de las verificaciones de seguridad (Gontharet & Testing, 2015).

Por otro lado, (López, 2015) señala que el Marco de Evaluación de la Seguridad de los Sistemas de Información está dirigido a una variedad de profesionales de la seguridad, incluidos administradores de seguridad perimetral, gestores de vulnerabilidades internas y externas, consultores e ingenieros de seguridad, así como gestores de sistemas y redes. Además, está diseñado para ser útil a los administradores funcionales y técnicos, así como a la comunidad más amplia de profesionales de la seguridad de la información.

2.3.2.3. Owasp

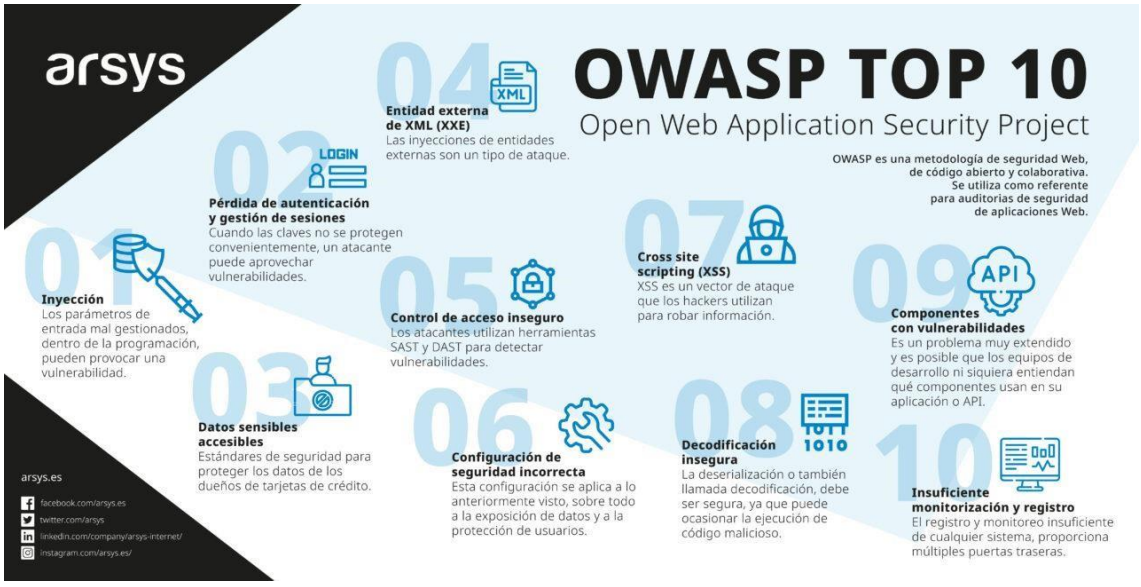
Según (Sanz, 2018), el Open Web Application Security Project (OWASP) es una iniciativa global enfocada en mejorar la seguridad de las aplicaciones web. Su objetivo es fomentar y motivar a los desarrolladores, tanto individuales como de empresas, para crear

aplicaciones que sean más seguras, proporcionando confianza en los sistemas de software utilizados en el ámbito corporativo. OWASP se ha consolidado como una referencia clave para modernizar y fortalecer la seguridad de las aplicaciones, ofreciendo recursos y directrices que permiten a las organizaciones mejorar la seguridad en sus desarrollos.

Por otro lado, (Valencia, 2013) destaca que OWASP, al ser una metodología centrada en la seguridad de las aplicaciones, impulsa a los recursos humanos involucrados en el desarrollo a verificar y aplicar medidas de seguridad durante todo el proceso de creación del software. Esta metodología resalta la importancia de identificar los costos de un software vulnerable y cómo estos costos impactan negativamente a las empresas, lo que finalmente lleva a las organizaciones a tomar decisiones más efectivas para mitigar los riesgos. Al integrar la seguridad en las etapas de desarrollo, OWASP busca garantizar que las aplicaciones sean seguras desde su concepción hasta su implementación.

Figura 6

Esquema de Open Web Application Project (OWASP).



Nota. La figura ilustra las características de cada proceso dentro de la metodología de OWASP (Beale, Long, Orebaugh, Kanclirz, & Haines, 2019).

A. OWASP Top 10 2017 Riesgos en Seguridad de Aplicaciones

A1:2017 Inyección

Según (Broad y Bindner, 2018) Las vulnerabilidades de inyección, como las de SQL, NoSQL, OS o LDAP, se presentan cuando se envían datos no seguros a un

procesador, como parte de un comando o consulta. Los atacantes pueden manipular estos datos para que el procesador ejecute acciones no deseadas o acceda a información sin autorización.

A2:2017 Pérdida de autenticación

Según (Broad y Bindner, 2018) Este riesgo se da cuando las funciones relacionadas con la autenticación y gestión de sesiones están mal implementadas, lo que permite que los atacantes comprometan credenciales de usuarios, tokens de sesión, o aprovechen otras fallas para suplantar la identidad de los usuarios, ya sea de manera temporal o permanente.

A3:201 Exposición de datos sensibles

Según (Broad y Bindner, 2018) Algunas aplicaciones web y APIs no protegen adecuadamente los datos sensibles, como información financiera, de salud o personalmente identificable (PII). Los atacantes pueden robar o alterar estos datos mal protegidos para llevar a cabo fraudes o robos de identidad. Para proteger estos datos, se requieren medidas adicionales como el cifrado tanto en tránsito como en almacenamiento.

A4:2017 Entidades externas XML (XXE)

Según (Broad y Bindner,2018) Algunos procesadores XML, especialmente los antiguos o mal configurados, pueden evaluar referencias a entidades externas dentro de documentos XML. Estas entidades pueden ser utilizadas por los atacantes para revelar archivos internos, realizar escaneos de puertos, ejecutar código de forma remota o provocar ataques de denegación de servicio (DoS).

A5:2017 Pérdida de control de acceso

Según (Broad y Bindner, 2018) Este problema ocurre cuando las restricciones de acceso para los usuarios autenticados no se implementan correctamente. Los atacantes pueden aprovechar esta falla para acceder sin autorización a funcionalidades o datos, ver archivos confidenciales, modificar información o cambiar permisos y derechos de acceso.

A6:2017 Configuración de seguridad incorrecta

Según (Broad y Bindne, (2018) Una configuración incorrecta de seguridad es común y suele deberse a configuraciones manuales, predeterminadas o mal gestionadas. Ejemplos incluyen almacenamiento sin protección de datos en S3, cabeceras HTTP mal

configuradas, errores que revelan información sensible, falta de actualizaciones o el uso de componentes desactualizados.

A7:2017 Secuencia de comandos en sitios Cruzados (XSS)

Según (Broad y Bindner, 2018) Los ataques XSS ocurren cuando una aplicación procesa datos no confiables y los envía al navegador sin una validación o codificación adecuada. Esto permite que los atacantes ejecuten comandos en el navegador de la víctima, secuestren sesiones, alteren el contenido de páginas o redirijan al usuario hacia sitios maliciosos.

A8:2017 Deserialización insegura

Según (Broad y Bindner, 2018) Estos defectos surgen cuando una aplicación procesa objetos serializados dañinos que pueden ser manipulados por los atacantes. Esto puede llevar a ataques de repetición, inyecciones o incluso a la ejecución remota de código en el servidor si la deserialización no es manejada de forma segura.

A9:2017 Componentes con vulnerabilidades conocidas

Según (Broad y Bindner, 2018) Cuando una aplicación utiliza componentes como bibliotecas o frameworks con vulnerabilidades conocidas, un atacante puede explotar estas fallas para obtener acceso no autorizado, comprometer datos o tomar control del servidor. Esto debilita las defensas de la aplicación y aumenta el riesgo de diversos ataques.

A10:2017 Registro y monitoreo insuficientes

Según (Broad y Bindner, 2018) La falta de un registro adecuado y un monitoreo eficaz de las actividades en las aplicaciones permite a los atacantes persistir en sus ataques, mover su acceso a otros sistemas y manipular o robar datos. Los estudios han mostrado que el tiempo promedio para detectar una brecha de seguridad supera los 200 días, y a menudo se detecta por terceros en lugar de por los procesos internos de seguridad.

2.4. Herramientas de hacking ético

2.4.1. Kali Linux

Según (Broad y Bindner, 2018), Kali Linux se presenta como una herramienta fundamental en la auditoría de sistemas de información, especialmente en el contexto del hacking ético. Kali Linux, desarrollado por Offensive Security, es ampliamente utilizado

por consultores de seguridad informática para realizar pruebas de intrusión debido a su vasta gama de herramientas integradas. Estas herramientas permiten a los hackers éticos realizar todas las etapas críticas del proceso de hacking ético, desde la recopilación de información hasta la explotación de vulnerabilidades y el análisis forense.

Entre las herramientas más destacadas que Kali Linux ofrece se incluyen:

Herramientas de análisis de vulnerabilidades

- **Nmap:** Herramienta de escaneo de redes utilizada para detectar puertos abiertos, servicios y sistemas operativos, permitiendo identificar posibles vulnerabilidades en la infraestructura de red.
- **Nikto**: Un escáner de vulnerabilidades web que analiza servidores web en busca de configuraciones inseguras y vulnerabilidades conocidas, como fallos en software y configuraciones incorrectas.
- **OWASP ZAP (Zed Attack Proxy):** Herramienta de seguridad de código abierto diseñada para encontrar vulnerabilidades en aplicaciones web, especialmente útil en pruebas de penetración automáticas y manuales.

Herramientas de explotación

- **SQLmap:** Herramienta automatizada que permite identificar y explotar vulnerabilidades de inyección SQL en aplicaciones web.
- **BeEF (Browser Exploitation Framework):** Framework que se utiliza para explotar vulnerabilidades en los navegadores web, facilitando la explotación de clientes a través de técnicas como el cross-site scripting (XSS).

Herramientas de post-explotación

- **Mimikatz:** Herramienta utilizada para la extracción de credenciales en sistemas Windows, permitiendo la captura de contraseñas y hashes de autenticación.
- **Netcat:** Herramienta versátil de red que se puede usar para establecer conexiones de red, escuchar puertos, transferir archivos, entre otros. Es útil durante la post-explotación para mantener accesos remotos.

- **PowerShell empire:** Herramienta de post-explotación para PowerShell que proporciona capacidades avanzadas para controlar máquinas Windows y ejecutar scripts maliciosos.
- **Cobalt strike**: Herramienta avanzada para post-explotación, conocida por su capacidad para crear agentes de acceso y realizar ataques de manipulación de memoria, entre otros.

Según (Gonzales y Sánchez, 2013), Kali Linux es un sistema operativo ampliamente utilizado por consultores de seguridad informática, especialmente en el ámbito de las pruebas de intrusión o hacking ético. Kali Linux, desarrollado por Offensive Security, se considera una distribución de seguridad robusta y madura debido a la amplia selección de herramientas que ofrece para realizar auditorías de seguridad y pruebas de penetración en sistemas y redes. Estas herramientas permiten llevar a cabo todas las etapas críticas del proceso de hacking ético, desde la recopilación de información hasta la explotación de vulnerabilidades.

2.4.2. Nmap

Según (Tovar, 2020), se trata de una herramienta informática que permite realizar escaneos de red. La mayoría de los profesionales de la seguridad la utilizan debido a que ofrece diversas opciones para llevar a cabo estos escaneos. Además, incluye una amplia gama de scripts que ayudan a obtener información más detallada sobre las redes que se están monitorizando. Esta herramienta proporciona datos sobre los servicios activos en los servidores escaneados, información sobre banners y otros detalles relevantes que pueden ser obtenidos a través de la red. También permite verificar si un dispositivo está activo y si está protegido por un firewall.

Según Por otro lado, (Bermeo, 2017) destaca que es una herramienta potente utilizada para la detección y escaneo de redes, así como para auditorías de seguridad. Permite verificar los servicios activos en un dispositivo, escanear puertos, redes, scripts y vulnerabilidades, y se emplea principalmente en auditorías de seguridad.

2.4.3. Nikto

Según (Tovar, 2020), define como una herramienta de escaneo de vulnerabilidades web de código abierto que se utiliza para detectar configuraciones inseguras y

vulnerabilidades comunes en servidores web. Esta herramienta realiza análisis exhaustivos, identificando fallos de seguridad como directorios y archivos inseguros, configuraciones erróneas, vulnerabilidades conocidas en el software, y más. Además, Nikto permite realizar escaneos en busca de vulnerabilidades específicas, como la exposición de información sensible, ataques de inyección y problemas de autenticación. La herramienta también es útil para detectar posibles vectores de ataque, como versiones antiguas de servidores o aplicaciones que pueden estar desactualizadas y, por lo tanto, ser más susceptibles a exploits conocidos.

Nikto es ampliamente utilizada por profesionales de la seguridad para realizar auditorías en servidores web y asegurarse de que estos cumplan con las mejores prácticas de seguridad.

2.4.4. Owasp zap (Zed Attack Proxy)

Según (Broad y Bindner, 2028) OWASP ZAP es una de las herramientas más populares y poderosas para realizar pruebas de seguridad en aplicaciones web. Diseñada tanto para profesionales de la seguridad como para desarrolladores, ZAP permite detectar vulnerabilidades en aplicaciones web mediante técnicas de escaneo automatizado y pruebas manuales. Es una herramienta de código abierto que proporciona una amplia gama de funcionalidades para analizar la seguridad de las aplicaciones, tales como escaneo activo, escaneo pasivo, análisis de tráfico, y análisis de posibles fallos de seguridad.

En este sentido, una de las características más destacadas de ZAP es su capacidad para interceptar y modificar solicitudes y respuestas HTTP, lo que permite realizar pruebas de penetración para identificar vulnerabilidades como inyecciones SQL, XSS, fallos de autenticación y autorización, entre otras. Además, ZAP incluye un conjunto de herramientas de automatización que pueden integrarse en los pipelines de CI/CD para realizar análisis de seguridad durante el proceso de desarrollo. Esta herramienta es ideal para detectar vulnerabilidades comunes y proporcionar soluciones prácticas para fortalecer la seguridad de las aplicaciones web.

2.4.5. Sqlmap

Según (Durand, 2019), SQLMap es un programa cuyo código fuente está disponible

públicamente. Está diseñado para automatizar y mejorar los procedimientos de detección y explotación de vulnerabilidades de inyección SQL.

2.5. Técnicas de hacking ético

Según (Rault, Schalkwijk, Agé, Acissi,y Crocfer, 2015). se ha producido un aumento de los asaltos a las distintas redes de datos de las empresas. Por esta razón, existen diversas formas para el diagnóstico de vulnerabilidades, y con el fin de evitar ataques informáticos, estas técnicas utilizan diversos enfoques. Algunas de estas tácticas son las siguientes:

a. Black-box

Según Sreenivasa y Kuman (2012), el método de caja negra es una técnica bien establecida que, además de permitir la identificación de vulnerabilidades en aplicaciones en línea, también simula un ataque al ejecutar pruebas desde la perspectiva de un atacante.

b. White-box

Según (Sreenivasa y Kuman, 2012) indican que el enfoque de caja blanca permite acceder a la información interna de la organización, lo que proporciona una visión más completa de las posibles vulnerabilidades.

c. Análisis estático de código o auditoria de código fuente

Este enfoque, según (Sreenivasa y Kuman, 2012), consiste en realizar un análisis directo del código fuente para identificar posibles fallos o vulnerabilidades de seguridad.

d. Pruebas de penetración:

Según (Jiménez, 2017) describe este método como una metodología activa diseñada para evaluar y detectar vulnerabilidades con alto potencial de explotación. Las pruebas incluyen tanto ataques locales como remotos, con el objetivo de identificar debilidades sin causar daño a la infraestructura o sistemas en línea.

e. Pruebas pasivas:

Según (Mammar, Cavalli y Jiménez, 2011), las pruebas pasivas se enfocan en el análisis de paquetes recogidos para estudiar el tráfico y detectar fallos, y generalmente se

realizan a través de Internet.

f. Pruebas activas:

(Zhang, Shao y Zheng, 2008) explican que las pruebas activas buscan investigar si los errores son evidentes o no, al intentar identificarlos en el sistema.

g. Fuzz testing (man in the middle) (pruebas de caja negra

Según (Zhang, Shao y Zhen, 2008), se ha observado que las vulnerabilidades de seguridad surgen debido a la presencia de datos aleatorios corruptos durante las pruebas de caja negra, en el contexto de ataques man in the middle.

Tabla 1

Técnicas de Hacking Ético

Técnicas	**Descripción**
Black Box	Permite detectar vulnerabilidades en aplicaciones web, basándose en un enfoque real, el del atacante.
White Box	En esta técnica, se tiene acceso al código fuente, a las credenciales válidas, a la configuración y datos técnicos del servidor.
Análisis Estático de Código	Se analiza el código fuente directamente, para poder determinar vacíos de seguridad.
Análisis Dinámico de Código	Al hacer el análisis, se comunica con la aplicación mediante front-end, para identificar debilidades de arquitectura de la aplicación.
Pruebas de Penetración	Simula ataques de delincuentes

	informáticos. Se analiza el sistema en busca de vulnerabilidades, las cuales pueden ser de configuración, falla de hardware o software, errores operativos en proceso o contramedidas técnicas.
Pruebas Pasivas	Analiza el tráfico de telecomunicaciones. Su característica es detectar fallas mediante un examen de live traffic, log files o paquetes capturados.
Pruebas Activas	Se usa en subprocesos para comprobar si las advertencias reportadas en un análisis del programa son errores reales.
Fuzz Testing o Pruebas de Caja Negra	En una prueba, al sistema usa datos aleatorios o alterados para detectar fallas en el comportamiento del sistema.

Nota. La tabla muestra las Técnicas de Hacking Etico para detectar vulnerabilidades de Información. Oswaldo Tamayo (2016).

2.6. Sistemas informáticos

Según (Tovar, 2018), se refiere al conjunto de recursos tecnológicos, que abarcan tanto el software como el hardware y los métodos informáticos, que facilitan el almacenamiento y procesamiento de información.

2.7. Seguridad informática

Según (López, 2015), la seguridad informática, también conocida como seguridad de las tecnologías de la información, consiste en proteger los recursos de estas tecnologías, como computadoras, servidores, sistemas informáticos, dispositivos móviles y electrónicos. Su propósito es permitir a los usuarios identificar y corregir fallos de seguridad en la infraestructura de red, lo que incrementa la capacidad para prevenir cualquier tipo de ataque perjudicial.

Por su parte, (García, 2015) define la seguridad de las tecnologías de la información como un conjunto de medidas tanto proactivas como reactivas en los sistemas técnicos y empresariales, destinadas a preservar y proteger la información. Esto tiene como fin garantizar la fiabilidad, integridad y disponibilidad de la misma dentro de las empresas.

Finalmente, (González, 2016) describe la seguridad de las tecnologías de la información como el proceso de proteger la disponibilidad, integridad y confidencialidad de los activos de la empresa. Además, resalta que la gestión de la seguridad debe ser realizada mediante un método documentado y sistemático, el cual debe ser reconocido en toda la organización.

2.8. Seguridad de la información y seguridad informática

Según (Tovar, 2020), la disciplina de la seguridad de la información es la encargada de garantizar que la información se mantenga confidencial, íntegra y disponible. Este objetivo solo se logra mediante la implementación de medidas de seguridad de la información, que, aunque están relacionadas con campos de estudio diferentes, son interdependientes. En este contexto, la seguridad de la información tiene la responsabilidad de establecer y regular los criterios que deben seguirse para proteger la información.

Por otro lado, Gutiérrez (2019) señala que, aunque no toda la información se encuentra en un sistema informático, sigue siendo información potencialmente sensible y susceptible de ser comprometida. En la seguridad de la información, es fundamental considerar todas las áreas en las que puedan existir riesgos de comprometer datos sensibles.

a. Seguridad física

La seguridad física se refiere a la protección de los elementos tangibles, como puertas, ventanas y otros accesos que podrían ser aprovechados por intrusos, o incluso la protección de documentos confidenciales escritos en papel. Aunque en la actualidad se presta menos atención a esta área debido a la mayor dependencia de tecnologías informáticas, sigue siendo fundamental. De nada sirve tener una computadora con antivirus y medidas contra ciberataques si un ladrón puede entrar por la ventana y robarla. Algunos ejemplos para mejorar la seguridad física incluyen la implementación de

seguridad perimetral, como cercas, bardas y puertas, así como el diseño de seguridad que favorezca la transparencia, iluminación y espacios abiertos. Además, es importante señalar que la protección de la integridad física de las personas es esencial, abarcando no solo la seguridad de bienes materiales, sino también la prevención de amenazas que puedan afectar a las personas, como terremotos o ataques terroristas. En este sentido, las medidas antropométricas, que evalúan aspectos como el peso, la longitud, la altura y el perímetro cefálico de los niños en las interacciones con los servicios sanitarios, permiten hacer un seguimiento de su crecimiento y determinar su estado nutricional, comparándolos con las normas de referencia para evaluar su desarrollo (Gutiérrez, 2019).

b. Seguridad social, o ingeniería social

Según (Gutiérrez, 2019), la clave en esta área es proteger la información que las personas poseen, ya que también es posible que información sensible sea filtrada a través de este medio. Esta forma de seguridad suele ser la más vulnerable en cualquier organización, ya que las personas son fácilmente manipulables. Para mitigar este riesgo, es esencial implementar buenas políticas de seguridad y capacitar adecuadamente al personal, asegurándose de que estén informados sobre las mejores prácticas y protocolos para proteger la información.

c. Seguridad lógica

Según (Gutiérrez, 2019), la seguridad lógica se refiere a todo lo que se encuentra dentro de un sistema, y es una de las formas más comunes de ataque en la actualidad. Estos ataques pueden dirigirse a servidores, bases de datos, computadoras o incluso teléfonos móviles. Para mitigar este tipo de amenazas, se pueden implementar soluciones de seguridad como firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS) y antivirus.

Figura 7

Triángulo de los ejes principales de la seguridad de la información.

Nota. La figura representa el triángulo de los ejes principales de la seguridad de la información (confidencialidad, integridad y disponibilidad) y cómo se interrelacionan. (Peña, 2020).

2.9. Ataques de penetración

Los ataques de penetración incluyen aquellos que permiten a un atacante no autorizado acceder a los recursos, privilegios o datos de un sistema. Una forma común de que esto ocurra es aprovechando vulnerabilidades en el software. Un ejemplo de esto ocurrió en julio de 2002, cuando se descubrió un exploit en el código de manejo de respuestas del desafío SSH (Secure Shell), que permitía a un atacante ejecutar código arbitrario como el usuario que ejecuta SSH, normalmente root. Este tipo de ataque se considera un ataque de penetración. Tener la capacidad de ejecutar código arbitrario como root otorga al atacante acceso completo a los recursos del sistema, lo que además podría habilitar otros ataques dentro del sistema comprometido o a otros sistemas conectados. (Chakrabarti, Chakraborty y Mukhopadhyay, 2010).

2.10. Open source

El código abierto es una forma de licenciamiento de software que permite su distribución libre y acceso al código fuente. Esto implica que los usuarios pueden realizar copias, compartirlas con otras personas e incluso obtener y modificar el código fuente. El propósito del código abierto es fomentar que los usuarios examinen y, si es posible, mejoren el código. Se cree que, mediante la revisión y mejora continua por parte de múltiples personas, un producto alcanzará un nivel de calidad superior más rápidamente que los productos comerciales (Damiani, 2016).

De acuerdo con OPENBIZ (2009), la Open Source Initiative establece criterios para determinar si una licencia de software puede considerarse de código abierto. Esta definición fue creada por Bruce Perens y se basa en las Directrices de Código Abierto de Debian. Para ser consideradas como licencias de software abierto, estas deben cumplir con diez características que, aunque similares, no son idénticas a los requisitos de las licencias de software libre.

2.11. Virtualbox

Según (Gillet, 2010), VirtualBox es una herramienta de virtualización de software que permite emular sistemas operativos completos dentro de un entorno virtual. Al igual que otras soluciones de virtualización, VirtualBox crea máquinas virtuales que simulan las características de hardware de un ordenador físico, proporcionando una experiencia similar a la de un sistema real. Esta herramienta permite ejecutar aplicaciones y sistemas operativos dentro de máquinas virtuales, lo que facilita la prueba de configuraciones, el análisis de seguridad y la realización de tareas de administración de redes sin afectar a un sistema físico. Entre los componentes que se simulan se incluyen la unidad central de procesamiento (CPU), la memoria RAM, el disco duro, la tarjeta gráfica, la tarjeta de red, y otros dispositivos esenciales, permitiendo que el usuario ejecute un sistema operativo completo dentro de su máquina host.

2.12. Seguridad corporativa

La seguridad corporativa puede definirse en una sola palabra: consolidación. Se entiende como el conjunto de políticas, procedimientos y recursos humanos, organizativos y técnicos destinados a proteger a las personas, los activos tangibles e

intangibles, así como la reputación de una organización. Aunque no existe una definición única debido a la flexibilidad del modelo, se considera un conjunto integral. Otra definición de seguridad corporativa describe esta función como aquella que identifica, gestiona y mitiga de manera efectiva, desde una etapa temprana, cualquier situación que pueda poner en riesgo la resiliencia y la capacidad de supervivencia de la organización. Esta función se encuadra dentro de lo que se conoce como seguridad corporativa (Muñoz, 2016).

Según Sarra (sf), la seguridad debe estar presente en todas las operaciones de la empresa, y en cada área debe ser aplicada según el riesgo y las necesidades específicas de cada una. Es decir, la seguridad debe integrarse en todos los procesos empresariales. Para reducir las pérdidas de cualquier tipo, la seguridad debe estar presente en todos los aspectos operativos de la empresa. Este enfoque es el único método para maximizar la rentabilidad de la organización, a la vez que reduce los riesgos y asegura su continuidad.

2.13. Población

Según (Chávez, 2007), la población es el universo de estudio de una investigación, sobre el cual se pretende generalizar los resultados. Está constituida por características o estratos que permiten distinguir los sujetos unos de otros.

Por su parte, (Tamayo y Tamayo, 2019) definen la población como la totalidad del fenómeno objeto de investigación. Las unidades que la conforman comparten una cualidad que es el foco de la investigación y proporciona la base de los datos para el análisis.

Por otro lado, (Fernández y Baptista, 2014) explica que una población se define como el conjunto de todos los casos que cumplen un determinado conjunto de criterios establecidos para el estudio.

2.14. Muestra

Según (Hernández Sampieri et al., 2014), "No siempre, pero en la mayoría de las situaciones sí realizamos el estudio en una muestra. Sólo cuando queremos efectuar un censo debemos incluir todos los casos (personas, animales, plantas, objetos) del universo o la población".

Esto significa que, en la mayoría de los estudios, se selecciona una muestra representativa de la población para realizar el análisis, ya que es más práctico y económico. Solo en el caso de un censo, se estudian todos los elementos de la población sin necesidad de seleccionar una muestra.

Capítulo III

Metodología de la investigación

3.1. Tipo y nivel de investigación

3.1.1. Tipo de investigación

Según (Murillo, 2008), la investigación aplicada, también conocida como "investigación práctica o empírica", se caracteriza por su enfoque en la aplicación y utilización de los conocimientos adquiridos. A través de este tipo de investigación, se busca implementar y sistematizar la práctica basada en la investigación, con el objetivo de generar nuevos conocimientos y resultados. El proceso de investigación aplicada implica una forma rigurosa, organizada y sistemática de conocer la realidad, a la vez que permite la adquisición de nuevos aprendizajes que pueden ser utilizados de manera práctica para resolver problemas específicos o mejorar una situación particular. Por esta consideración el tipo de investigación es aplicada.

3.2. Nivel de investigación

Según (Hernández Sampieri et al., 2010), la investigación descriptiva tiene como objetivo especificar las propiedades, características y perfiles relevantes de personas, grupos, comunidades u otros fenómenos sujetos a análisis. Esta modalidad de investigación se enfoca en seleccionar las características fundamentales del objeto de estudio y en describir detalladamente sus partes, categorías o clases. De acuerdo con los autores, la investigación descriptiva es una de las más comunes entre los principiantes en investigación, y es utilizada frecuentemente en trabajos de grado y en programas de pregrado y maestría. En estos estudios, se describen hechos, situaciones, rasgos característicos de un objeto de estudio, o se diseñan productos, modelos, prototipos, guías, entre otros (p.112).

Por otro lado, (Carrasco, 2006) menciona que la investigación descriptiva se apoya principalmente en técnicas como la encuesta, la entrevista, la observación y la revisión documental. Este tipo de investigación se dedica a estudiar, analizar y especificar situaciones y propiedades de personas, grupos, comunidades o cualquier otro fenómeno u objeto que esté bajo análisis. Por esta consideración el nivel de investigación es descriptivo.

3.3. Diseño de la investigación

Según (Hernández Sampieri et al., 2010), la investigación no experimental se define como aquella investigación que se realiza sin manipular deliberadamente las variables. Es decir, en estos estudios no se altera intencionalmente las variables independientes para observar su efecto sobre otras variables. Este tipo de investigación se utiliza cuando no se busca modificar ni controlar las condiciones del fenómeno estudiado, sino simplemente observar y describir las variables tal como se presentan en su contexto natural (p.191).

Por otro lado, (Carrasco, 2018) señala que el diseño de investigación transversal descriptivo se emplea para analizar y conocer las características, cualidades internas y externas, propiedades y rasgos esenciales de hechos y fenómenos en un momento específico del tiempo. Este enfoque permite obtener una visión detallada y comprensible de los fenómenos en el tiempo exacto en que ocurren, sin intervenir o manipular el contexto de la investigación.

En esta investigación, fue necesario analizar procesos, identificar características, estudiar rasgos y comprender funcionalidades para obtener los datos esenciales en el análisis de vulnerabilidades. Por ello, el diseño de investigación adoptado es no experimental, de tipo transversal y descriptivo.

3.4. Hipótesis de la investigación

Según (Hernández, Baptista y Collado, 2014) en el contexto de las investigaciones cuantitativas, mencionan que no siempre se planean hipótesis, y la decisión de formularlas depende del alcance inicial del estudio. En investigaciones cuantitativas con un enfoque correlacional o explicativo, es común formular hipótesis, ya que el estudio busca establecer relaciones entre variables. Sin embargo, incluso en investigaciones de tipo descriptivo, cuando el objetivo es pronosticar alguna cifra o hecho, también se puede formular una hipótesis (p. 104).

Por otro lado, (Berna, 2010) señala que las investigaciones descriptivas no requieren la formulación de hipótesis. En este tipo de investigaciones, lo que se necesita son preguntas de investigación, que surgen del planteamiento del problema, los objetivos del estudio y el marco teórico que lo sustenta. Así, las investigaciones descriptivas se enfocan en

observar y detallar las características de los fenómenos sin necesidad de establecer hipótesis previas (p. 136).

La investigación que se desarrollara es de tipo descriptivo, por lo que no se pretende pronosticar hallar o verificar lo planteado en los objetivos, se optó por no plantear hipótesis.

3.5. Población y muestra

3.5.1. Población

La población estuvo compuesta por los sistemas informáticos:

- 1 Red Mikrotik.
- 5 Router.
- 6 Switch.
- 1 Servidor de la página web de la Municipalidad.
- 140 computadoras personales.
- 15 laptops.

3.5.2. Muestra

Se utilizó el Muestreo no probabilístico, muestreo por juicio de experto.
La muestra incluyó a todos los elementos de la población objetivo.

- 5 computadoras personales:
    - 2 computadoras de la Oficina de Gestión de Recursos Humanos
    - 2 computadoras de Gerencia de Recaudación y Administración Tributaria
    - 1 computadoras de la Oficina TIC.
- 3 laptops:
    - 1 laptop de Gerencia Municipal
    - 2 laptops de Oficina General de Planeamiento y Presupuesto.
- 1 servidor de la página web.
- 1 red administrada con un dispositivo MikroTik.

3.6. Definición conceptual de las variables

3.6.1. Variable de interés

Análisis de vulnerabilidades. El análisis de vulnerabilidades, según McNab (2004), es un procedimiento estructurado que tiene como objetivo identificar y evaluar las debilidades presentes en un sistema informático, para así determinar su grado de vulnerabilidad ante posibles amenazas. Este proceso es fundamental para fortalecer la seguridad del sistema y prevenir posibles intrusiones o ataques.

Variables descriptivas

A. **Recopilación de la información.** Este proceso consiste en reunir y evaluar datos relevantes sobre las diversas vulnerabilidades y amenazas que podrían afectar la seguridad de la información dentro de una organización.
B. **Identificación y análisis de vulnerabilidades.** Este paso implica la revisión de sistemas y redes informáticas para detectar posibles vulnerabilidades, seguido de un análisis sobre cómo estas debilidades podrían impactar la seguridad de la información.
C. **Medidas de seguridad informática.** Se refiere al conjunto de estrategias, herramientas y procedimientos diseñados para proteger la información almacenada o procesada en sistemas informáticos, previniendo el acceso no autorizado, su alteración o destrucción.

3.7.Definición operacional de las variables

Variable de interés

Análisis de vulnerabilidades.

Variables descriptivas

- **A.** Recopilación de la información
- **B.** Identificación y análisis de vulnerabilidades
- **C.** Medidas de seguridad informática

3.8. Técnicas e instrumentos de recolección de datos

A. Técnicas

Revisión documental automatizada

B. Instrumentos

Sistema Operativo Kali Linux

- Nmap
- Owasp zap
- Nikto
- SQLMap
- Shodan

Capítulo IV
Resultados y discusión

4.1.Fase I: Planificación

Esta fase representa el punto de inicio clave para llevar a cabo una evaluación estructurada de la seguridad informática, siguiendo los lineamientos de la metodología NIST SP 800-115. Esta metodología ofrece un marco estandarizado y detallado para realizar pruebas de penetración (Pentesting) en entornos organizacionales, asegurando una evaluación exhaustiva y controlada de las vulnerabilidades de los sistemas.

4.1.1. Definición del alcance.

El alcance del proyecto abarca un análisis exhaustivo de los equipos informáticos y la infraestructura de red de la Municipalidad Distrital de San Juan Bautista. Esto incluye la evaluación de computadoras personales, laptops y redes gestionadas con tecnología MikroTik, con el objetivo de identificar vulnerabilidades y proponer medidas correctivas que fortalezcan la seguridad de los sistemas y protejan la infraestructura tecnológica de la municipalidad.

A. Equipos informáticos.

La municipalidad cuenta con diversos recursos informáticos, de los cuales se seleccionaron los siguientes para esta investigación:

- 5 computadoras personales.
- 3 laptops.
- 1 servidor de la página web de la Municipalidad.
- 1 red administrada con un dispositivo MikroTik.

B. Página web de la Municipalidad Distrital de San Juan Bautista

La municipalidad cuenta con una página web activa, actualmente alojada en un servidor basado en Joomla. Este recurso requiere mantenimiento y posibles actualizaciones para garantizar su seguridad y funcionalidad.

4.1.2. Preparación del entorno

Para llevar a cabo el análisis de vulnerabilidades y las pruebas de seguridad, se

configura un entorno controlado utilizando VirtualBox, donde se implementa Kali Linux, un sistema operativo especializado en ciberseguridad. Dentro de este entorno, se emplean diversas herramientas para evaluar la seguridad de los sistemas, tales como Nmap para el escaneo de redes y la detección de servicios activos, Owasp Zap para realizar pruebas de seguridad en aplicaciones web, Nikto para identificar fallos en servidores web, SQLMap para detectar y explotar vulnerabilidades en bases de datos mediante inyecciones SQL, y Shodan como motor de búsqueda para el reconocimiento y análisis de dispositivos y servicios expuestos en Internet.

4.2.Fase II Descubrimiento

4.2.1. Reconocimiento pasivo

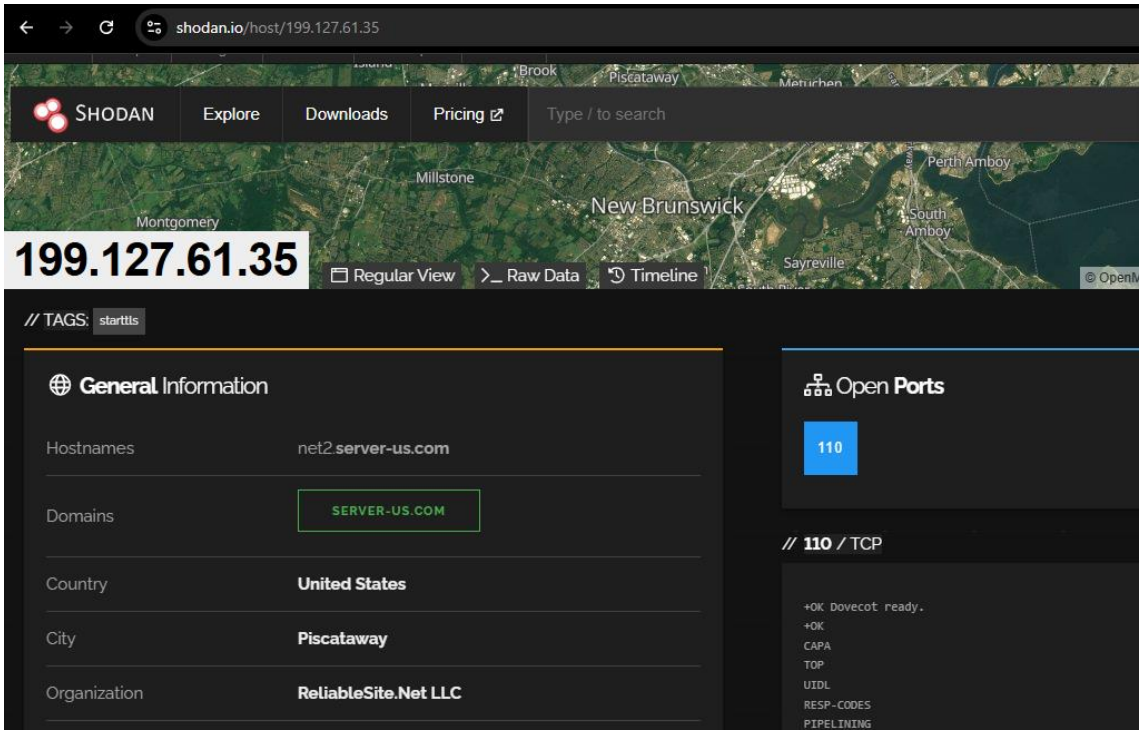
En esta fase, se emplean herramientas y recursos disponibles públicamente para recolectar datos relevantes. El objetivo principal es identificar posibles vectores de ataque y obtener una visión general del entorno de la Municipalidad Distrital San Juan Bautista.

4.2.1.1. Reconocimiento Pasivo Utilizando Shodan en la Página Web de la Municipalidad

A continuación, se muestra una captura de pantalla del servicio Shodan, utilizado para realizar un reconocimiento pasivo de la Página Web de la Municipalidad Distrital San Juan Bautista. En la figura, se puede observar la consulta de la dirección IP 199.127.61.35, donde se detallan los puertos abiertos, en este caso, el puerto 110/TCP correspondiente al servicio POP3. Este tipo de análisis ayuda a identificar posibles vulnerabilidades o servicios expuestos en la red sin necesidad de interactuar directamente con el sistema objetivo.

Figura 8

Imagen de la consulta de Shodan.



Nota. En la figura de muestra la consulta al Ip de la red de la Municipalidad de San Juan Bautista.

a. **Revisión del servicio activo en el puerto 110 (POP3):**

- El puerto 110, utilizado para el protocolo POP3 (Post Office Protocol v3), indica que el sistema puede estar configurado para recibir correos electrónicos.
- La respuesta recibida (+OK Dovecot ready) confirma que el servicio POP3 está siendo gestionado por Dovecot, un servidor de correo ampliamente utilizado.

b. Características del servidor identificado:

- Soporta autenticación mediante los métodos SASL PLAIN y LOGIN.
- Proporciona opciones de seguridad como STLS (StartTLS), lo que indica la posibilidad de establecer conexiones seguras.

c. Información del certificado SSL:

El sistema cuenta con un certificado digital emitido por Let's Encrypt, una autoridad de certificación reconocida.

d. Detalles relevantes del certificado:

- Dominio asociado: net2.server-us.com.
- Validez:
- Fecha de inicio: 4 de diciembre de 2023.
- Fecha de expiración: 4 de marzo de 2024.
- Soporte para autenticación TLS para cliente y servidor.
- El certificado incluye un SAN (Subject Alternative Name) que amplía la compatibilidad con nombres adicionales.

4.2.1.2. BuiltWith para Analizar Pgina Web de la municipalidad

La consulta realizada a la página web de la Municipalidad de San Juan Bautista utilizando la herramienta BuiltWith. En la imagen se muestran detalles sobre la tecnología utilizada en el sitio web, como los servicios de Facebook Domain Insights para el análisis y seguimiento de tráfico en línea, así como información adicional relacionada con el perfil tecnológico de la página. Esta consulta permite obtener una visión general sobre los recursos y herramientas utilizadas en el desarrollo de la página web de la municipalidad.

A. Gestión de Contenidos

Joomla Sistema de gestión de contenidos (CMS) utilizado para estructurar y administrar el contenido del sitio. Es una herramienta de código abierto que permite personalización y flexibilidad en el desarrollo web.

B. Librerías y Frameworks:

- PHP: Lenguaje de programación ampliamente utilizado para el desarrollo web dinámico, integrado en el contenido HTML.
- jQuery Librería de JavaScript que facilita la manipulación del DOM, animaciones y la integración de interacciones dinámicas en la web.
- jQuery UI y jQuery Parallax: Extensiones de jQuery para implementar efectos de animación avanzados y fondos dinámicos en las páginas.

C. Tipografía y diseño visual:

Google Font API: Herramienta que permite integrar tipografías personalizadas en el

diseño web.

Font Awesome: Kit de iconos y tipografía para enriquecer la estética visual del sitio.

D. Compatibilidad y optimización móvil:

Meta Viewport: Configuración para asegurar que el contenido se adapte adecuadamente a dispositivos móviles.

Apple Mobile Web App Capable: Habilitación de características para que el sitio se comporte como una aplicación nativa en dispositivos iOS.

E. Idiomas:

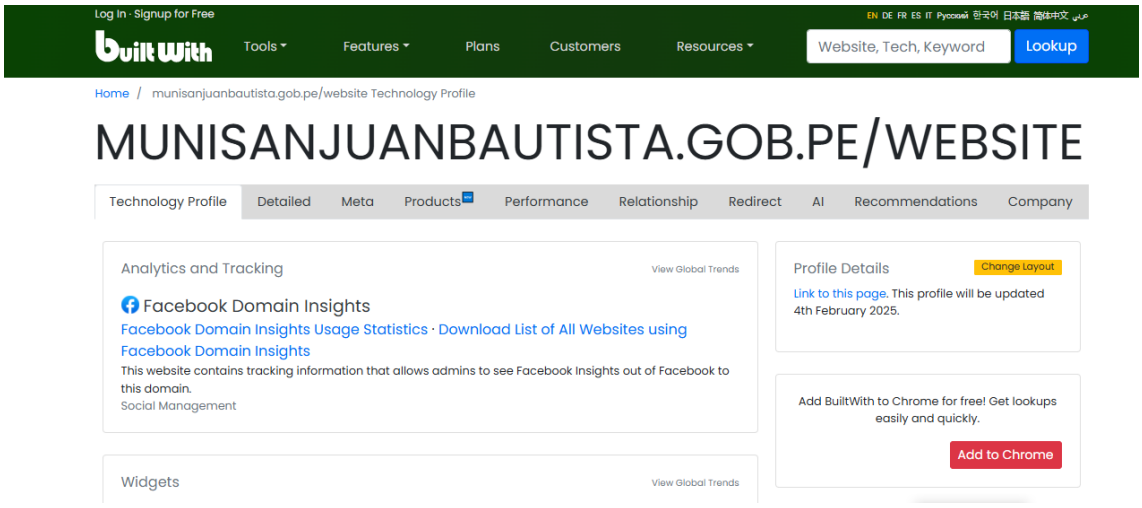
Contenido principalmente en español, identificado mediante los atributos de lenguaje en el código HTML.

F. Análisis y gestión social:

Facebook Domain Insights: Herramienta de análisis que permite obtener métricas sobre el comportamiento de los usuarios provenientes de Facebook.

Figura 9

Consulta de página web san juan bautista.



Nota. En la imagen se ilustra la consulta de página web de san juan bautista con Built With.

4.2.1.3. Google dork

Identificación de páginas indexadas mediante Google dorks es una etapa esencial para mejorar la seguridad y evitar que información crítica sea accesible para atacantes malintencionados. Este tipo de escaneo ayuda a detectar errores de configuración en la página web y sistemas de la municipalidad

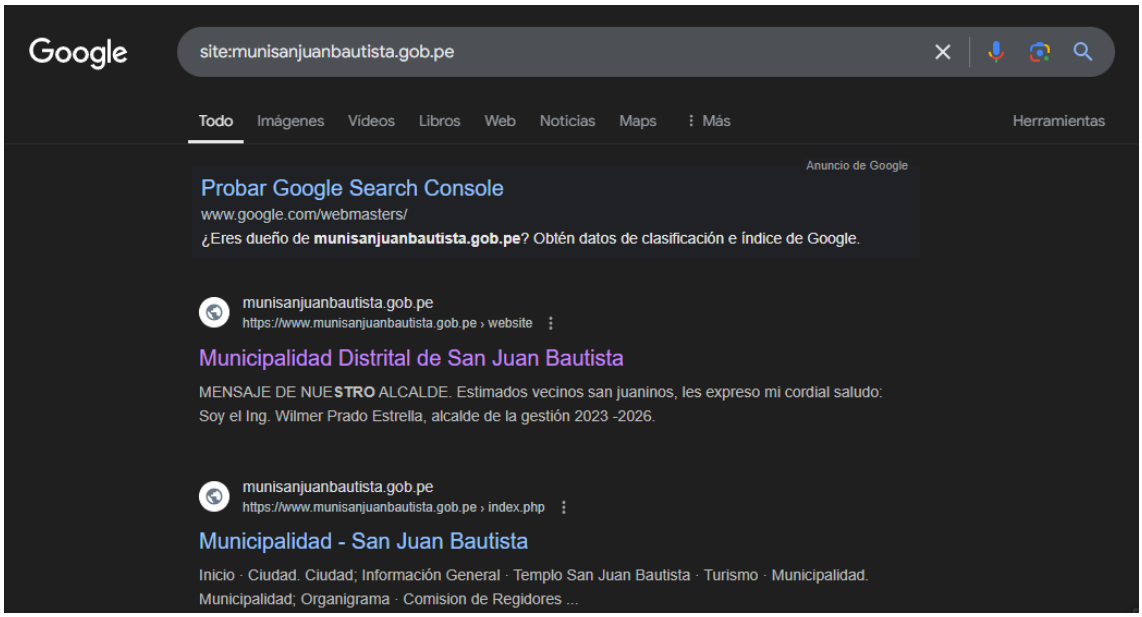
A. Identificación de Páginas y Archivos Sensibles de la Página Web de la Municipalidad

A.1. Buscar páginas indexadas

El sitio web oficial de la Municipalidad Distrital de San Juan Bautista (https://www.munisanjuanbautista.gob.pe/website/) es una plataforma digital diseñada para ofrecer información y servicios a los ciudadanos de este distrito. Está estructurada para cumplir con las necesidades informativas de la comunidad y facilitar el acceso a recursos municipales. A continuación, se resumen los aspectos principales:

Figura 10

Páginas indexadas por Google.



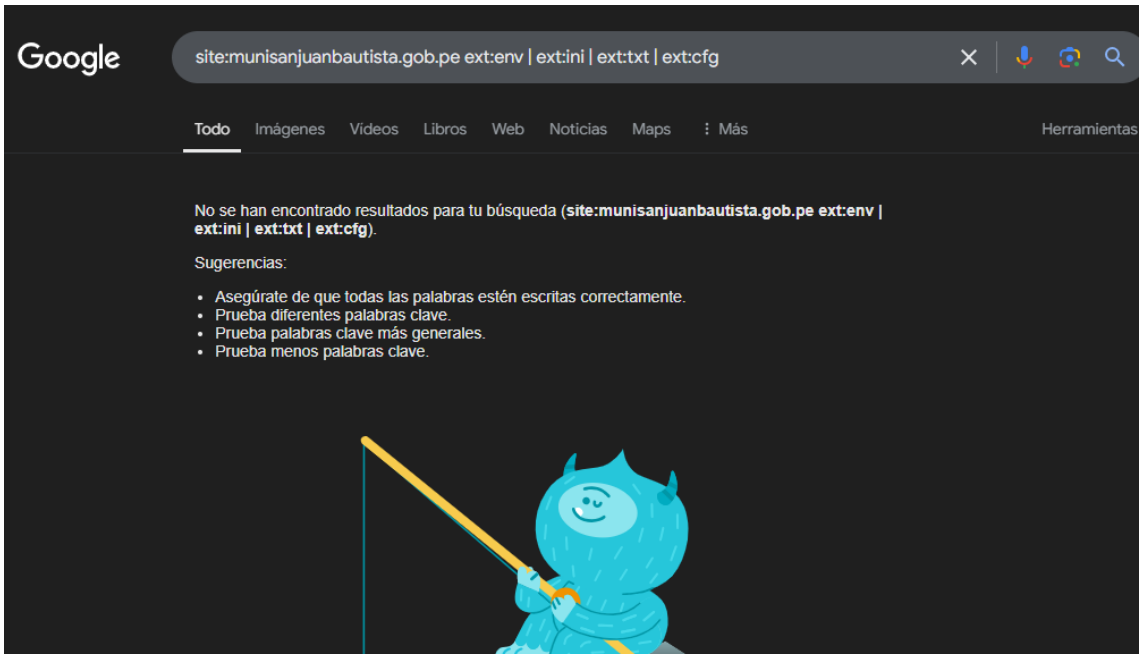
Nota. En la figura se muestra todas las páginas indexadas por Google.

A.2. Archivos de configuración comunes

En la figura se muestra una búsqueda realizada en Google para identificar archivos sensibles en la página web de la Municipalidad de San Juan Bautista. La consulta está orientada a encontrar archivos comunes de configuración, como .env, config.ini, entre otros, que podrían contener información confidencial. Sin embargo, en este caso, la búsqueda no arrojó resultados, lo que sugiere que no se han encontrado tales archivos expuestos públicamente en el sitio.

Figura 11

Busca archivos sensibles como .env, config.ini, etc.



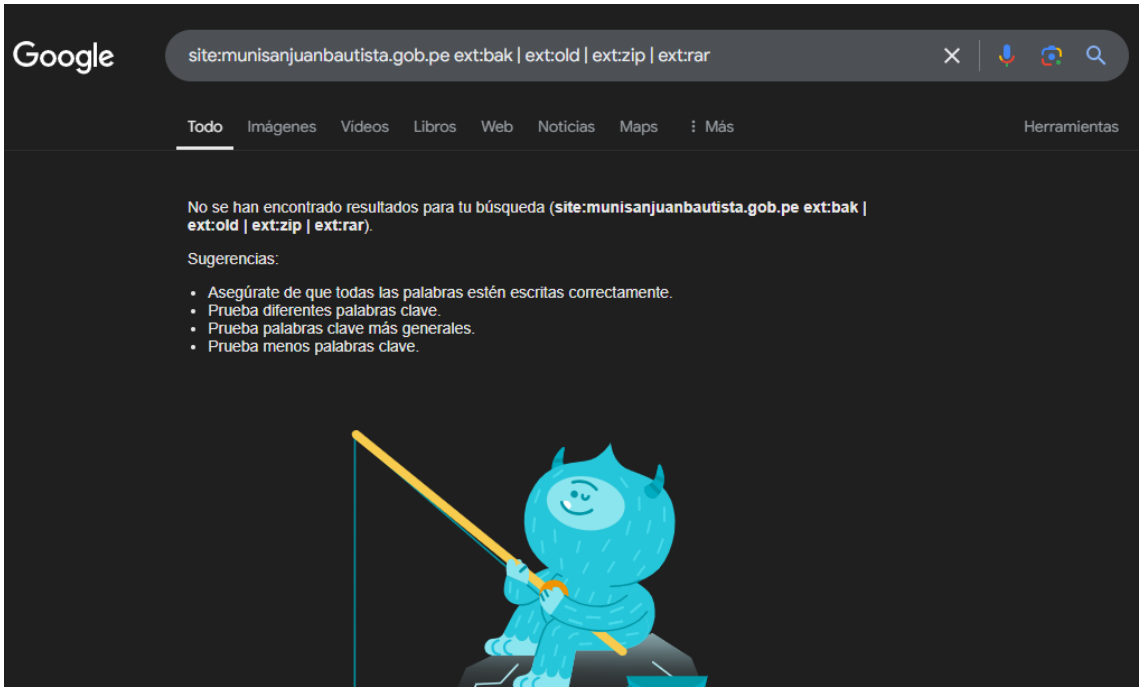
Nota. En la búsqueda no se encontraron ningún resultado.

A.3. Archivos de respaldo o copias de seguridad

En la figura se muestra una búsqueda en Google destinada a detectar archivos de respaldo o copias de seguridad expuestas de la página web de la Municipalidad de San Juan Bautista. La consulta está dirigida a identificar archivos de tipo .bak, .tar.gz, .zip, entre otros, que podrían contener información crítica o sensible. Sin embargo, la búsqueda no muestra ningún resultado, lo que sugiere que estos archivos no están accesibles públicamente en el sitio web.

Figura 12

Detecta archivos de respaldo que puedan haberse dejado accesibles.



Nota. En la figura no se muestra ningún resultado

Esto detecta archivos de respaldo que puedan haberse dejado accesibles.

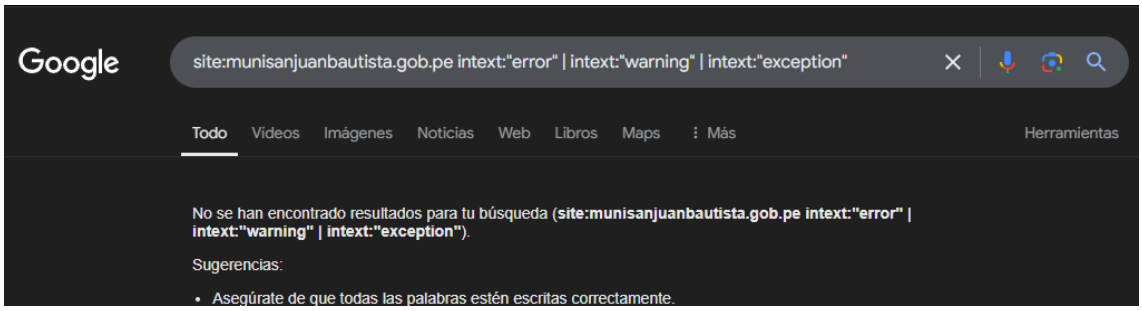
B. Verificación de vulnerabilidades potenciales

B.1. Errores expuestos:

En la figura se muestra una búsqueda realizada en Google para identificar posibles errores expuestos en la página web de la Municipalidad de San Juan Bautista. La consulta está orientada a encontrar mensajes de error comunes como "error", "warning", y "exception", los cuales podrían dar pistas sobre la infraestructura o el entorno del servidor. Sin embargo, en esta búsqueda no se obtuvo ningún resultado, lo que sugiere que no se encontraron errores visibles públicamente en el sitio web.

Figura 13

Identifica errores que puedan dar pistas sobre el entorno o infraestructura.



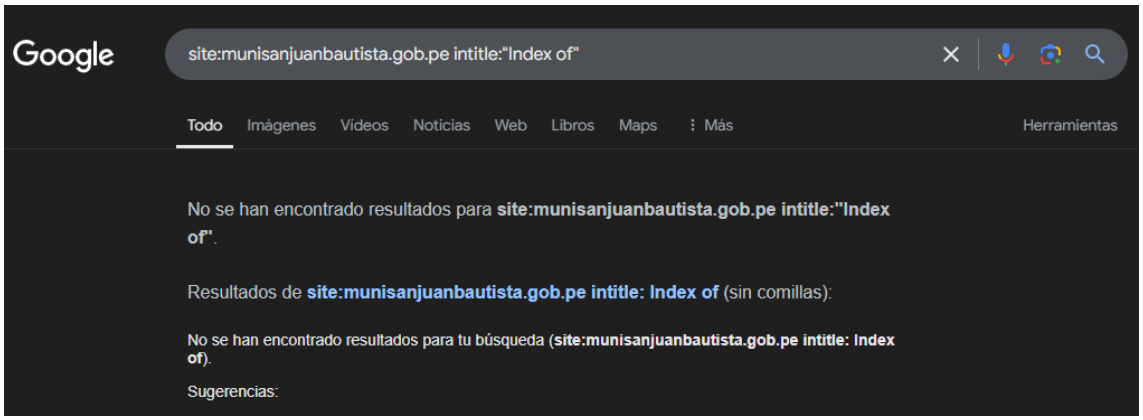
Nota. En la figura no se encuentra ningún resultado.

B.2. Directorios abiertos

A continuación, se muestra una búsqueda realizada en Google para detectar posibles directorios abiertos en la página web de la Municipalidad de San Juan Bautista. La consulta está dirigida a encontrar directorios sin protección utilizando la sintaxis "Index of", que a menudo revela listas de archivos o carpetas disponibles públicamente. En este caso, no se encontraron resultados, lo que sugiere que no hay directorios abiertos accesibles desde el sitio web.

Figura 14

Busca directorios sin protección.



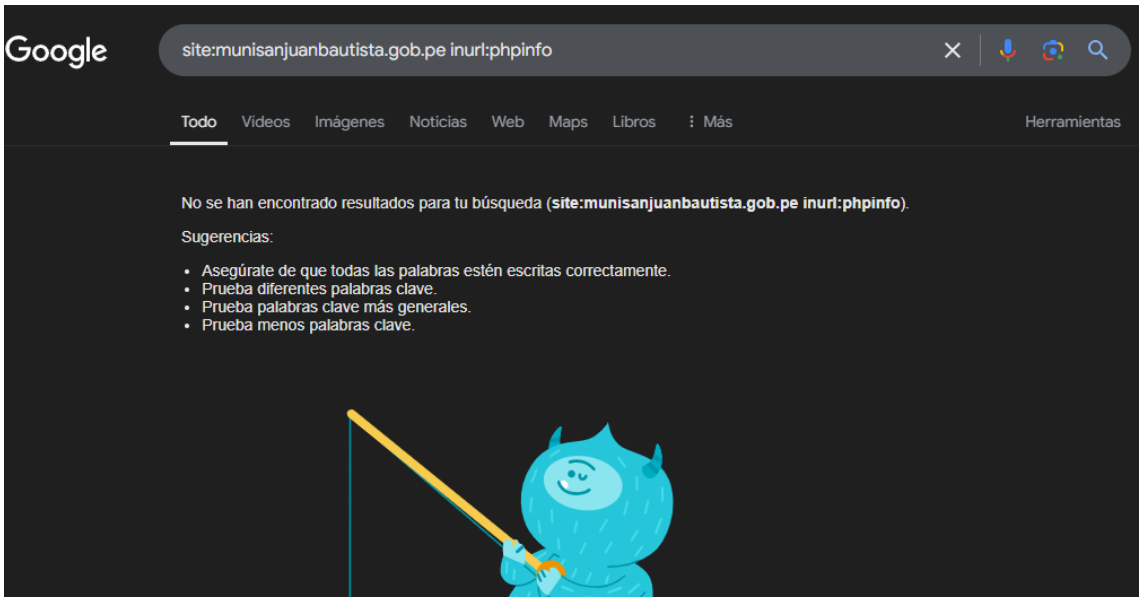
Nota. En la figura se muestra ningún resultado.

C. Análisis de tecnologías

La imagen muestra una búsqueda en Google para identificar páginas que puedan contener información sobre el sistema utilizado por la Municipalidad de San Juan Bautista. La consulta se centra en encontrar páginas con datos del tipo /inputinfo. En este caso, no se obtuvieron resultados, lo que indica que no se encontraron páginas accesibles públicamente que revelen detalles sobre el sistema utilizado por la entidad.

Figura 15

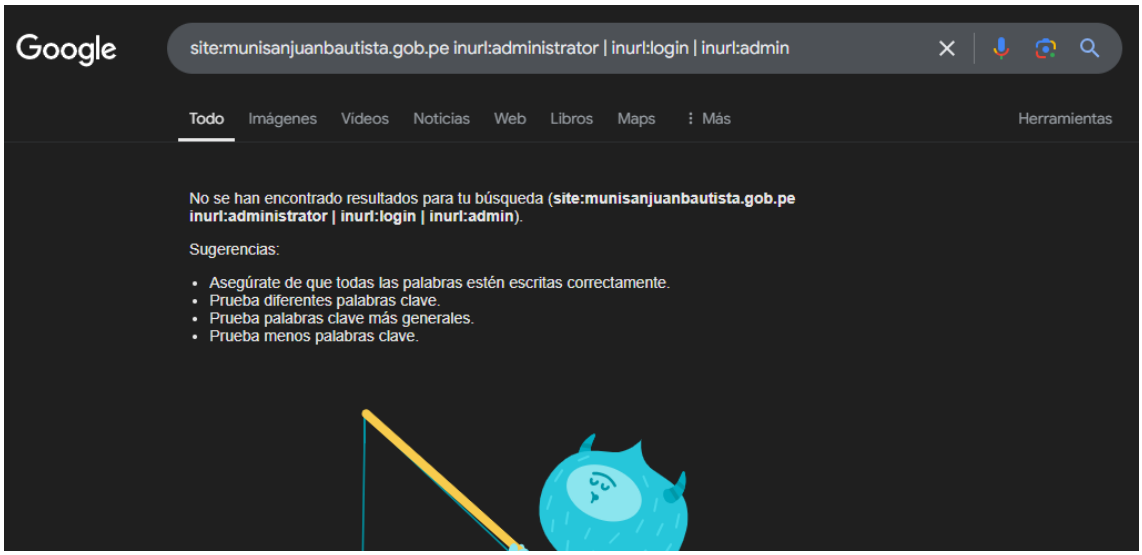
Identificar páginas con información del sistema.



Nota. En la figura no se muestra ningún resultado.

Figura 16

Identificar sistemas de administración de contenido.



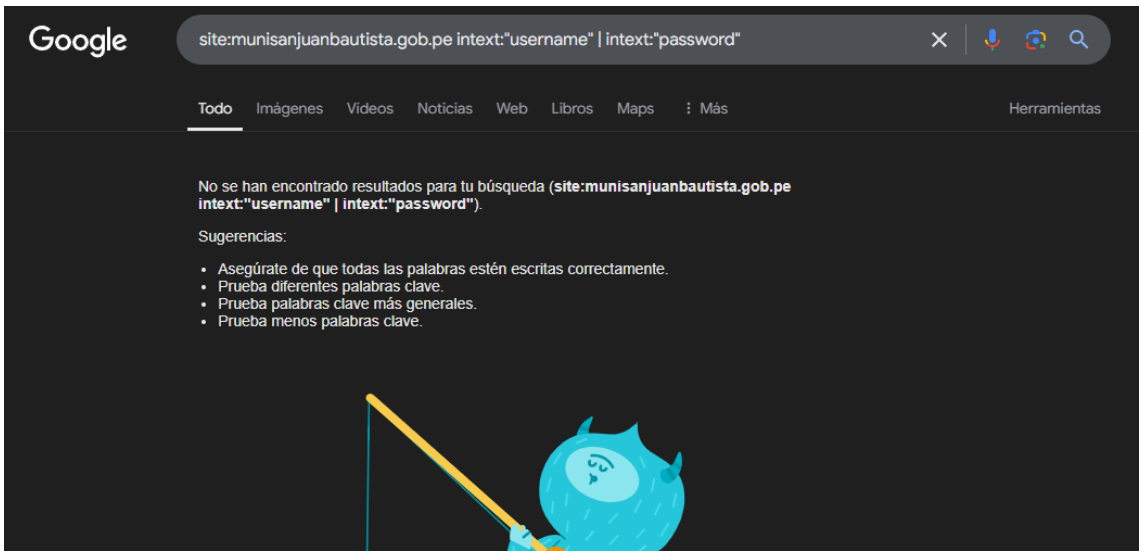
Nota. En la figura no se muestra ningún resultado.

D. Información sobre usuarios y seguridad

En la imagen se presenta una búsqueda realizada en Google para identificar posibles usuarios o credenciales expuestas en la página web de la Municipalidad de San Juan Bautista. La consulta está orientada a encontrar patrones comunes en la URL que contengan términos como "username" o "password", que podrían indicar que información sensible ha sido expuesta públicamente. Sin embargo, no se encontraron resultados, lo que sugiere que no hay credenciales accesibles públicamente en el sitio web.

Figura 17

Buscar usuarios o credenciales expuestos.

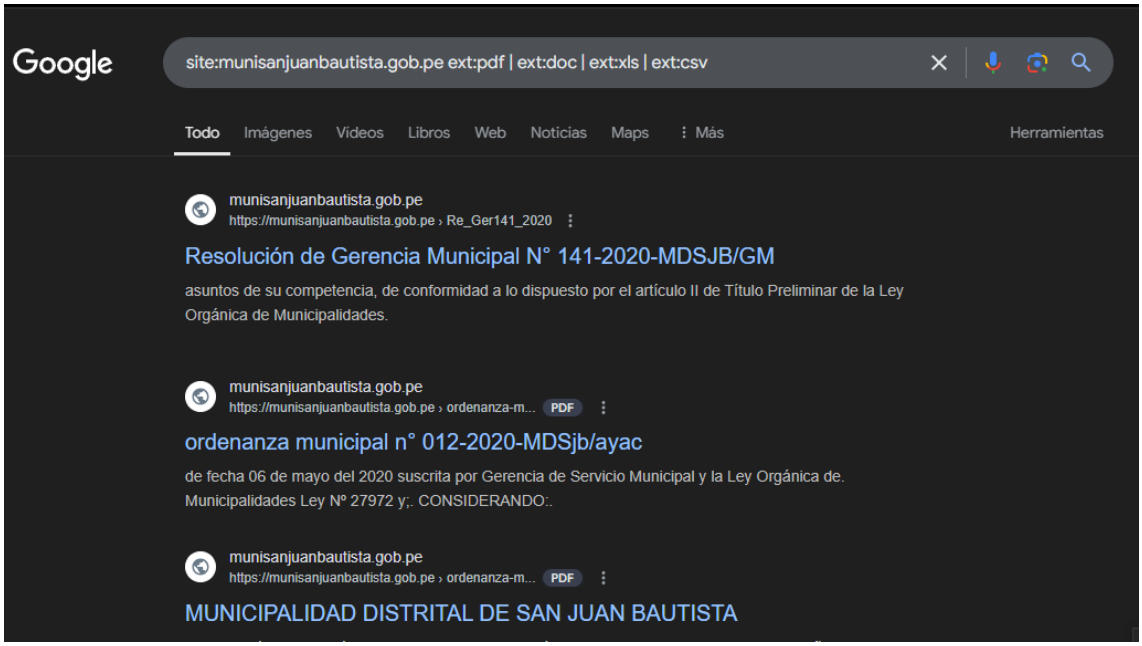


Nota. En la figura no muestra ningún resultado.

La imagen muestra una búsqueda en Google para identificar posibles documentos confidenciales expuestos en la página web de la Municipalidad de San Juan Bautista. La consulta está dirigida a encontrar archivos PDF con términos como "extracto" o "extractos", que podrían incluir documentos sensibles. En este caso, se muestra un resultado relacionado con una Resolución de Gerencia Municipal, pero la búsqueda no arroja más resultados, lo que sugiere que no se encontraron más documentos confidenciales accesibles públicamente en el sitio.

Figura 18

Buscar documentos confidenciales.



Nota. En la figura no muestra ningún resultado.

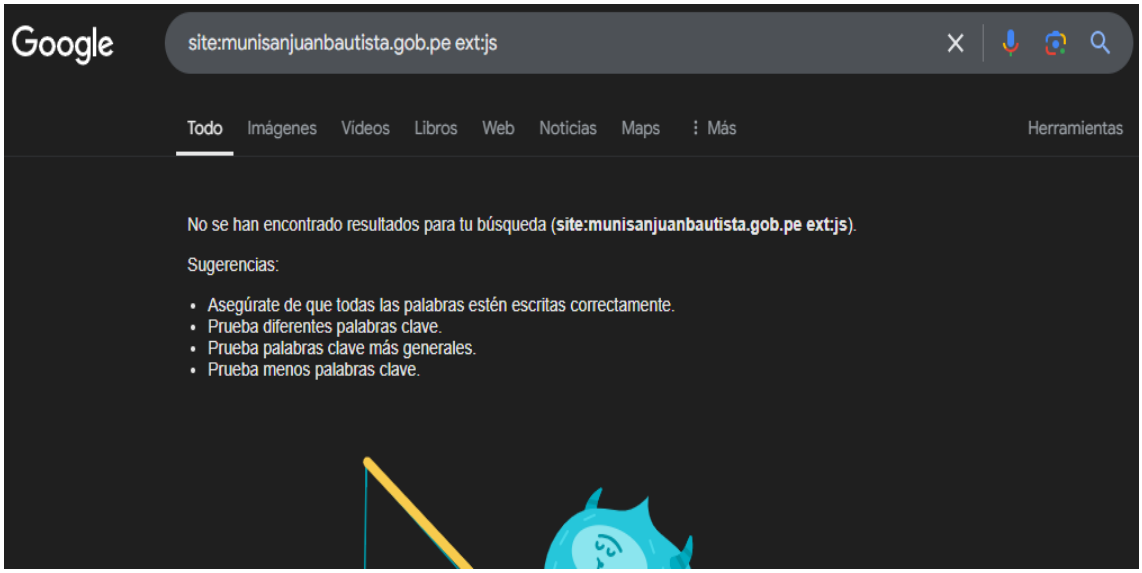
E. Exploración de recursos específicos

La imagen presenta una búsqueda en Google dirigida a identificar posibles archivos JavaScript públicos en la página web de la Municipalidad de San Juan Bautista. La consulta busca encontrar archivos .js expuestos que puedan contener información relevante sobre la estructura o funcionalidades del sitio web. Sin embargo, no se

encontraron resultados, lo que indica que no hay archivos JavaScript accesibles públicamente en el sitio.

Figura 19

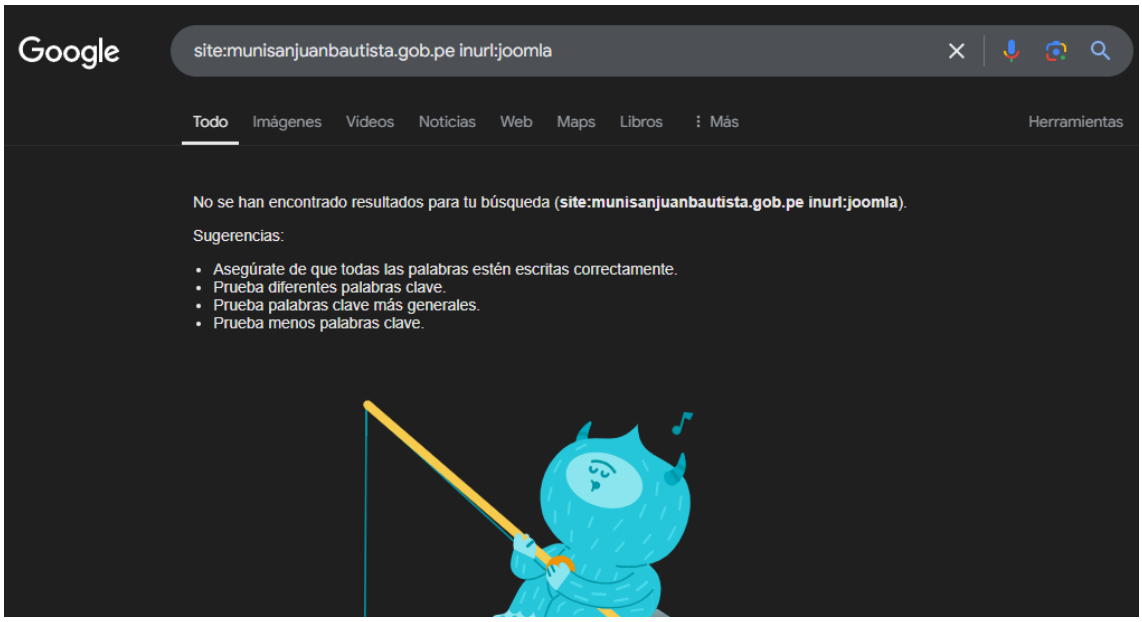
Archivos JavaScript públicos.



Nota. En la figura no se muestra ningún resultado.

Figura 20

Buscar configuraciones específicas de Joomla.



N*ota.* En la figura no se muestra ningún resultado.

4.2.2. Reconocimiento activo

En esta fase, se lleva a cabo una interacción directa con los sistemas y redes de la municipalidad con el fin de recopilar información crucial sobre sus recursos y estructuras tecnológicas. Para ello, se utilizan herramientas como Nmap y nslookup, que permiten realizar un escaneo exhaustivo de los servicios y puertos abiertos en la infraestructura de la municipalidad. Este proceso ayuda a identificar vulnerabilidades potenciales, configuraciones erróneas o puntos débiles en la seguridad, lo que podría ser aprovechado por atacantes.

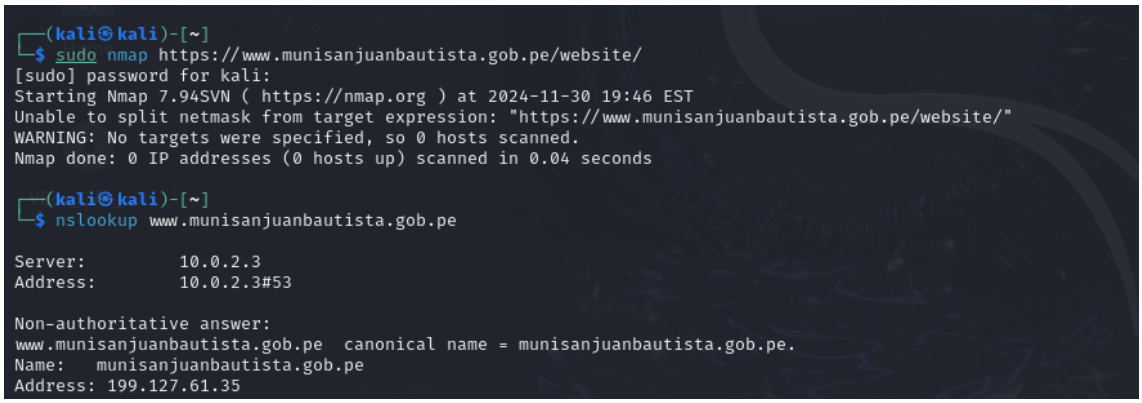
4.2.2.1. Análisis con Nmap

Se realizó un análisis preliminar del dominio www.munisanjuanbautista.gob.pe/website/ utilizando herramientas de reconocimiento como Nmap y nslookup. Nmap no pudo procesar la URL debido a un formato incorrecto, destacando la necesidad de usar direcciones IP o nombres de dominio sin el protocolo. Por otro lado, nslookup permitió resolver el dominio, obteniendo la dirección IP asociada: 199.127.61.35. Este proceso evidencia la importancia de herramientas de reconocimiento para identificar recursos en sistemas web.

La imagen muestra un análisis realizado en la página web de la Municipalidad de San Juan Bautista utilizando las herramientas Nmap y Nlookup. El comando ejecutado con Nmap revela información sobre el servidor y la dirección IP asociada al dominio munisansanjuanbautista.gob.pe. Se muestra que la dirección IP del servidor es 10.0.2.3 y el servidor es 10.0.2.2. Además, se observa que Nmap no detectó puertos abiertos durante el escaneo. Este tipo de análisis proporciona detalles sobre la infraestructura y configuración del sitio web.

Figura 21

Análisis de página web de la municipalidad de san juan bautista.



Nota. En la imagen se muestra el resultado de Nmap y Nslookup.

A. Análisis de Vulnerabilidad de Dirección IP con Nmap en la Página Web de la Municipalidad

Se realizó un análisis de puertos utilizando Nmap sobre la dirección IP 199.127.61.35, correspondiente al dominio net2.server-us.com. Los resultados obtenidos indican que el host está activo con una latencia de 0.0042s. De un total de 1000 puertos analizados, se

observaron 967 puertos filtrados y los siguientes servicios en los puertos abiertos o cerrados.

Puertos abiertos

- 21/tcp: FTP
- 53/tcp: DNS (Domain)
- 80/tcp: HTTP
- 110/tcp: POP3
- 143/tcp: IMAP
- 443/tcp: HTTPS
- 465/tcp: SMTPS
- 587/tcp: Submission
- 993/tcp: IMAPS
- 995/tcp: POP3S
- 3306/tcp: MySQL

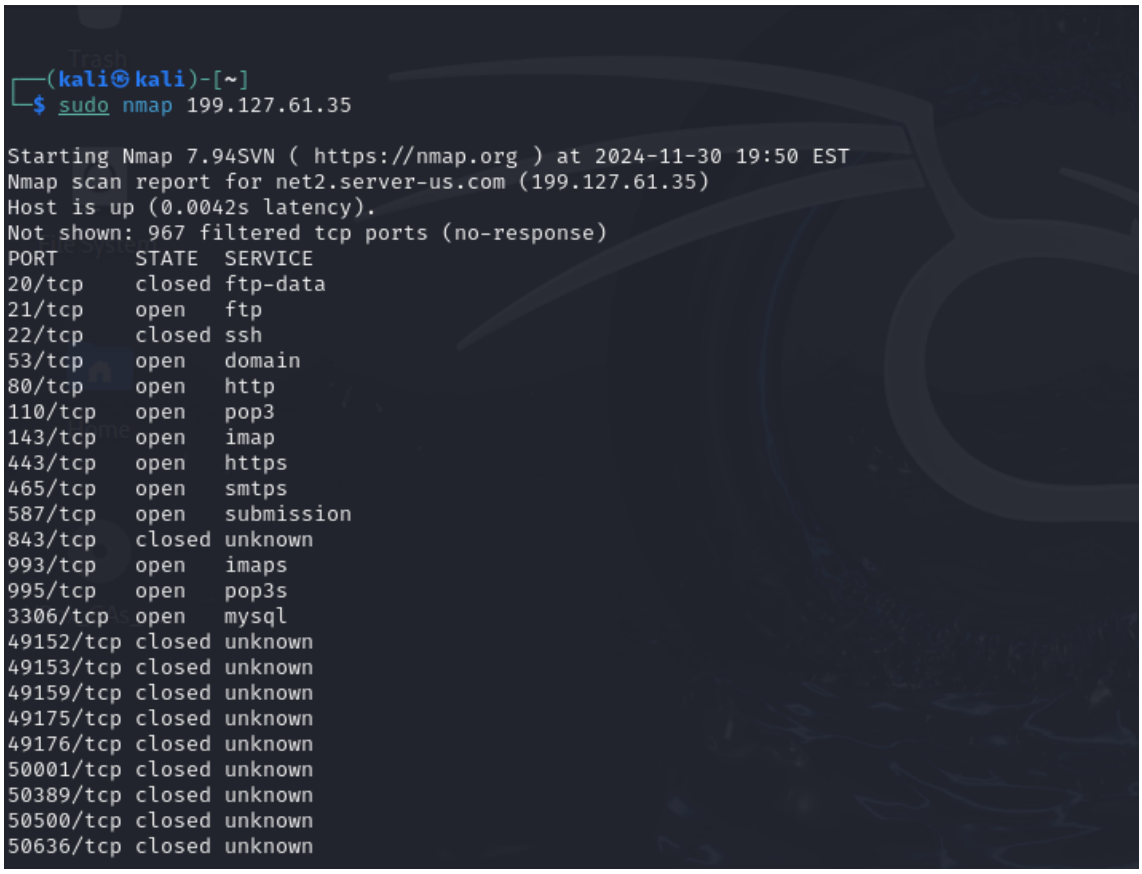
Puertos cerrados

- 20/tcp: FTP-DATA
- 22/tcp: SSH
- Varios puertos dinámicos y desconocidos en el rango de 49152/tcp a 50636/tcp.

La imagen muestra el resultado de un escaneo realizado con Nmap en la dirección IP 199.127.61.35. Se pueden observar los puertos y servicios asociados a cada uno, indicando el estado de cada puerto como abierto (open) o cerrado (closed). Entre los puertos abiertos, destacan servicios como ftp (puerto 21), ssh (puerto 22), y http (puerto 80). Además, algunos puertos están identificados como desconocidos (unknown). Este tipo de análisis permite identificar los servicios activos en el servidor y evaluar su seguridad.

Figura 22

Análisis de dirección ip de la página web 199.127.61.35.



Nota. En la figura se muestra el resulta de análisis con Nmap del ip de la página web

B. Identificar Servicios Accesibles

Se realizó un escaneo de puertos sobre el host 199.127.61.35 con el propósito de identificar servicios accesibles y determinar posibles vectores de ataque. Las opciones empleadas fueron:

- -T4: Ajusta el nivel de velocidad del escaneo para hacerlo más rápido.
- -Pn: Desactiva la comprobación de si el host está activo (sin enviar paquetes ICMP).
- -n: Evita la resolución de nombres DNS para agilizar el escaneo.
- -ON escaneomuni.txt: Guarda el resultado en un archivo de texto llamado escaneomuni.txt.

Resultados del escaneo:

El host respondió (latencia de 0.12s).

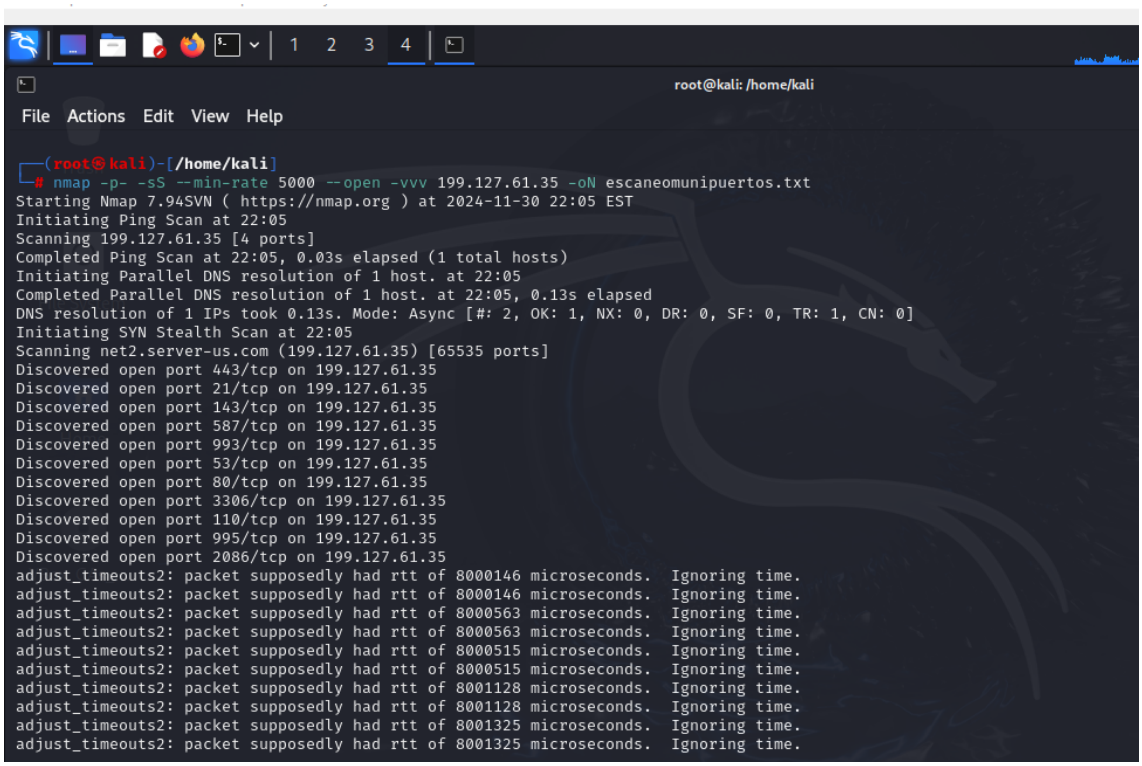
Se identificaron 12 puertos abiertos con servicios asociados:

- 21/tcp: FTP (protocolo de transferencia de archivos).
- 53/tcp: Domain (posiblemente un servidor DNS).
- 80/tcp: HTTP (servidor web no seguro).
- 110/tcp: POP3 (protocolo de correo entrante no seguro).
- 143/tcp: IMAP (protocolo de acceso a correos).
- 443/tcp: HTTPS (servidor web seguro).
- 465/tcp: SMTPS (correo saliente seguro).
- 587/tcp: Submission (envío de correos seguro).
- 993/tcp: IMAPS (correo seguro con IMAP).
- 995/tcp: POP3S (correo seguro con POP3).
- 3306/tcp: MySQL (base de datos).
- 9090/tcp: Zeus-admin (panel de administración).

La imagen muestra el resultado de un escaneo de puertos realizado en la dirección IP 199.127.61.35 con el objetivo de identificar los servicios accesibles en el host y evaluar posibles vectores de ataque. El escaneo se ejecutó utilizando Nmap, y los resultados detallan los puertos abiertos y cerrados, lo que permite obtener información sobre los servicios disponibles en el servidor para posibles pruebas de seguridad.

Figura 23

Escaneo de puertos sobre el host 199.127.61.35.



Nota. En la imagen se muestra escaneo de puertos sobre el host 199.127.61.35 con el propósito de identificar servicios accesibles y determinar posibles vectores de ataque.

C. Análisis de Servicio FTP con Nmap

Se realizó un escaneo enfocado en el puerto 21/tcp (asociado al protocolo FTP) para recopilar información sobre el servicio y su configuración en el host 199.127.61.35. Se utilizaron las siguientes opciones y scripts:

- -sV: Detecta la versión del servicio en el puerto especificado.
- -p 21: Escanea únicamente el puerto 21 (asociado al FTP).
- script ftp-anon: Ejecuta un script de Nmap para comprobar si el servicio FTP permite accesos anónimos.
- script ftp-syst: Ejecuta un script para obtener información sobre el sistema FTP a través del comando SYST.

Estado del host: Activo (latencia de 0.027s).

Puerto identificado:

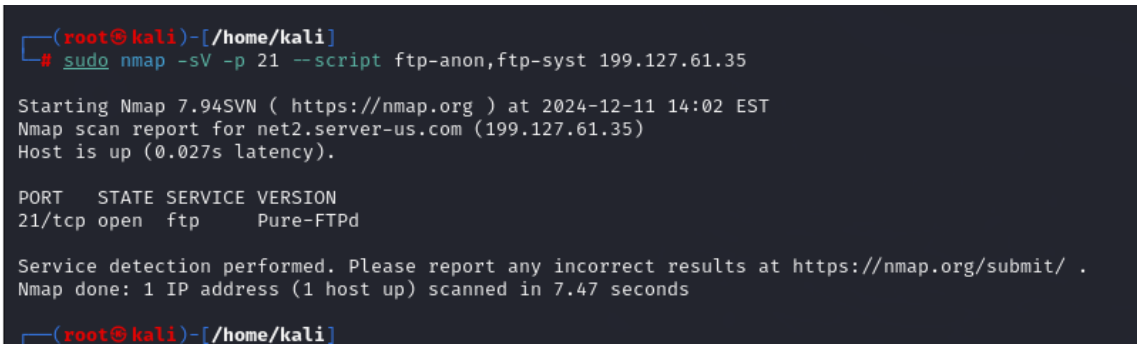
- 21/tcp: Abierto.

- Servicio: FTP (Pure-FTPd).
- Versión: Pure-FTPd (determinada por el servicio de detección).

La imagen muestra un escaneo enfocado en el puerto 21/tcp (utilizado por el protocolo FTP) realizado con Nmap. El comando ejecutado incluye el script ftp-anon, que está diseñado para detectar configuraciones de FTP que permitan el acceso anónimo. En el resultado se observa que el puerto 21 está abierto y el servicio identificado es ProFTPD, lo que sugiere que el servidor está configurado para permitir conexiones FTP. Este tipo de escaneo ayuda a recopilar información sobre el servicio FTP y su configuración en el host 199.127.61.35.

Figura 24

Escaneo enfocado en el puerto 21/tcp.



Nota. En la imagen se muestra escaneo enfocado en el puerto 21/tcp (asociado al protocolo FTP) para recopilar información sobre el servicio y su configuración en el host 199.127.61.35.

D. Escaneo de Servicio FTP para Acceso Anónimo

Se llevó a cabo un escaneo con Nmap sobre el puerto 21/tcp del host 199.127.61.35, empleando el script ftp-anon para verificar si el servidor FTP permite acceso anónimo. Este análisis es útil para identificar configuraciones potencialmente inseguras en el servicio.

Parámetros utilizados:

- script ftp-anon: Evalúa si el servidor FTP permite conexiones anónimas.
- -p 21: Escanea únicamente el puerto 21, asignado al protocolo FTP.

Estado del host: Activo (latencia de 0.027s).

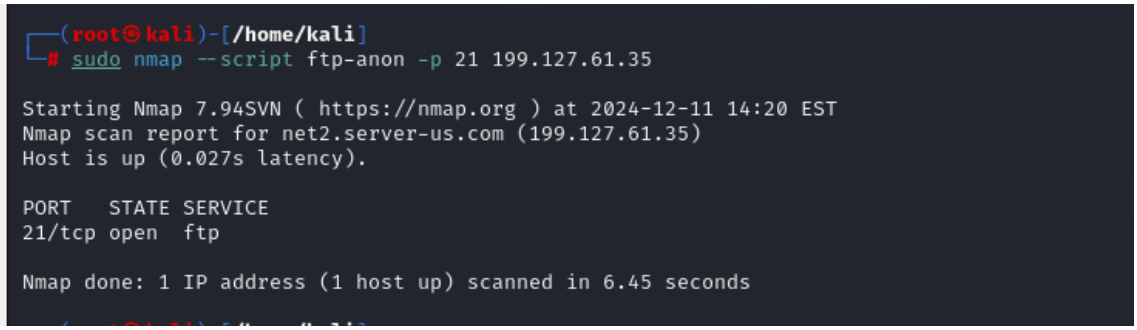
Puerto analizado:

- 21/tcp: Abierto.
- Servicio: FTP.

La imagen presenta un escaneo realizado con Nmap sobre el puerto 21/tcp del host 199.127.61.35, utilizando el script ftp-anon para verificar si el servidor FTP permite acceso anónimo. El resultado muestra que el puerto está abierto y el servicio detectado es FTP, lo que confirma que el servidor permite conexiones sin autenticación. Este tipo de escaneo es útil para evaluar la seguridad del servicio FTP y asegurarse de que no se esté exponiendo información sensible de manera inadvertida.

Figura 25

Escaneo con Nmap sobre el puerto 21/tcp



Nota. En la imagen se muestra escaneo con Nmap sobre el puerto 21/tcp del host 199.127.61.35, empleando el script ftp-anon para verificar si el servidor FTP permite acceso anónimo.

E. Escaneo del Servicio Dns en el Puerto 53

Se realizó un escaneo con Nmap sobre el puerto 53/tcp del host 199.127.61.35 para analizar el servicio DNS y determinar si existe riesgo de abuso mediante ataques de amplificación o consultas recursivas maliciosas. El comando empleó el script dns-recursion, diseñado para identificar si el servidor DNS permite recursion.

Parámetros utilizados:

- --script=dns-recursion: Evalúa si el servidor DNS permite recursion, una configuración que puede ser explotada por atacantes para realizar ataques de amplificación.
- -p 53: Escanea únicamente el puerto 53, reservado para servicios de DNS.

Estado del host: Activo (latencia de 0.027s).

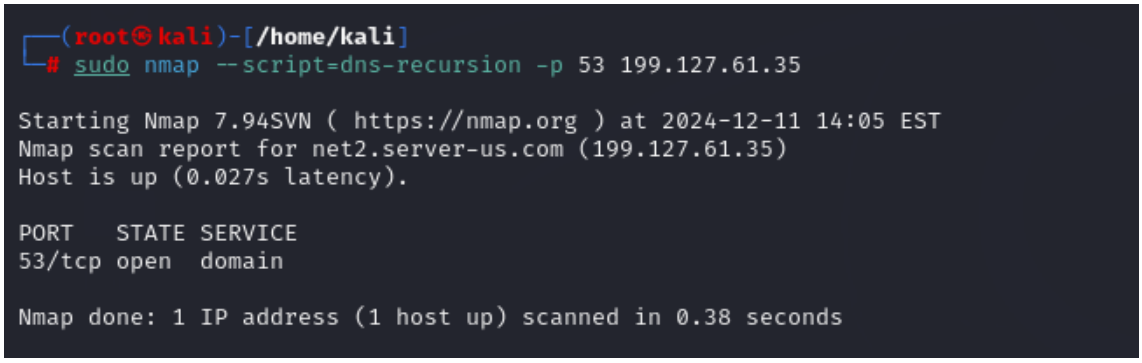
Puerto analizado:

- 53/tcp: Abierto.
- Servicio: DNS (domain).

La imagen muestra un escaneo realizado con Nmap sobre el puerto 53/tcp del host 199.127.61.35, utilizando el script dns-recurrsion para analizar el servicio DNS. El escaneo indica que el puerto 53 está abierto y que el servicio DNS está habilitado, lo que permite realizar consultas de nombres de dominio. Este tipo de análisis es útil para detectar posibles configuraciones inseguras o vulnerabilidades relacionadas con la resolución de nombres en la red.

Figura 26

Escaneo con Nmap sobre el puerto 53/tcp



Nota. En la imagen se muestra escaneo con Nmap sobre el puerto 53/tcp del host 199.127.61.35 para analizar el servicio DNS.

F. Escaneo del Servicio HTTP en el Puerto 80

Se realizó un análisis con Nmap sobre el puerto 80/tcp del host 199.127.61.35, utilizando scripts específicos para obtener información del encabezado HTTP y el título

de la página principal. Este análisis ayuda a identificar el servidor web en uso y posibles configuraciones visibles.

Parámetros utilizados:

- -SV: Detecta la versión del servicio en ejecución en el puerto.
- --script=http-title, http-headers: Obtiene el título de la página HTTP y los encabezados de respuesta para identificar configuraciones del servidor**.**

Estado del host: Activo (latencia de 0.014s).

Puerto analizado:

- 80/tcp: Abierto.
- Servicio: HTTP (servido por LiteSpeed).
- Versión detectada: LiteSpeed Web Server.
- Encabezados HTTP:
- HTTP/1.0 404 Not Found: Indica que el recurso solicitado no está disponible.
- Content-Type: text/html.
- Date: Wed, 11 Dec 2024 19:06:06 GMT.
- Server: LiteSpeed.
- HTML del error 404:
- Indica un diseño básico para la página de error del servidor.
- Incluye estilos y metadatos que destacan configuraciones predeterminadas de LiteSpeed, como:
- Soporte de codificación UTF-8.
- Desactivación de caché.

En la captura se observa un análisis realizado con Nmap sobre el puerto 80/tcp del host 199.127.61.35. Se utiliza el script http-title_http-headers para obtener información sobre el servidor web, como los encabezados HTTP y el título de la página. El resultado muestra que el puerto 80 está abierto y que el servicio es un servidor web HTTP/1.0, con un encabezado que incluye detalles sobre el contenido y las configuraciones del servidor. Este tipo de análisis es útil para evaluar la configuración y seguridad del servidor web.

Figura 27

Análisis con Nmap sobre el puerto 80/tcp

Nota. En la imagen se muestra análisis con Nmap sobre el puerto 80/tcp del host 199.127.61.35

G. Escaneo de los Servicios POP3 y POP3S en los Puertos 110 y 995

Se realizó un análisis con Nmap para identificar los servicios relacionados con el protocolo de correo electrónico en los puertos 110 (POP3) y 995 (POP3S) del host 199.127.61.35. Este tipo de escaneo es útil para verificar configuraciones de servicios de correo y detectar posibles vulnerabilidades en ellos.

Parámetros utilizados:

- -SV: Detecta la versión de los servicios ejecutándose en los puertos especificados.
- -p 110,995: Escanea únicamente los puertos POP3 y POP3S.

Estado del host: Activo (latencia de 0.027s).

110/tcp:

- Estado: Abierto.

- Servicio: POP3.
- Versión detectada: Servidor Dovecot pop3d.

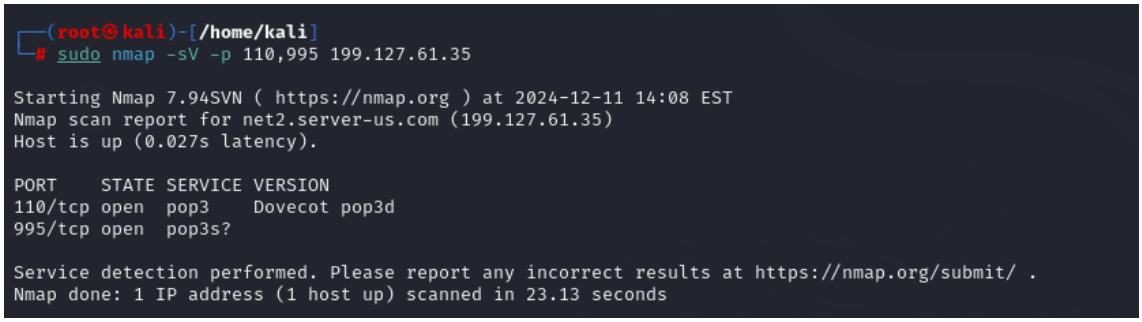
995/tcp:

- Estado: Abierto.
- Servicio: POP3S (POP3 sobre SSL/TLS).
- Versión: No completamente detectada (marcada como pop3s?), lo que indica que no se obtuvo suficiente información para determinar la versión exacta o que el servicio requiere autenticación.

A continuación, se muestra un escaneo realizado con Nmap para identificar los servicios relacionados con el protocolo de correo electrónico POP3 en los puertos 110 (POP3) y 995 (POP3S) del host 199.127.61.35. El análisis indica que ambos puertos están abiertos, revelando que el servidor está configurado para permitir la recepción de correos electrónicos de manera no segura (POP3) y segura (POP3S). Este tipo de análisis es útil para evaluar la configuración y seguridad de los servicios de correo electrónico del servidor.

Figura 28

Escaneo de los Servicios POP3 y POP3 con Nma.



Nota. En la imagen se muestra análisis con Nmap para identificar los servicios relacionados con el protocolo de correo electrónico en los puertos 110 (POP3) y 995 (POP3S) del host 199.127.61.35.

H. Escaneo de Servicios Imap en los Puertos 143 y 993

Se realizó un escaneo con Nmap para identificar los servicios relacionados con el protocolo de correo IMAP en los puertos 143 (IMAP) y 993 (IMAPS) del host 199.127.61.35. Este análisis es útil para verificar configuraciones de servicios de correo

y detectar posibles vulnerabilidades en la administración de correos electrónicos.

Parámetros utilizados:

- sV: Detecta la versión de los servicios ejecutándose en los puertos especificados.
- p 143,993: Escanea únicamente los puertos para IMAP e IMAPS.

Estado del host: Activo (latencia de 0.027s).

143/tcp:

- Estado: Abierto.
- Servicio: IMAP.
- Versión detectada: Servidor Dovecot imapd.

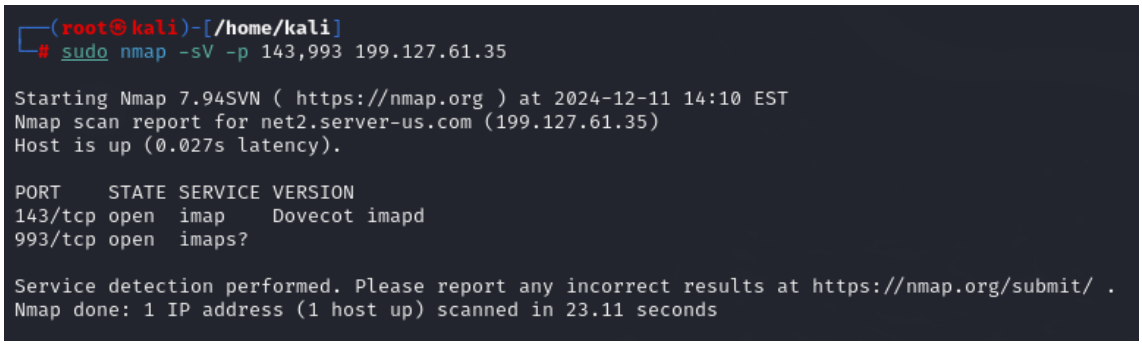
993/tcp:

- Estado: Abierto.
- Servicio: IMAPS (IMAP sobre SSL/TLS).
- Versión: No completamente detectada (marcada como imaps?), lo que indica que no se obtuvo suficiente información para determinar la versión exacta o que el servicio requiere autenticación.

El presenta un escaneo realizado con Nmap para identificar los servicios relacionados con el protocolo de correo electrónico IMAP en los puertos 143 (IMAP) y 993 (IMAPS) del host 199.127.61.35. El análisis muestra que ambos puertos están abiertos, indicando que el servidor permite la gestión de correos electrónicos de manera no segura (IMAP) y segura (IMAPS). Este tipo de escaneo es útil para evaluar la configuración de los servicios de correo electrónico en el servidor y su seguridad.

Figura 29

Escaneo de Servicios IMAP en los Puertos 143 y 993 con Nmap.



Nota. En la imagen se muestra escaneo con Nmap para identificar los servicios relacionados con el protocolo de correo IMAP en los puertos 143 (IMAP) y 993 (IMAPS) del host 199.127.61.35.

I. Escaneo de Cifras SSL/TLS en el Puerto 443

Se ejecutó un análisis con Nmap utilizando el script ssl-enum-ciphers para identificar las configuraciones de seguridad relacionadas con los protocolos SSL/TLS en el puerto 443 (HTTPS) del host 199.127.61.35. Este escaneo es útil para evaluar la seguridad de las conexiones cifradas y las cifras soportadas.

Parámetros utilizados:

- --script ssl-enum-ciphers: Permite enumerar los algoritmos de cifrado (ciphers) y configuraciones SSL/TLS activas.
- -p 443: Escaneo específico del puerto HTTPS.

Estado del host: Activo (latencia de 0.027s).

Puerto analizado: 443/tcp:

Estado: Abierto.

Servicio detectado: HTTPS.

TLSv1.2 Cifras soportadas

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - Fuerza: A.
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - Fuerza: A.

- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - Fuerza: A.
- Compresores: NULL (sin compresión).
- Preferencia de cifra: servidor (el servidor elige el cifrado a usar).

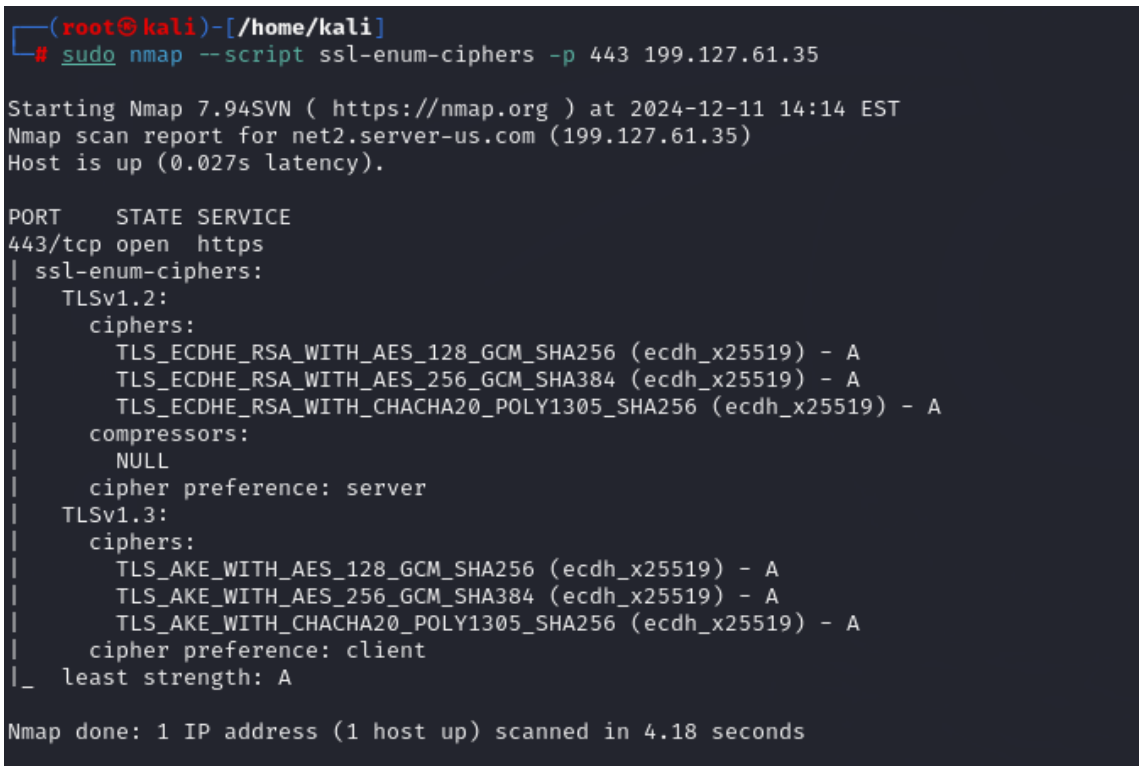
TLSv1.3 Cifras soportadas:

- TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - Fuerza: A.
- TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - Fuerza: A.
- TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - Fuerza: A.
- Preferencia de cifra: cliente (el cliente tiene prioridad para elegir el cifrado).

El escaneo realizado con Nmap utilizando el script ssl-enum-ciphers para identificar las configuraciones de seguridad relacionadas con los protocolos SSL/TLS en el puerto 443 del host 199.127.61.35. El resultado revela los algoritmos de cifrado soportados por el servidor, mostrando una variedad de opciones de cifrado TLS con diferentes configuraciones de seguridad. Este tipo de escaneo es útil para evaluar la fortaleza de las conexiones seguras y detectar posibles vulnerabilidades en la implementación de SSL/TLS.

Figura 30

Escaneo de Cifras SSL/TLS en el Puerto 44.



Nota. En la imagen se muestra con Nmap utilizando el script ssl-enum-ciphers para identificar las configuraciones de seguridad relacionadas con los protocolos SSL/TLS en el puerto 443.

J. Escaneo SMTP en el Puerto 587

El escaneo realizado con Nmap permite identificar los servicios y comandos soportados por el servidor SMTP configurado en este puerto. El puerto 587 generalmente se utiliza para envío de correos electrónicos de forma segura con autenticación.

Parámetros utilizados:

- -p 587: Escaneo específico del puerto SMTP.
- -sV: Detección de versión del servicio.
- --script smtp-commands: Enumeración de comandos soportados por el servidor SMTP.

Estado del host: Activo (latencia de 0.027s).

Puerto analizado: 587/tcp:

Estado: Abierto.

Servicio detectado: SMTP (Exim smtpd) versión 4.97.1.

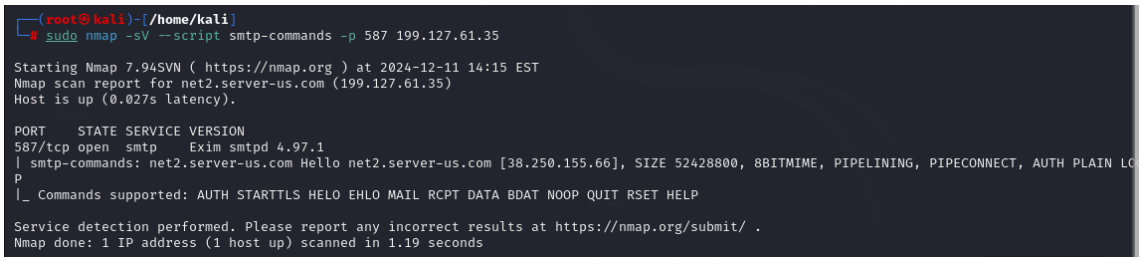
Comandos SMTP soportados: El servidor SMTP soporta los siguientes comandos:

- AUTH: Permite autenticación (soporta PLAIN y posiblemente LOGIN).
- STARTTLS: Protocolo para iniciar una conexión cifrada mediante TLS.
- HELO/EHLO: Identificación del cliente al servidor SMTP.
- MAIL/RCPT/DATA: Envío de correos electrónicos (dirección de remitente, destinatario y contenido).
- NOOP/QUIT/RSET/HELP: Comandos básicos de control.
- PIPELINING: Permite el envío de múltiples comandos sin esperar respuesta, mejorando la eficiencia.
- 8BITMIME: Soporte para mensajes en 8 bits (extendiendo ASCII estándar).
- SIZE: Límite máximo de tamaño de mensajes soportado por el servidor (52428800 bytes, ~50 MB).
- PIPECONNECT: Indica que el servidor soporta conexiones seguras dentro de PIPELINING.

El escaneo realizado con Nmap para identificar los servicios y comandos soportados por el servidor SMTP en el puerto 587 del host 199.127.61.35. El escaneo revela que el puerto está abierto y que el servidor SMTP está configurado para aceptar una serie de comandos relacionados con la transferencia de correo, como STARTTLS, EHLO, entre otros. Este análisis es útil para evaluar las capacidades y configuraciones del servidor de correo, así como para identificar posibles vectores de ataque relacionados con el servicio SMTP.

Figura 31

Escaneo SMTP en el Puerto 587 con Nmap.



Nota. En la imagen se muestra escaneo realizado con Nmap permite identificar los servicios y comandos soportados por el servidor SMTP configurado en este puerto.

K. Escaneo MySQL en el Puerto 3306

El puerto 3306 es utilizado por defecto para el servicio de bases de datos MySQL. Este escaneo ha identificado tanto el servicio como su versión, además de extraer detalles relacionados con las capacidades y la configuración del servidor MySQL.Parámetros utilizados:

- -p 3306: Escaneo del puerto de MySQL.
- -sV: Detección de la versión del servicio.
- --script mysql-info: Recopilación de información detallada sobre la configuración de MySQL.

Activo (latencia de 0.027s).

Puerto analizado: 3306/tcp:

- Estado: Abierto.
- Servicio detectado: MySQL versión 5.5.5-10.6.19-MariaDB.

Información detallada del servidor MySQL:

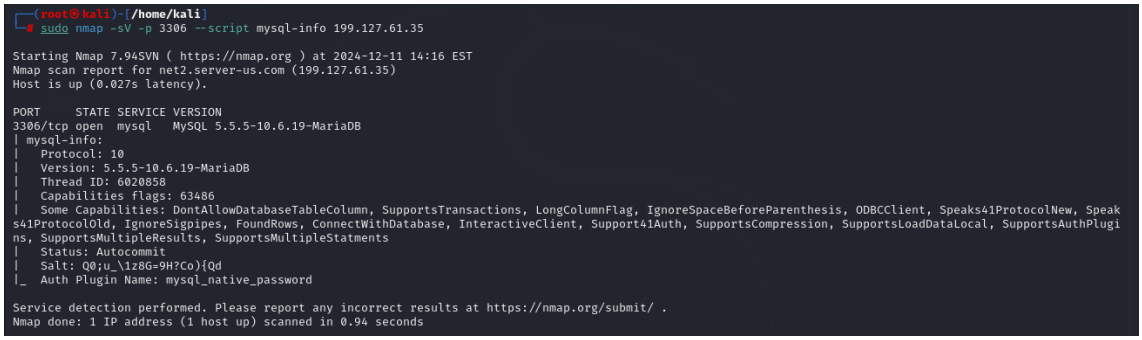
- Protocolo: 10.
- Versión de MySQL: 5.5.5-10.6.19-MariaDB.
- Thread ID: 6020858.
- Flags de capacidad: El servidor soporta varias características, como:
- Soporte de transacciones.

- Permite bases de datos, tablas y columnas largas.
- Soporte para múltiples resultados y múltiples declaraciones.
- Compresión de datos.
- Soporte para carga local de datos.
- Manejo de autenticación mediante el plugin mysql_native_password.
- Estado de autocommit: Activado (esto significa que cada declaración se confirma de manera automática, lo cual puede ser adecuado o no dependiendo de la aplicación).
  - Salts de autenticación: Q0; u_\1z8G-9?Co){Qd (Este valor se utiliza en el proceso de autenticación).

El escaneo realizado con Nmap sobre el puerto 3306, utilizado por defecto para el servicio de bases de datos MySQL. El análisis revela información sobre la versión del servidor MySQL, en este caso 5.5.5-10.1.48-MariaDB y los protocolos y características soportadas por el servicio, como MySQL Protocol, Compression, y Auth Plugins. Este tipo de escaneo es útil para identificar configuraciones del servidor de bases de datos y detectar posibles vulnerabilidades relacionadas con la seguridad en su configuración.

Figura 32

Escaneo MySQL en el Puerto 3306 con Nma.



Nota. En la imagen se muestra escaneo del puerto 3306 es utilizado por defecto para el servicio de bases de datos MySQL

4.2.2.2. Netcraft para Recolectar Datos de Servidores y Certificados SSSL en la Página Web de la Municipalidad Distrital San Juan Bautista.

a. Información general

- Título del sitio: Coming Soon
- Fecha de primera detección: Diciembre 2016

- Idioma principal: Inglés
- Proveedor de Hosting: GoDaddy.com, LLC
- Dirección IP: 192.169.146.218
- Sistema Autónomo IPv4: AS398101
- DNS Reverso: 218.146.169.192.host.secureserver.net
- Extensión de dominio: .gob.pe (Perú)
- Seguridad DNS (DNSSEC): Habilitado

b. Infraestructura y Red

- Rango de IP: 192.169.128.0 - 192.169.255.255
- Organización del Nameserver: whois.wildwestdomains.com
- Administrador de DNS: dns@jomax.net
- Empresa de registro del dominio: No disponible

c. Seguridad SSL/TLS

- Autoridad de Certificación: Let's Encrypt
- Validez del certificado: 17 de diciembre de 2024 - 17 de marzo de 2025
- Servidor Web: Apache
- Protocolo TLS: TLSv1.2
- Cifrado: ECDHE-RSA-AES256-GCM-SHA384
- Algoritmo de firma: sha256WithRSAEncryption
- Longitud de clave pública: 2048 bits
- Certificado válido para:
- mail.munisanjuanbautista.gob.pe
- munisanjuanbautista.gob.pe
- webmail.munisanjuanbautista.gob.pe
- www.munisanjuanbautista.gob.pe

d. Vulnerabilidades Analizadas

- SSLv3/POODLE: No soporta SSLv3 (seguro contra POODLE)
- Heartbleed: No explotable

e. Certificación y Transparencia

- Emisor del Certificado: ISRG Root X1
- Validez del Certificado Raíz: 2015 - 2035
- OCSP Stapling: No disponible

f. Políticas de Envío de Correos (SPF)

- Permite envíos desde secureserver.net
- Bloquea otros servidores (-all)

La consulta realizada con Netcraft para el sitio web https://www.munisanjuanbautista.gob.pe. El reporte muestra detalles sobre el fondo, la red y la infraestructura del sitio, brindando información sobre el servidor web y su tecnología subyacente. Este tipo de consulta es útil para obtener una visión general de la plataforma tecnológica que sustenta el sitio web, así como para identificar posibles configuraciones o vulnerabilidades.

Figura 33

Reporte de consulta de Netcraft.

Nota. En la figura se muestra el reporte de consulta de Netcraft.

4.3.Fase III: Escaneo de Vulnerabilidades

El escaneo de vulnerabilidades es una etapa clave en la evaluación de la seguridad de los sistemas informáticos, cuyo objetivo es identificar posibles debilidades en la infraestructura tecnológica que puedan ser explotadas por atacantes. En este caso, se utilizó un escaneo automatizado con herramientas como Owasp zap para analizar la página web de la Municipalidad Distrital de San Juan Bautista.

4.3.1. Evaluación Automática.

La evaluación automática es un proceso sistemático que utiliza herramientas especializadas para identificar vulnerabilidades en aplicaciones web sin intervención manual directa. En el marco de esta investigación, se emplearon dos herramientas ampliamente reconocidas en el ámbito de la seguridad web: Owasp zap . Ambas herramientas permiten realizar escaneos detallados de la infraestructura web de la municipalidad, detectando vulnerabilidades comunes como inyecciones SQL, Cross-Site Scripting (XSS) y configuraciones inseguras.

4.3.1.1. OWASP ZAP Página Web de la Municipalidad Distrital de San Juan Bautista.

Se identificaron distintos niveles de riesgo en la evaluación de seguridad, determinando vulnerabilidades potenciales en la infraestructura analizada.

El escaneo de seguridad realizado sobre la dirección IP 199.127.61.35 reveló la presencia de varios puertos abiertos y servicios en ejecución. A continuación, se presentan las observaciones clave:

Tabla 2

Análisis de riesgos de seguridad en aplicación Web de la municipalidad.

Sitio	Riesgo Alto	Riesgo Medio	Riesgo Bajo	Informativo
https://connect.facebook.net	0	1	0	0
https://use.fontawesome.com	0	1	2	0
https://www.munisanjuanbautista.gob.pe:2096	0	0	0	1
https://www.munisanjuanbautista.gob.pe	1	0	1	0
https://munisanjuanbautista.gob.pe	0	1	2	3

Nota. Elaboración propia

Se observaron riesgos de seguridad en varios sitios, incluyendo uno con riesgo alto en https://www.munisanjuanbautista.gob.pe. Además, se detectaron riesgos medios y bajos en otros dominios, como https://use.fontawesome.com y https://munisanjuanbautista.gob.pe. En general, la mayoría de los sitios presentaron un riesgo bajo o informativo, pero aún se deben abordar las vulnerabilidades detectadas.

4.3.1.2. Análisis de Riesgos de Seguridad en Página Web de la Municipalidad Distrital de San Juan Bautista.

Los hallazgos en el análisis de seguridad muestran vulnerabilidades críticas y medias que pueden comprometer la integridad, confidencialidad y disponibilidad de la aplicación. Es fundamental aplicar estrategias de mitigación para reducir los riesgos y mejorar la postura de seguridad del sistema. A continuación, se presentan las observaciones clave:

Tabla 3

Análisis de riesgos de página web de la municipalidad.

Tipo de Riesgo	Cantidad alertas	Descripción
Divulgación de Información Personal Identificable (PII Disclosure)	14 (63.6%)	Exposición de información personal identificable, con riesgos de privacidad y cumplimiento normativo.
Ausencia de Tokens Anti-CSRF	7 (31.8%)	Falta de protección contra ataques CSRF, permitiendo acciones maliciosas en nombre del usuario.
Divulgación de Errores de Aplicación (Application Error Disclosure)	58 (263.6%)	Revelación de detalles técnicos en errores, facilitando la explotación por atacantes.
Encabezado Content	186 (845.5%)	Ausencia de CSP permite inyección de

Security Policy (CSP) No Configurado		contenido malicioso como XSS.
Mala Configuración de Cross-Domain	2 (9.1%)	Configuración incorrecta de CORS que permite accesos no autorizados.

Nota. Elaboración propia

Se identificaron vulnerabilidades críticas como la divulgación de información personal (PII), la falta de protección contra ataques CSRF y la revelación de errores técnicos, lo que facilita la explotación por parte de atacantes. También se detectó la ausencia de la cabecera Content Security Policy (CSP), lo que expone a ataques de inyección maliciosa, y una mala configuración de Cross-Domain que permite accesos no autorizados. Estas debilidades deben ser corregidas para mejorar la seguridad de la aplicación.

4.3.1.3. Análisis de Riesgo de Seguridad en la Página Web de la Municipalidad Distrital San Juan Bautista con Nikto

Nikto es una herramienta especializada que detecta fallos de seguridad como encabezados mal configurados, tecnologías desactualizadas o vulnerabilidades comunes en la infraestructura web. En el caso de la Municipalidad Distrital de San Juan Bautista, se utilizó Nikto para evaluar la seguridad de la página web, identificando vulnerabilidades clave.

Tabla 4

Resultados del Análisis con Nikto de la municipalidad.

Vulnerabilidad	Descripción
X-Powered-By Header	Se encontró el encabezado X-Powered-By: PHP/8.0.30, lo que puede revelar información sobre la tecnología utilizada.
Strict-Transport-Security no definido	No se encontró la cabecera HSTS, lo que podría exponer la conexión a ataques de intermediario.
Alt-Svc Header HTTP/3	Se detectó un encabezado alt-svc que

	anuncia HTTP/3, pero Nikto no puede probar QUIC.
X-Content-Type-Options no configurado	La falta de este encabezado podría permitir que el contenido se interprete incorrectamente.
Divulgación de dirección IP	Se encontró una dirección IP en la cabecera Location, lo que podría revelar información sensible.
Encabezado Drupal Link	Se detectó un enlace que sugiere la presencia de Drupal.
Encabezado Joomla	Se encontró un encabezado no común X-Content-Encoded-By indicando el uso de Joomla.
Vulnerabilidad BREACH	El encabezado Content-Encoding: deflate podría significar que el servidor es vulnerable al ataque BREACH.
Certificado Wildcard	El sitio usa un certificado wildcard *.munisanjuanbautista.gob.pe, lo que podría ser un riesgo si no se administra adecuadamente.

Nota. Elaboración propia

Se detectaron varias vulnerabilidades de seguridad, incluyendo la divulgación de tecnología a través del encabezado X-Powered-By, la falta de cabeceras críticas como HSTS y X-Content-Type-Options, y posibles exposiciones de información sensible, como direcciones IP y detalles de la infraestructura de Drupal y Joomla. Además, se identificó una vulnerabilidad BREACH y el uso de un certificado wildcard que podría representar un riesgo. Estas debilidades deben ser mitigadas para mejorar la seguridad general.

4.3.2. Análisis de Configuración

El análisis de configuración es un paso crucial para identificar posibles configuraciones inseguras en la infraestructura tecnológica, incluidas las configuraciones de dispositivos de red, servidores web, y sistemas de aplicaciones. Este análisis tiene como objetivo garantizar que las mejores prácticas de seguridad se hayan implementado adecuadamente para proteger la red y las aplicaciones de posibles ataques.

4.3.2.1. Revisión de Configuraciones del Router Mikrotik

Durante esta fase se revisaron los dispositivos críticos de la red, como routers, switches y servidores, para identificar configuraciones inseguras que puedan ser explotadas por atacantes. Los aspectos revisados incluyen:

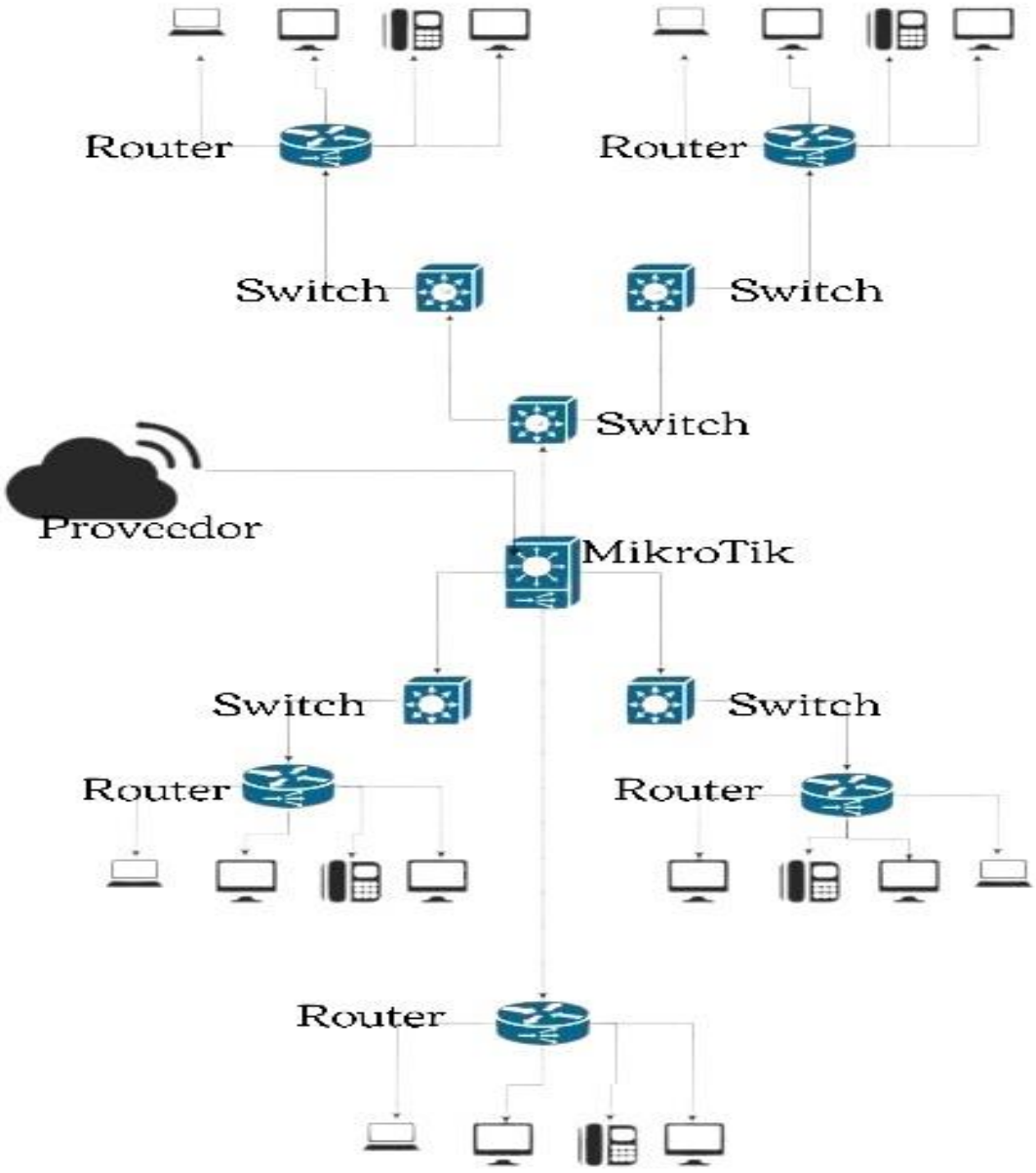
- Gestión de contraseñas y acceso: Se verificó que las contraseñas y las claves de acceso se gestionen adecuadamente, con la implementación de políticas de contraseñas fuertes y el uso de autenticación multifactor (MFA) donde fuera posible.

a. Gestión de Contraseñas y Accesos

Se evaluó la implementación de políticas de gestión de contraseñas y control de acceso en los sistemas críticos. Se verificó que las contraseñas cumplieran con los requisitos de seguridad, incluyendo al menos 8 caracteres con una combinación de mayúsculas, minúsculas, números y caracteres especiales.

Figura 34

Topología de red de la Municipalidad de San Juan Bautista.



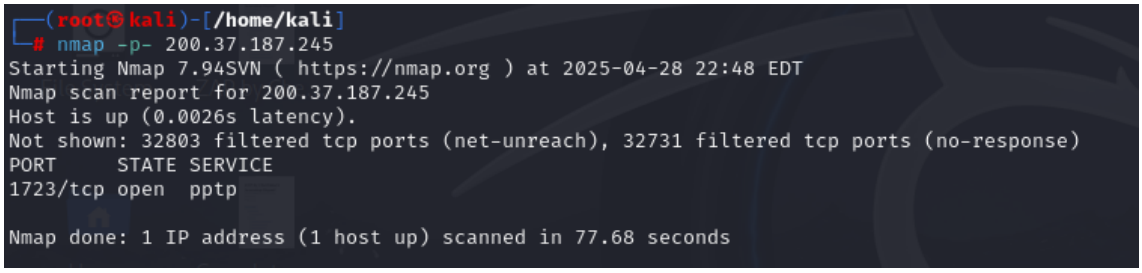
Nota. La figura representa la topología de red estrella en este caso de la Municipalidad de San Juan Bautista y los equipos interconectados. Elaboración propia.

La infraestructura de red de la Municipalidad Distrital de San Juan Bautista adopta una topología tipo estrella, lo que le otorga características clave como centralización y

escalabilidad. En este diseño, todos los dispositivos de la red, tales como routers, switches y computadoras, se conectan a un único dispositivo central, que en este caso es un switch o un servidor de red, siendo el MikroTik el dispositivo central que gestiona y coordina las conexiones de la red. Esta topología facilita la administración eficiente de la infraestructura tecnológica, ya que permite un control centralizado del tráfico y las configuraciones, mientras que su naturaleza escalable asegura que la red pueda crecer y adaptarse conforme aumenten las necesidades de la municipalidad.

Figura 35

Escaneo de los puertos de la IP 200.37.187.245



Nota. La figura muestra escaneo de los puertos con Nmap

El resultado del escaneo realizado con Nmap muestra información clave sobre la red y la infraestructura de puertos de la IP 200.37.187.245. Aquí está el análisis detallado:

Estado del host:

- El host está activo y responde a las solicitudes de red.

Puertos escaneados:

- Se escanearon 65,535 puertos en total.
- 32,803 puertos fueron filtrados (no se pudo acceder a ellos debido a reglas de firewall, o el dispositivo los bloquea).
- 32,731 puertos fueron inaccesibles (es decir, no respondieron a las solicitudes de Nmap).

Puertos abiertos:

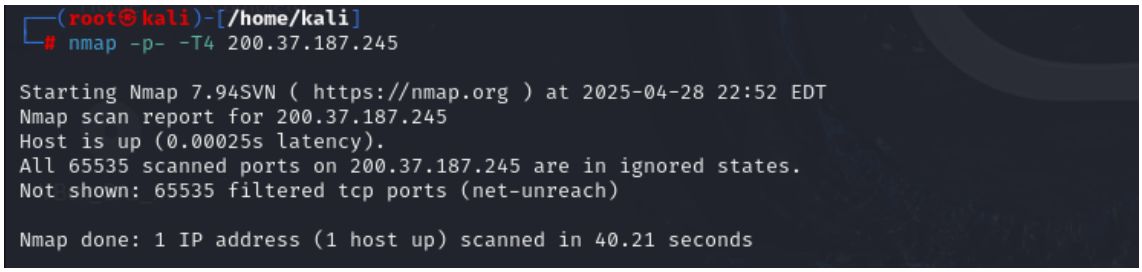
- El único puerto abierto es el 1723/tcp, que corresponde al servicio PPTP (Point-

to-Point Tunneling Protocol). Este servicio es típicamente utilizado para crear túneles VPN (Virtual Private Network).

- El puerto está marcado como open (abierto), lo que significa que el servicio PPTP está escuchando en ese puerto y accesible para los usuarios.

Figura 36

Escaneo de manera rápida con Nmap



Nota. En la figura se muestra un escaneo de manera rápida del IP 200.37.187.245

Puertos escaneados:

- El comando escaneó todos los 65535 puertos disponibles en la IP.

Estado de los puertos:

- Todos los puertos están en "ignored states", lo que significa que Nmap no recibió respuesta o que no pudo obtener una respuesta válida de esos puertos.
- 65535 puertos filtrados: Esto indica que los puertos están bloqueados o filtrados, probablemente por un firewall o sistema de protección de red. Los puertos "filtrados" son aquellos que no han respondido a las solicitudes de Nmap, probablemente porque las conexiones son rechazadas antes de que puedan ser establecidas.
- "net-unreach": Esto significa que Nmap no puede alcanzar la red de esos puertos, lo cual es una señal de que puede haber reglas de firewall o dispositivos de seguridad que impiden el acceso.

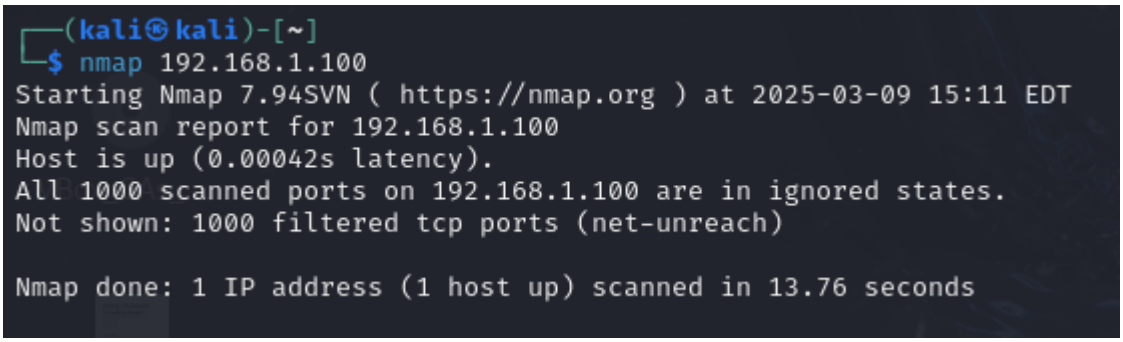
4.3.1.4. Análisis de Resultados del Scaneo de Puertos en Laptops Personales con Nmap.

A. Oficina Gerencia Municipal laptop 1.

El objetivo del escaneo fue identificar los puertos accesibles en el rango completo (1-65535), comenzando con un escaneo inicial de los 1000 puertos más comunes según la base de datos de Nmap. Este proceso permitió evaluar la exposición del sistema a posibles amenazas y analizar su configuración de red y seguridad.

Figura 37

Reporte de consulta de Nmap.



Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

- Host is up (0.00042s latency)": Indica que el sistema está activo y responde en la red IP 192.168.1.100. La latencia extremadamente baja (0.00042 segundos) confirma que ambas máquinas operan dentro de la misma subred local, validando la configuración de red en modo Puente (Bridge Adapter) en VirtualBox.

- "All 1000 scanned ports... ignored states": Los 1000 puertos analizados, correspondientes a los más utilizados (como 80, 443, 445, entre otros), no mostraron actividad detectable, lo que indica que no hay servicios expuestos en esos puertos o que están protegidos por reglas de firewall.

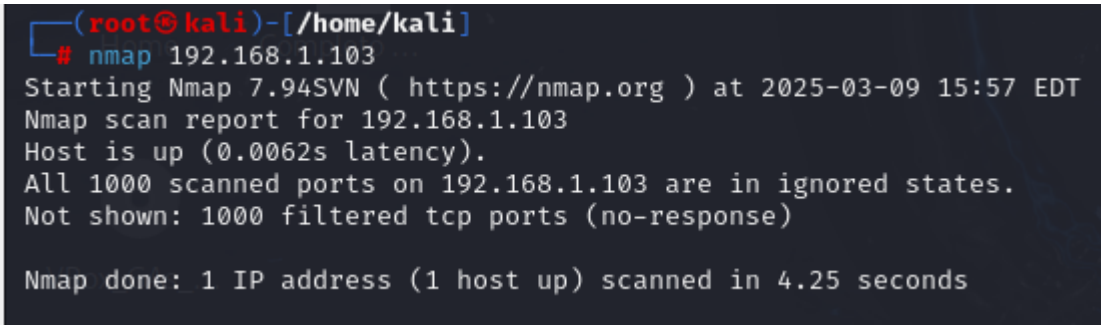
- "1000 filtered tcp ports (net-unreach)": El estado "filtered" indica que los paquetes enviados por Nmap no recibieron una respuesta definitiva (ni aceptación ni rechazo explícito), lo que sugiere la presencia de un firewall o reglas de filtrado activas. El mensaje "net-unreach" sugiere que los paquetes fueron bloqueados antes de alcanzar los servicios correspondientes o que la red está configurada para no responder a solicitudes de escaneo.

B. Oficina Gerencia Municipal laptop 2.

El objetivo principal de este análisis fue identificar vulnerabilidades y evaluar el nivel de exposición a posibles amenazas en los sistemas informáticos de la Gerencia Municipal.

Figura 38

Reporte de consulta de Nmap.



Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

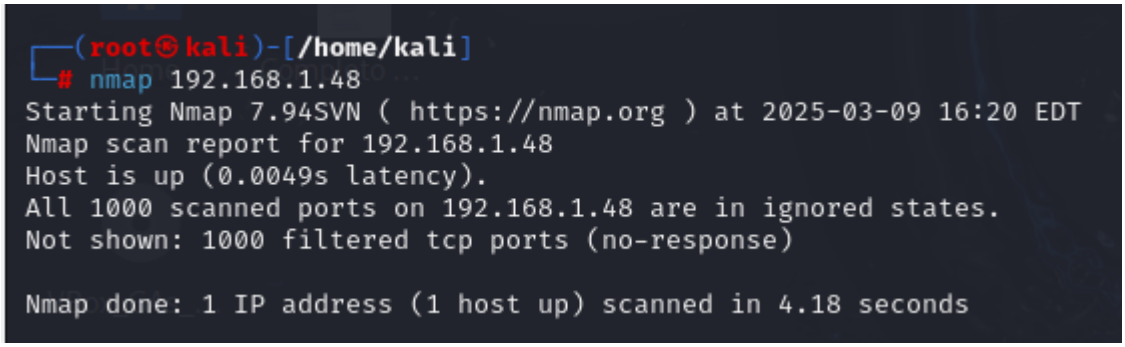
- **Estado del host:** El host con la dirección IP 192.168.1.103 respondió a las solicitudes de red, indicando que está activo y accesible en la red local.
- **Puertos escaneados:** Los 1000 puertos analizados, correspondientes a los más comunes según la base de datos de Nmap (como 80, 443, 445, entre otros), no mostraron actividad detectable.
- **Puertos filtrados:** El estado "filtered" implica que los paquetes enviados por Nmap no recibieron una respuesta definitiva (ni aceptación ni rechazo explícito). Esto sugiere que un firewall o dispositivo de seguridad está bloqueando el tráfico hacia esos puertos, impidiendo su detección.

C. Oficina Gerencia Municipal laptop 3.

El objetivo principal de este análisis fue identificar vulnerabilidades y evaluar el nivel de exposición a posibles amenazas en los sistemas informáticos de la Gerencia Municipal.

Figura 39

Reporte de consulta de Nmap.



Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

- Host is up (0.0049s latency): El host con la dirección IP 192.168.1.48 está activo y responde a las solicitudes de red, con una latencia de 0.0049 segundos, lo que indica una conexión rápida y estable.
- All 1000 scanned ports on 192.168.1.48 are in ignored states: Nmap escaneó los 1000 puertos TCP más comunes y determinó que todos están en "ignored states". Este término indica que Nmap no recibió respuestas útiles de esos puertos, por lo que los omitió en el listado detallado.
- Not shown: 1000 filtered tcp ports (no-response): Los 1000 puertos TCP están en estado "filtered", lo que significa que las sondas de Nmap no recibieron respuesta, posiblemente debido a que un firewall o dispositivo de seguridad está bloqueando el tráfico hacia esos puertos.

4.3.1.5. Análisis de Resultados del Scaneo de Puertos en Computadoras Personales con Nmap.

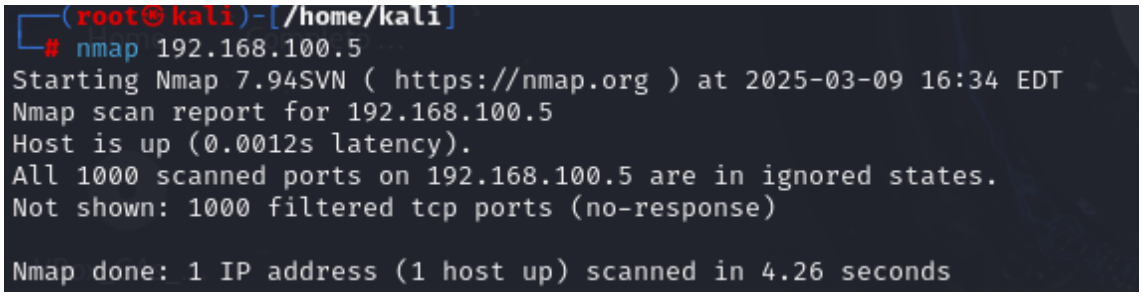
En esta fase, se lleva a cabo un escaneo exhaustivo de puertos utilizando la herramienta Nmap en las diversas computadoras seleccionadas de la Municipalidad Distrital de San Juan Bautista. Este proceso permite identificar los puertos abiertos y los servicios asociados en cada máquina, lo que ayuda a detectar posibles vulnerabilidades y configuraciones inseguras.

A. Oficina TIC

El análisis tuvo como finalidad identificar los puertos accesibles dentro del rango total (1-65535), comenzando con un escaneo preliminar de los 1000 puertos más utilizados, según la base de datos de Nmap. Los resultados obtenidos brindan una perspectiva inicial sobre la interacción entre el sistema analizado y sus configuraciones de red y seguridad.

Figura 40

Reporte de consulta de Nmap.



Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

- "Host is up (0.00042s latency)": Este resultado confirma que el sistema Windows 10 está en funcionamiento y responde dentro de la red. La latencia reducida (0.00042 segundos) indica que ambas máquinas se encuentran en la misma subred local, lo que valida la configuración de red en modo Puente (Bridge Adapter) en VirtualBox.
- "All 1000 scanned ports... ignored states": Los 1000 puertos analizados, que incluyen los más utilizados según la base de datos de Nmap (como 80, 443, 445, entre otros), no reflejaron actividad aparente.
- "1000 filtered tcp ports (net-unreach)": La condición "filtered" indica que los paquetes enviados por Nmap no recibieron una respuesta concreta (ni aceptación ni rechazo). El mensaje "net-unreach" sugiere que los paquetes no lograron llegar a su destino o fueron bloqueados antes de alcanzar los servicios correspondientes.

B. Oficina de Gestión de Recursos Humanos Computadora 1.

El objetivo principal de este análisis fue identificar vulnerabilidades y evaluar el nivel

de exposición a posibles amenazas en los sistemas informáticos.

Figura 41

Reporte de consulta de Nmap.

Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

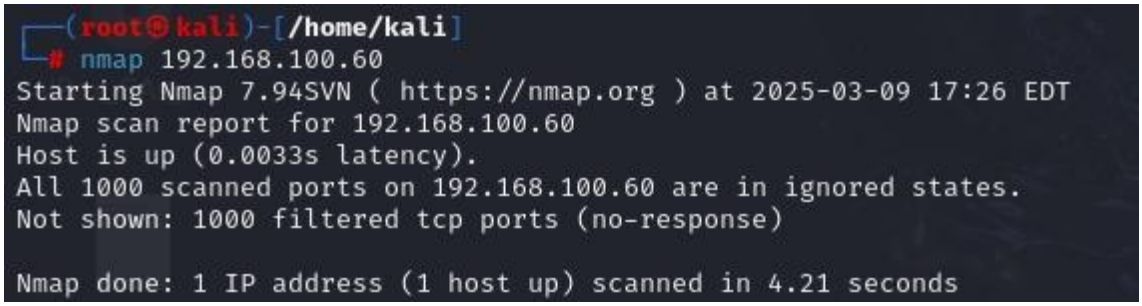
- "Host is up (0.0021s latency)": Esto indica que el host (dispositivo en la dirección IP 192.168.100.50) está activo y responde, con una latencia de 0.0021 segundos, lo que significa que la respuesta del host fue muy rápida.
- "All 1000 scanned ports on 192.168.100.50 open": Este mensaje indica que todos los 1000 puertos escaneados en esa dirección IP están abiertos y accesibles. No hay puertos cerrados ni filtrados, lo que sugiere que no hay restricciones de firewall o medidas de seguridad que estén bloqueando el acceso a esos puertos.
- "Not shown: 1000 filtered tcp ports (no-response)": Este mensaje parece contradictorio con la información anterior, ya que Nmap está reportando que todos los puertos están abiertos, pero también menciona puertos filtrados. Sin embargo, es posible que la frase "filtered tcp ports" se refiera a puertos que no respondieron al escaneo o que fueron ignorados por algún otro motivo, como un firewall intermedio que bloqueó las respuestas sin llegar a bloquear todos los puertos.
- "Nmap done: 1 IP address (1 host up) scanned in 4.18 seconds": Esto indica que Nmap ha terminado el escaneo de una dirección IP (192.168.100.50) y que el escaneo se completó en 4.18 segundos.

C. Oficina de Gestión de Recursos Humanos Computadora 2

El objetivo principal de este análisis fue identificar vulnerabilidades y evaluar el nivel de exposición a posibles amenazas en los sistemas informáticos.

Figura 42

Reporte de consulta de Nmap.



Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

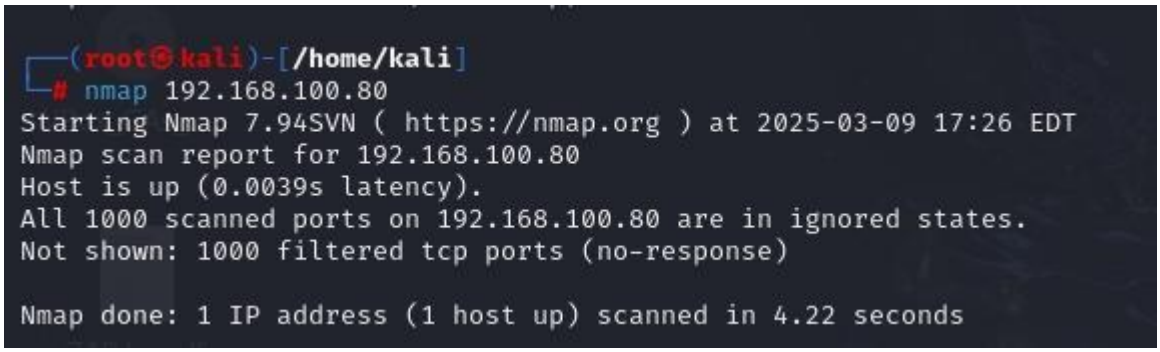
- Host is up (0.0033s latency): El sistema con la dirección IP 192.168.100.60 está activo y responde en la red. La latencia es extremadamente baja, lo que indica que la comunicación entre las máquinas es rápida.
- All 1000 scanned ports on 192.168.100.60 are in ignored states: Los 1000 puertos escaneados no mostraron ningún servicio accesible o respuesta. Los estados de estos puertos son "ignorados", lo que generalmente significa que no se pudo obtener información sobre ellos o que no se permiten conexiones externas.
- Not shown: 1000 filtered tcp ports (no-response): Todos los 1000 puertos filtrados no respondieron. Esto indica que los paquetes enviados para explorar los puertos fueron bloqueados por un firewall u otra forma de seguridad, lo que impide que Nmap reciba respuestas. El estado "no-response" sugiere que los puertos están protegidos, posiblemente mediante filtrado de tráfico.
- Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds: El escaneo de la IP 192.168.100.60 fue completado exitosamente en 4.21 segundos, y 1 host fue identificado como activo.

D. Gerencia de Recaudación y Administración Tributaria Computadora 1

El objetivo principal de este análisis fue identificar vulnerabilidades y evaluar el nivel de exposición a posibles amenazas en los sistemas informáticos.

Figura 43

Reporte de consulta de Nmap.



Nota. En la figura se muestra el reporte de consulta de Nmap.

Resultados obtenidos:

- Host is up (0.0039s latency): El sistema con la dirección IP 192.168.100.80 está activo y responde en la red. La latencia extremadamente baja (0.0039 segundos) confirma que el dispositivo está en la misma subred local, lo que permite una comunicación rápida.
- All 1000 scanned ports on 192.168.100.80 are in ignored states: Los 1000 puertos escaneados no mostraron ningún servicio accesible o respuesta. Los estados de estos puertos son "ignorados", lo que generalmente significa que no se pudo obtener información sobre ellos o que no se permiten conexiones externas.
- Not shown: 1000 filtered tcp ports (no-response): El estado "filtered" indica que los paquetes enviados por Nmap no recibieron una respuesta definitiva (ni aceptación ni rechazo explícito), lo que sugiere la presencia de un firewall o dispositivo de seguridad bloqueando el tráfico hacia esos puertos. El mensaje "no-response" indica que los paquetes no llegaron al destino o fueron bloqueados antes de llegar.
- Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds: El escaneo de la IP 192.168.100.80 fue completado exitosamente en 4.22 segundos, y 1 host fue identificado como activo.

E. Gerencia de Recaudación y Administración Tributaria computadora 2

El objetivo principal de este análisis fue identificar vulnerabilidades y evaluar el nivel de

exposición a posibles amenazas en los sistemas informáticos.

Figura 44

Reporte de consulta de Nmap.

Nota. En la figura se muestra el reporte de consulta de Nmap.

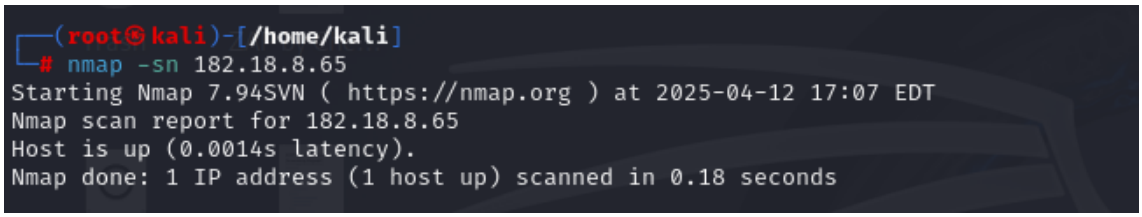
Resultados obtenidos:

- Host is up (0.0066s latency): El sistema con la dirección IP 192.168.100.86 está activo y responde en la red. La latencia extremadamente baja (0.0066 segundos) confirma que la comunicación entre el dispositivo y la máquina que ejecuta el escaneo es rápida y que están en la misma subred local.
- All 1000 scanned ports on 192.168.100.86 are in ignored states: Los 1000 puertos escaneados no mostraron ningún servicio accesible o respuesta. Los estados de estos puertos son "ignorados", lo que sugiere que no se obtuvo ninguna información sobre esos puertos, probablemente porque no están abiertos o no permiten conexiones externas.
- Not shown: 1000 filtered tcp ports (no-response): El estado "filtered" indica que los paquetes enviados por Nmap no recibieron una respuesta definitiva (ni aceptación ni rechazo explícito). Esto sugiere que un firewall o dispositivo de seguridad está bloqueando el tráfico hacia esos puertos, lo que impide que Nmap reciba respuestas. El mensaje "no-response" indica que los paquetes no llegaron al destino o fueron bloqueados antes de llegar a los puertos solicitados.
- Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds: El escaneo de la IP 192.168.100.86 fue completado exitosamente en 4.21 segundos, y 1 host fue identificado como activo.

4.3.3. Reconocimiento de la Red de los Sistemas Informáticos de la Municipalidad Distrital de San Juan Bautista.

El reconocimiento de la red es una etapa crítica en la evaluación de la seguridad, que consiste en identificar y mapear la infraestructura de red de una organización. En esta fase, se utiliza la herramienta Nmap para escanear direcciones ip y puertos, con el fin de detectar servicios activos y configuraciones vulnerables. En el caso de la Municipalidad Distrital de San Juan Bautista, el reconocimiento de la red se realizó específicamente para identificar equipos y sistemas que tuvieran protocolos abiertos, como el ftp, lo que podría representar un riesgo si no están correctamente asegurados.

4.3.3.1. Identificación de la Red con Protocolo FTP Abierto



Nmap scan report for 182.18.8.65: Informa que Nmap está escaneando la dirección IP 182.18.8.65.

Host is up (0.0014s latency): Significa que el host con la IP 182.18.8.65 está activo y ha respondido al "ping" enviado por Nmap. La latencia de respuesta fue de 0.0014 segundos, lo que indica una respuesta rápida.

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds: El escaneo ha terminado, y se ha escaneado 1 dirección IP (la de 182.18.8.65) en 0.18 segundos, y se ha confirmado que el host está activo y protocolo ftp abierto.

4.4.Fase IV: Pruebas de ejecución

4.4.1. Análisis de Vulnerabilidades de XSS.

Se llevó a cabo una ejecucion de vulnerabilidades de Cross-Site Scripting (XSS) en la página web de la Municipalidad de San Juan Bautista utilizando la herramienta BeEF (Browser Exploitation Framework).

A. Variaciones del Payload en la URL

Durante la evaluación, se identificó que la aplicación acepta parámetros en la

URL, lo que permitió realizar pruebas con diferentes variaciones de payloads para verificar la ejecución de JavaScript en el navegador.

B. Inyección de Script Básico

Se intentó ejecutar un script simple para evaluar si la aplicación reflejaba contenido sin sanitización:

https://www.munisanjuanbautista.gob.pe/website/?q=<script>alert('XSS')</script>

Figura 45

Portal de la municipalidad de San Juan Bautista.

Nota. Tomado de https://www.munisanjuanbautista.gob.pe/website/

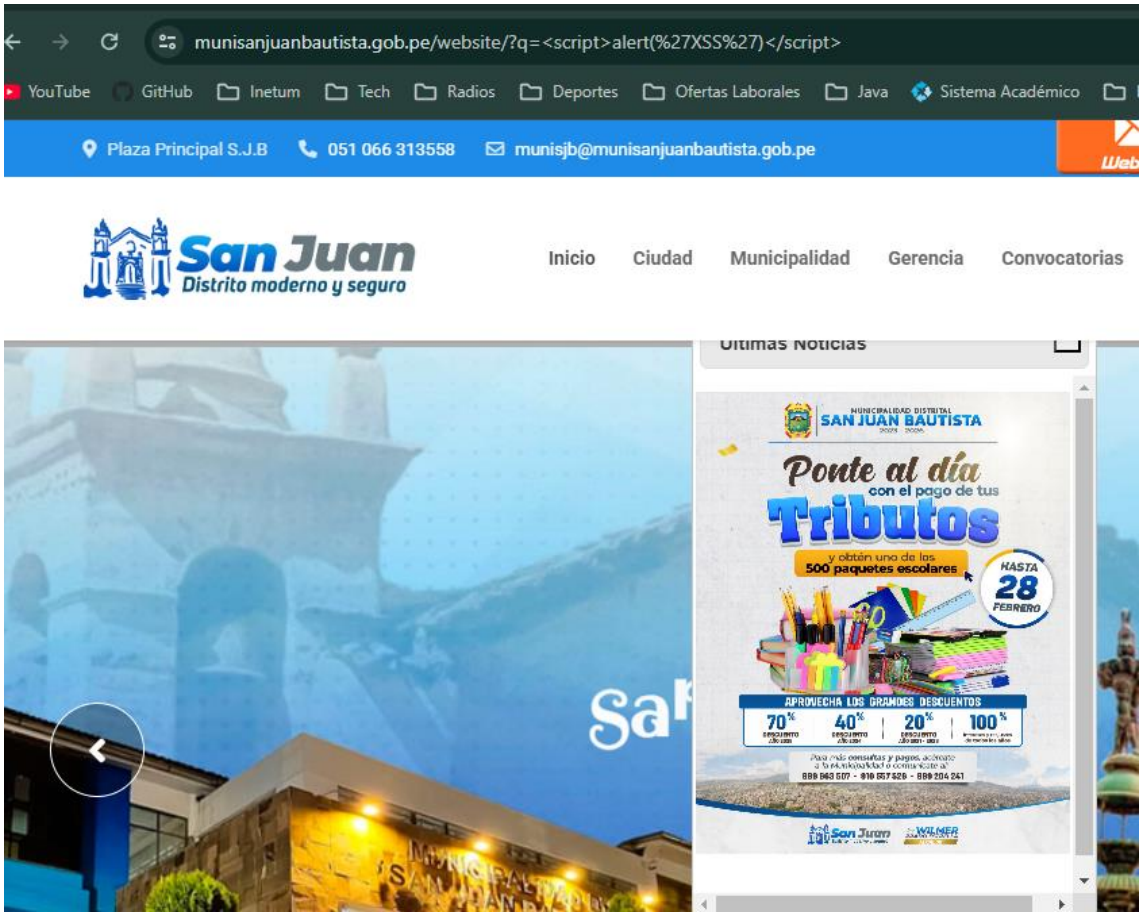
C. Codificación de Caracteres

Algunas aplicaciones bloquean <script>, pero puedes intentar codificarlo:

https://www.munisanjuanbautista.gob.pe/website/?q=%3Cscript%3Ealert(%27XSS%27)%3C/script%3E

Figura 46

Página web de la municipalidad de San Juan Bautista.



Nota. Tomado de https://www.munisanjuanbautista.gob.pe/website/

D. Event Handlers

Se probaron payloads que ejecutan código JavaScript mediante eventos en imágenes y elementos SVG:

- https://www.munisanjuanbautista.gob.pe/website/?q=<img src=x onerror=alert('XSS')>
- https://www.munisanjuanbautista.gob.pe/website/?q=<svg onload=alert('XSS')>

Figura 47

Página web de la municipalidad de San Juan Bautista.

Nota. Tomado de https://www.munisanjuanbautista.gob.pe/website/

E. Inyección en Atributos HTML

Si la aplicación permite la inyección de atributos en elementos HTML, se intentaron los siguientes métodos:https://www.munisanjuanbautista.gob.pe/website/?q=<ahref="javascript:alert('XSS')">Click aquí

- https://www.munisanjuanbautista.gob.pe/website/?q=" onmouseover="alert('XSS')".

Figura 48

Página web de la municipalidad de San Juan Bautista.

Nota. Tomado de https://www.munisanjuanbautista.gob.pe/website/

4.4.2. Vulnerabilidades de SQL Injection a la Página Web de la Municipalidad de San Juan Bautista

Se evaluó la posible existencia de SQL Injection (SQLi) en la página web de la Municipalidad de San Juan Bautista mediante herramientas automatizadas y técnicas manuales.

4.4.1.1. El servidor Responde con un Código 403 (Forbidden)

Durante el análisis de seguridad, se identificó que el servidor de la página web de la Municipalidad Distrital de San Juan Bautista responde con un código 403 (Forbidden) a ciertas solicitudes. Este código HTTP indica que el servidor está bloqueando o denegando el acceso a los recursos solicitados, lo que sugiere que existen mecanismos de protección implementados en el servidor. Las posibles medidas de seguridad que podrían estar en

funcionamiento incluyen:

- **Firewall de Aplicación Web (WAF):** Un WAF podría estar configurado para bloquear solicitudes sospechosas, como aquellas que contienen patrones que indican intentos de explotación de vulnerabilidades, como en el caso de un ataque de SQL Injection (SQLi).
- **Reglas de bloqueo de patrones sospechosos en el servidor:** El servidor podría estar configurado para identificar y bloquear patrones inusuales en las solicitudes, como secuencias de comandos o parámetros de entrada que podrían utilizarse en ataques.

4.4.1.2. Evaluación del Parámetro id

- SQLMap verificó si id=1 afecta la respuesta del servidor, pero no detectó cambios significativos.
- Esto sugiere que la aplicación podría estar manejando las consultas de manera segura o filtrando valores inesperados.
- sqlmap -u "https://www.munisanjuanbautista.gob.pe/website/?id=1" --dbs

4.4.1.3. No Se Detectó Inyección SQL en los Métodos Probados

Se probaron múltiples técnicas de sql injection:

- Boolean-based blind
- Error-based
- Stacked queries
- Time-based blind
- Union-based
- Ninguna de ellas funcionó, lo que indica que la aplicación probablemente tiene medidas de seguridad implementadas.

4.4.1.4. Vulnerabilidades de SQL Injection y su Nivel de Prueba en la Página Web de la Municipalidad Distrital de San Juan Bautista.

Código HTTP 403 (Forbidden):

- El servidor respondió con el código 403 a múltiples solicitudes, lo que indica un mecanismo de protección en el servidor como:
- Firewall de Aplicación Web (WAF).

- Políticas de bloqueo para solicitudes sospechosas.
- Boolean-based blind: No se encontraron indicios de inyección en las pruebas AND/OR.
- Error-based: Sin éxito en la identificación de errores de bases de datos.

4.4.3. Analisis con Beef

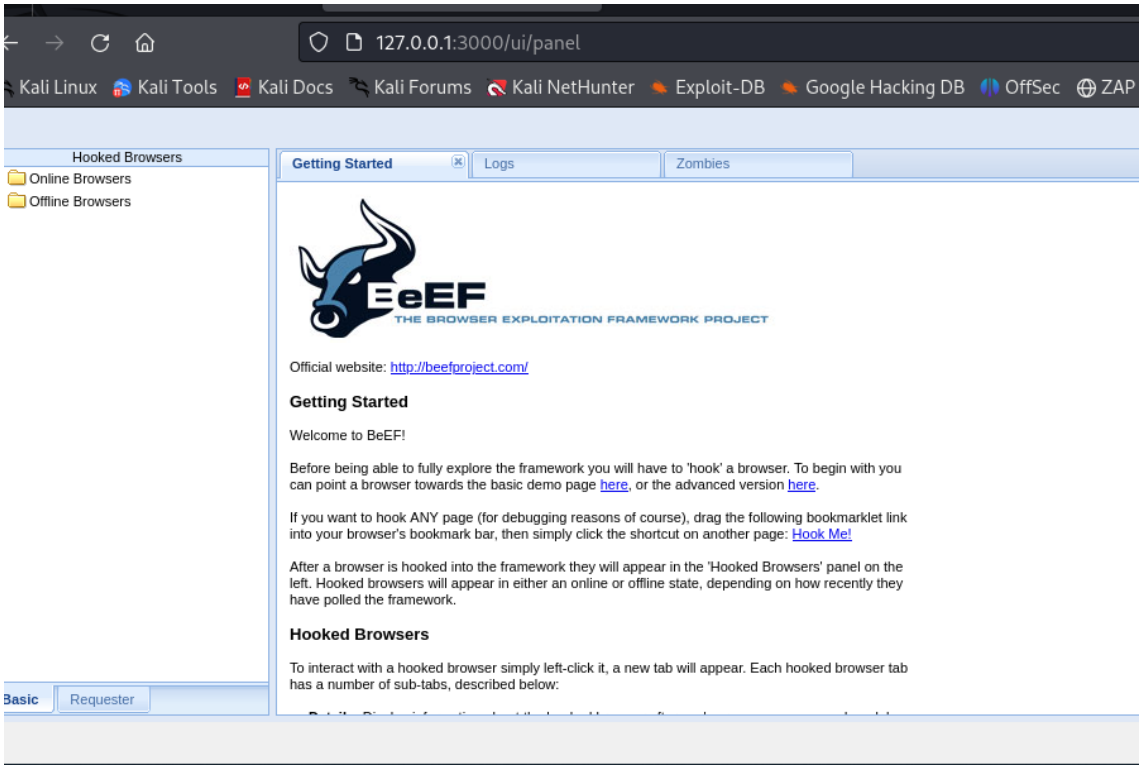
Se intentó inyectar el Hook de BeEF en la aplicación web mediante un payload XSS:

<script src="http://192.168.1.50:3000/hook.js"></script>

No se logró establecer conexión con el navegador de la víctima, lo que indica que la página web no es vulnerable a XSS reflejado ni almacenado.

Figura 49

Página web de beef.



Nota. Tomado de https://beefproject.com/

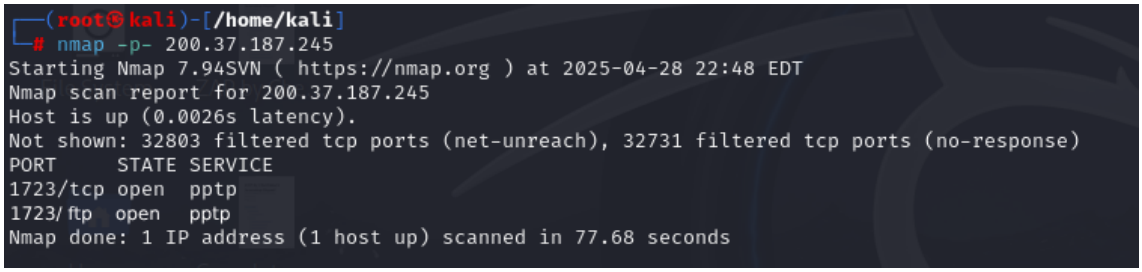
4.3.4. Exploración de Puerto FTP del router Mikrotik

Se ha identificado que el puerto 21, utilizado para el servicio FTP, está abierto en el router

MikroTik que forma parte de la infraestructura de red de la Municipalidad de San Juan Bautista, computadora de la oficina TIC.

Figura 50

Identificación de puerto FTP



Nota. Elaboración propia

Al realizar el análisis del puerto 21, se identificaron diversas carpetas que están disponibles en la red compartida a lo largo de toda la infraestructura de la Municipalidad de San Juan Bautista.

Figura 51

Explorando archivos de la red

Nota. Elaboración propia.

4.4.4. Análisis de vulnerabilidades de equipos informáticos con Nmap.

A través de este análisis, se logró acceder a la computadora de la Oficina de Recursos Humanos, donde se obtuvo acceso a todos los archivos almacenados en el equipo, así como a las carpetas compartidas en la red. En este caso, se evaluó específicamente el protocolo FTP, comúnmente utilizado para compartir archivos en la red, lo que permitió exponer la vulnerabilidad de acceso no autorizado a información confidencial.

Figura 52

Archivos confidenciales en la carpeta compartida

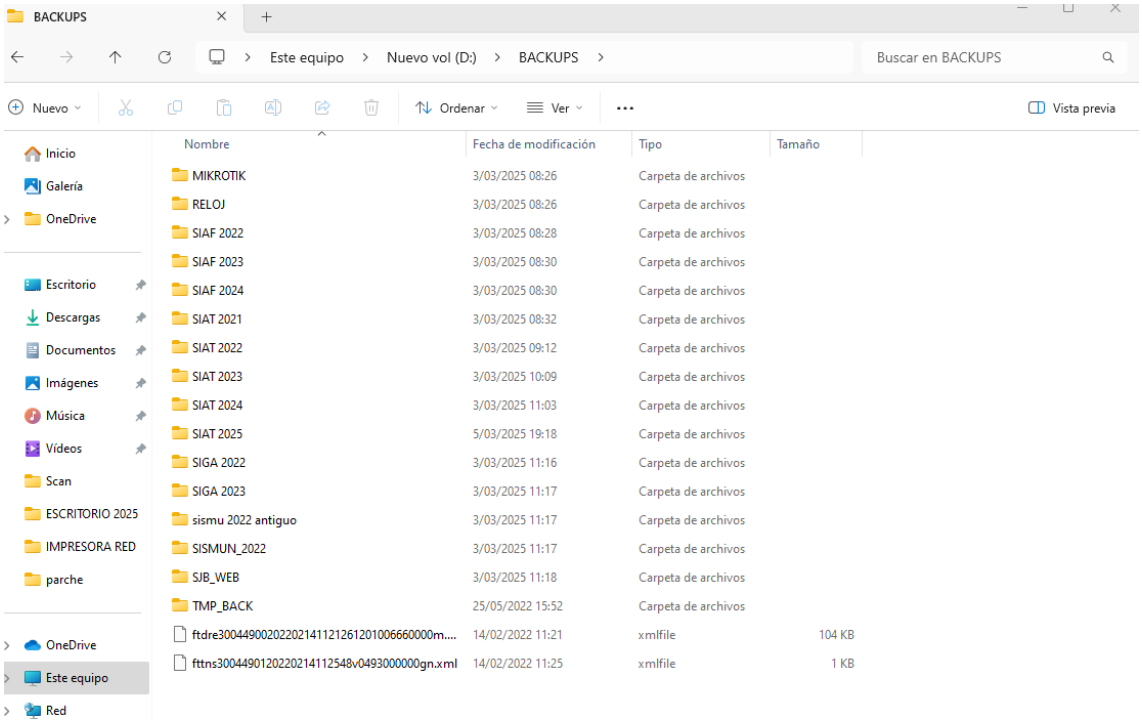
Nota. Elaboración propia

4.4.5. Explotación de la computadora de Recursos Humanos.

El acceso a estas carpetas demuestra que la computadora de Recursos Humanos está interconectada en la red, sin las medidas de seguridad adecuadas, lo que permite la exposición de información confidencial. La presencia de archivos de respaldo en la computadora, como los de SIAF, sugiere que podrían contener registros históricos de datos importantes de los empleados o actividades municipales. Sin las restricciones necesarias para evitar accesos no autorizados, esta información está en riesgo de ser explotada.

Figura 53

Carpeta Backups de la Oficina Recursos Humanos.



Nota: Elaboración propia

Figura 54

Archivo bloc de notas con datos confidenciales.

Nota: Elaboración propia

Se obtuvo acceso a un archivo de bloc de notas que almacenaba información confidencial, incluyendo nombres de usuario y contraseñas de sistemas internos. Este archivo, al no contar con medidas de protección adecuadas, expuso datos críticos que podrían ser utilizados para comprometer la seguridad de los sistemas y acceder de manera no autorizada a recursos sensibles de la Municipalidad Distrital de San Juan Bautista.

4.4.6. Explotación de la Red para Acceso no Autorizado a Recursos Compartidos debido a la Falta de Seguridad.

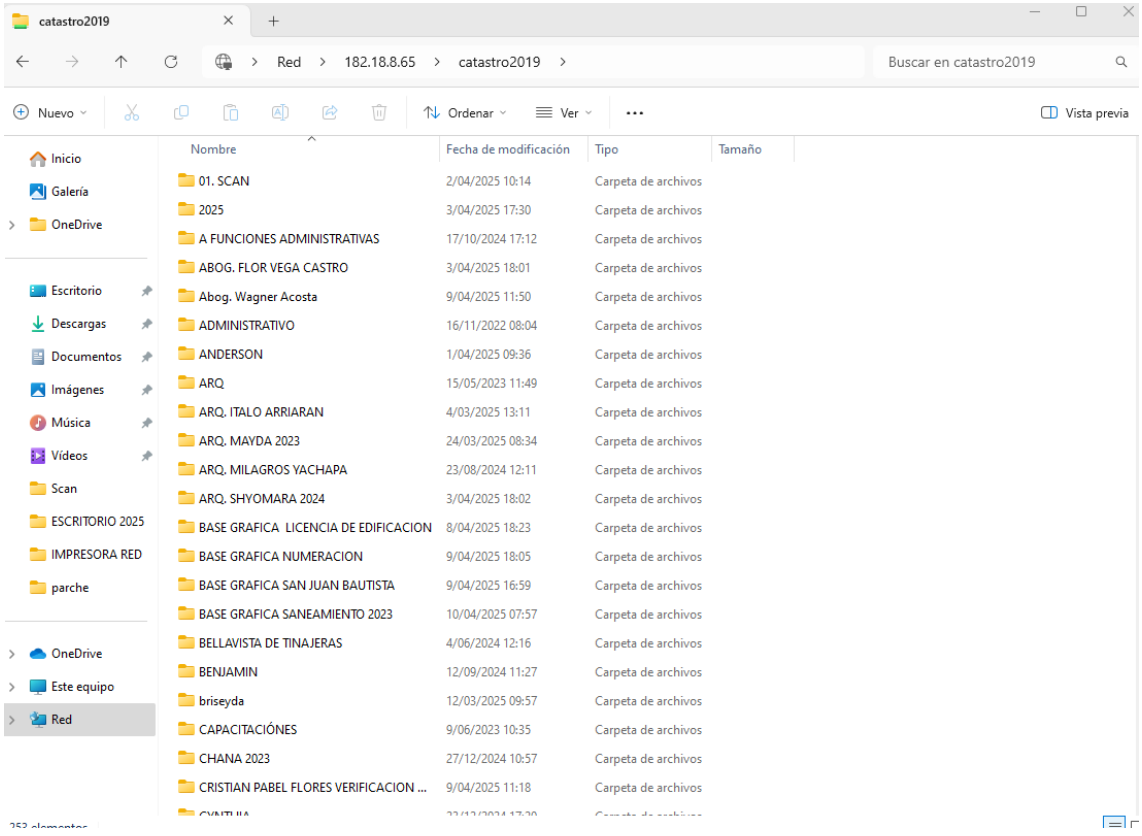
Como resultado de la explotación realizada desde la computadora de la Oficina de Recursos Humanos, se obtuvo acceso a los archivos confidenciales de la Municipalidad Distrital de San Juan Bautista. Este acceso permitió visualizar los documentos compartidos entre las oficinas interconectadas, exponiendo información sensible que debe estar protegida adecuadamente para asegurar su confidencialidad y seguridad. Durante la explotación, se identificaron diversas carpetas compartidas en la red de la Municipalidad. Como parte de la prueba, se accedió a una de estas carpetas compartidas, obteniendo información crítica sin las medidas de seguridad necesarias para evitar accesos no autorizados

A. Carpeta Compartida de la Oficina Catastro

Se identifican en el archivo compartido carpetas de gran relevancia pertenecientes a la Oficina de Catastro de la Municipalidad.

Figura 55

Carpeta compartida de la Oficina Catastro.



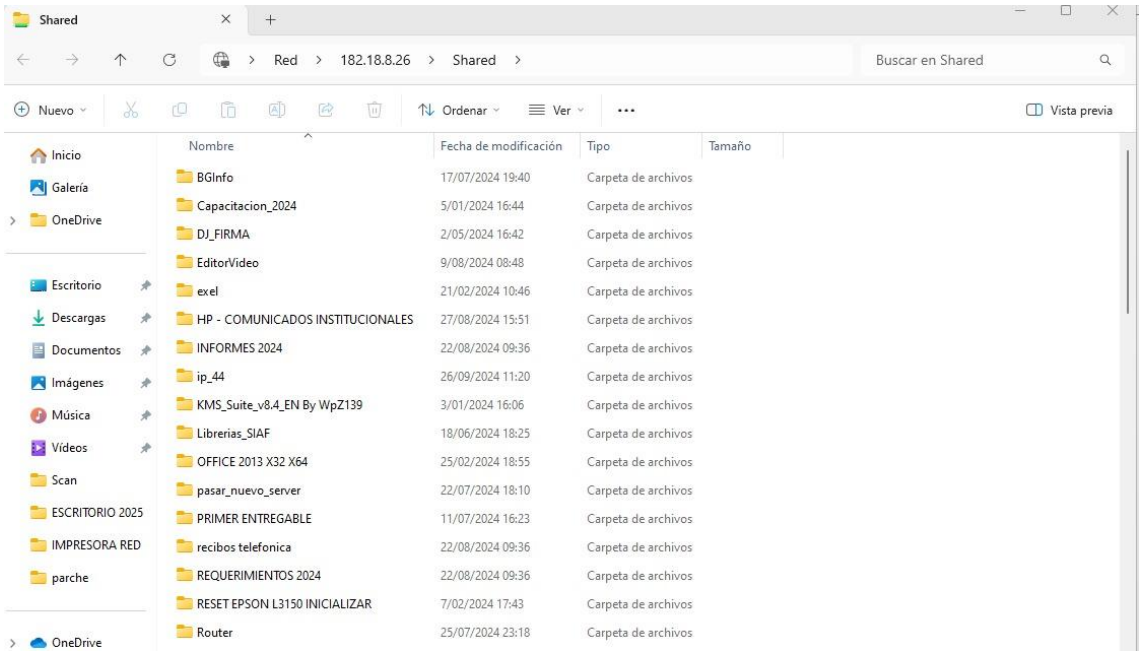
Nota: Elaboración propia

B. Carpeta Compartida de la Oficina Logística

Se identifican en el archivo compartido carpetas de gran relevancia pertenecientes a la Oficina de Logística de la Municipalidad.

Figura 56

Carpeta compartida de la Oficina TIC



Nota: Elaboración propia

4.5.Fase V: Elaboración del informe y documentación

Este procedimiento se basó en la metodología NIST SP 800-115, combinada con herramientas avanzadas de Hacking Ético, como Kali Linux (sistema operativo principal), y aplicaciones especializadas como Shodan, BuiltWith, Google Dorks, Nmap, Nslookup, Netcraft, BeEF, Forbidden, OWASP ZAP, Nikto y Burp Suite. Este enfoque integral garantizó un análisis estructurado y efectivo de la infraestructura tecnológica de la Municipalidad Distrital de San Juan Bautista, permitiendo la identificación de vulnerabilidades en sus sistemas informáticos. La metodología NIST SP 800-115 proporcionó un marco claro para la ejecución de pruebas de penetración, asegurando que el proceso se llevara a cabo de manera sistemática, controlada y ética, con el objetivo de evaluar la seguridad de los sistemas de la municipalidad y proponer medidas correctivas fundamentadas en los resultados obtenidos.

4.6.1. Revisión preliminar:

4.6.1.1. Revisión de la infraestructura de seguridad, configuraciones de red y protocolos empleados

En este proceso, se llevó a cabo un análisis exhaustivo de la infraestructura tecnológica de la Municipalidad Distrital de San Juan Bautista. Se revisaron configuraciones críticas en su red y los protocolos empleados para asegurar la protección de los sistemas informáticos. Durante el análisis, se utilizó la metodología NIST SP 800-115 y herramientas avanzadas como Nmap, OWASP ZAP y Nikto para realizar una evaluación de vulnerabilidades, observando aspectos como puertos abiertos, servicios activos y configuraciones de seguridad.

4.6.1.2. Identificación de los activos más críticos de la red y las aplicaciones a analizar

Se identificaron los recursos clave que componen la infraestructura tecnológica de la municipalidad, un servidor web, equipos informáticos (computadoras personales y laptops) y redes gestionadas con dispositivos MikroTik. Se priorizaron las aplicaciones y servicios expuestos en la red para el análisis de vulnerabilidades, identificando aquellos que representan un mayor riesgo si no se aseguran adecuadamente.

4.6.1.3. Identificación de equipos informáticos en cada gerencia

Durante la evaluación, se detalló el inventario de equipos informáticos pertenecientes a las diferentes gerencias de la municipalidad. Estos equipos, que incluyen computadoras de la Oficina de Gestión de Recursos Humanos, Gerencia de Recaudación y Administración Tributaria, y la Oficina TIC, fueron sometidos a un análisis profundo. Se utilizó Nmap para detectar vulnerabilidades en sus configuraciones de red y en los servicios expuestos, como el protocolo FTP y los puertos de red.

4.6.2. Análisis automatizado:

Se emplearon herramientas especializadas como OWASP ZAP, Burp Suite, Nikto, Nmap y Nikto para realizar un escaneo exhaustivo de la infraestructura web y de red de la Municipalidad Distrital de San Juan Bautista. Estas herramientas permitieron un análisis detallado de la aplicación web, identificando vulnerabilidades comunes como inyecciones de código, configuraciones inseguras y otros vectores de ataque típicos en aplicaciones web. Adicionalmente, se utilizó Nmap y Nikto para detectar puertos abiertos,

servicios activos y configuraciones erróneas en dispositivos de red, específicamente en los routers MikroTik, lo que permitió evaluar la exposición de la red a posibles ataques.

Los resultados obtenidos fueron recopilados y clasificados según su nivel de severidad: alto, medio y bajo. Este enfoque permitió priorizar las vulnerabilidades más críticas.

Este análisis automatizado fue fundamental para evaluar la seguridad de la infraestructura digital de la municipalidad y fortalecer su capacidad frente a ciberamenazas.

4.6.3. Análisis manual:

El análisis manual consistió en validar las vulnerabilidades detectadas por las herramientas automatizadas mediante pruebas manuales y observaciones directas en las oficinas de la Municipalidad Distrital de San Juan Bautista. Durante la visita, se identificaron múltiples debilidades de seguridad, como antivirus desactualizados, contraseñas inseguras, falta de cifrado de datos, y configuraciones incorrectas en dispositivos y redes. Este análisis permitió confirmar la existencia de fallos críticos y revelar áreas urgentes para mejorar, tales como la actualización de software, implementación de autenticación multifactor, y la adopción de políticas de seguridad más estrictas en contraseñas y acceso a información sensible.

- .

4.6.4. Resultados detallados

4.6.4.1. Clasificación de vulnerabilidades para el servidor de la página web de la municipalidad.

En esta tabla se presenta un análisis detallado de los principales riesgos de seguridad identificados en el entorno de los sistemas evaluados, junto con su nivel de severidad, frecuencia de ocurrencia y estrategias de mitigación recomendadas. Se abordan riesgos como la divulgación de información personal, la falta de protección contra ataques CSRF, la exposición de errores de aplicación, la ausencia de configuraciones adecuadas de seguridad web. La finalidad de este estudio es proporcionar una visión clara sobre las vulnerabilidades existentes y las mejores prácticas para fortalecer la seguridad de los sistemas evaluados.

Tabla 5 .

Reporte de evaluación de seguridad de la página web de la municipalidad.

Tipo de Riesgo	**Nivel de Riesgo**	**Cantidad de Alertas**	**Descripción**	**Mitigación**
Divulgación de Información Personal Identificable (PII Disclosure)	Alto	14 (63.6%)	Exposición de información personal identificable, con riesgos de privacidad y cumplimiento normativo.	- Implementar encriptación de datos sensibles.- Aplicar controles de acceso estrictos.- Realizar auditorías de seguridad periódicas.
Ausencia de Tokens Anti-CSRF	Medio	7 (31.8%)	Falta de protección contra ataques CSRF, permitiendo acciones maliciosas en nombre del usuario.	- Implementar tokens CSRF en formularios y peticiones sensibles.- Utilizar encabezados de seguridad como SameSite en cookies.
Divulgación de Errores de Aplicación (Application	Medio	58 (263.6%)	Revelación de detalles técnicos en errores,	- Configurar mensajes de error genéricos.-

Error Disclosure)			facilitando la explotación por atacantes.	Registrar detalles técnicos solo en logs del servidor.- Implementar manejo de errores adecuado.
Encabezado Content Security Policy (CSP) No Configurado	Medio	186 (845.5%)	Ausencia de CSP permite inyección de contenido malicioso como XSS.	- Configurar el encabezado Content-Security-Policy.- Restringir el origen de los recursos cargados.- Deshabilitar ejecución de scripts en línea.
Mala Configuración de Cross-Domain	Medio	2 (9.1%)	Configuración incorrecta de CORS que permite accesos no autorizados.	- Limitar los orígenes permitidos en CORS.- Evitar el uso de * como origen permitido.- Implementar autenticación y validaciones en accesos a APIs.

Nota. Elaboración propia

El análisis de riesgos destacó vulnerabilidades críticas como la divulgación de información personal identificable (PII), la falta de protección contra CSRF y la revelación de errores de la aplicación. Además, se identificaron problemas con la configuración del encabezado Content Security Policy (CSP) y una mala configuración de Cross-Domain. Las mitigaciones recomendadas incluyen encriptación de datos, implementación de tokens CSRF, manejo adecuado de errores, y restricciones en la configuración de CORS y CSP.

4.6.4.2. Clasificación de vulnerabilidades para computadoras y laptops.

Tabla 6

Vulnerabilidades de computadoras y laptops

Tipo de Riesgo	Nivel de Riesgo	Cantidad de Alertas	Descripción
Antivirus desactualizados.	Alto	1	La falta de actualización de los antivirus expone a las computadoras y laptops a virus, malware y otros ataques cibernéticos.
Contraseñas inseguras.	Alto	1	Las contraseñas inseguras, como combinaciones de nombres y números del 1 al 6, facilitan el acceso no autorizado a los sistemas.
Falta de cifrado de datos.	Alto	1	La ausencia de cifrado de datos en dispositivos y

			redes expone la información sensible a ser interceptada y robada.
Actualización de software deficiente.	Medio	1	La falta de actualizaciones regulares del software aumenta la vulnerabilidad frente a exploits de seguridad ya conocidos.
Accesos no autorizados a través de dispositivos USB	Alto	1	. El acceso a través de dispositivos USB no controlados puede permitir la entrada de malware y la exfiltración de datos sensibles.
Falta de autenticación multifactor	Alto	1	La falta de autenticación multifactor aumenta el riesgo de acceso no autorizado a sistemas, especialmente si se comprometen las contraseñas.
Acceso a información sensible por personal no autorizado	Alto	1	El acceso a información sensible por parte de personal no autorizado pone en riesgo la privacidad de los datos y puede derivar en filtraciones de información.

Configuración incorrecta de firewalls.	Alto	1	Una configuración incorrecta de los firewalls puede permitir el acceso no deseado a la red y exponer los sistemas a ataques externos.
Software no licenciado o pirata	Alto	1	El uso de software no licenciado o de dudosa procedencia puede exponer a vulnerabilidades y carecer de soporte de seguridad.
Uso de contraseñas por defecto en dispositivos IoT	Alto	1	Muchos dispositivos conectados a la red, como impresoras, vienen con contraseñas predeterminadas que no se cambian, lo que permite a los atacantes explotarlas fácilmente.
Falta de segmentación de red	Alto	1	La falta de segmentación de la red permite que un atacante obtenga acceso a sistemas críticos o sensibles con mayor facilidad.
Proveedor externo.	Alto	1	Los proveedores externos pueden ser un punto de entrada para ataques

			cibernéticos si no siguen las mejores prácticas de seguridad.
Mal manejo de permisos y roles	Alto	1	La asignación incorrecta de permisos o la falta de control sobre roles de usuarios puede resultar en accesos indebidos a datos sensibles.
Falta de protección en el puerto FTP	Alto	1	El FTP abierto en la computadora del área de Recursos Humanos permitió el acceso no autorizado a los archivos compartidos en la red, exponiendo información sensible.
Falta de formación y concientización en seguridad	Medio	1	La falta de formación en seguridad y la concientización deficiente permiten que los empleados caigan en ataques de phishing u otras amenazas.

Nota. Elaboración propia

El análisis de riesgos identificó vulnerabilidades críticas en las computadoras y laptops de la Municipalidad Distrital de San Juan Bautista, tales como la divulgación de información personal identificable (PII), la falta de protección contra malware debido a antivirus desactualizados, y la ausencia de autenticación multifactor (MFA). Además, se detectaron problemas significativos relacionados con la gestión de parches, contraseñas inseguras y accesos no autorizados, lo que incrementa la exposición a posibles ataques

cibernéticos. Estas debilidades representan riesgos altos y deben ser abordadas con urgencia para fortalecer la seguridad de la infraestructura y proteger la información sensible de la municipalidad.

4.6.4.3. Clasificación de vulnerabilidades para Router Mikrotik

Tabla 7

Vulnerabilidades de router mikrotik

Tipo de Riesgo	**Nivel de Riesgo**	**Descripción**
Falta de protección en el puerto FTP	Alto	El router MikroTik está vulnerable a ataques a través del puerto FTP abierto, lo que permite el acceso no autorizado a los archivos compartidos en la red.
Falta de Gestión de Parcheo de Software	Medio	La falta de actualizaciones en el firmware del MikroTik deja vulnerabilidades sin corregir, exponiendo el dispositivo a posibles ataques.
Falta de autenticación segura	Alto	La ausencia de configuraciones adecuadas de autenticación en servicios como FTP permite a los atacantes obtener acceso sin restricciones.

Nota. Elaboración propia

El análisis de riesgos en el router MikroTik identificó vulnerabilidades críticas, como la falta de protección en el puerto FTP y la ausencia de gestión de parches, lo que aumenta

la exposición a ataques. Además, se detectó la falta de autenticación segura, lo que permite accesos no autorizados. Estas vulnerabilidades requieren atención inmediata para fortalecer la seguridad de la red.

4.6.5. Validación con la Municipalidad

La validación de los resultados obtenidos durante la investigación se realizó en colaboración estrecha con el equipo técnico de la Municipalidad. El objetivo fue asegurar que los hallazgos fueran pertinentes y adaptados al contexto local, además de recoger información adicional que pudiera enriquecer el informe final. La Municipalidad también definió las normas y directrices para la realización del hacking ético, garantizando que las pruebas se llevaran a cabo de manera controlada, ética y con el propósito exclusivo de fortalecer la seguridad de su infraestructura tecnológica.

4.6.6.1. Presentación de los hallazgos al equipo técnico de la municipalidad:

Una vez elaborado el informe preliminar con los resultados, se convocó a una reunión con el equipo técnico de la municipalidad para presentar los hallazgos clave de la investigación. En esta reunión, se explicaron de manera clara y concisa los aspectos más relevantes y sus posibles implicaciones para la gestión pública. El objetivo de la presentación fue proporcionar una visión comprensible de los datos y conclusiones, permitiendo que el equipo técnico evaluara de forma efectiva la relevancia de los hallazgos en el contexto municipal.

4.6.6.2. Recepción de retroalimentación y ajustes al informe:

Después de la presentación, se abrió un espacio para que el equipo técnico de la municipalidad proporcionara retroalimentación sobre los hallazgos y el informe preliminar. Fue fundamental que esta retroalimentación fuera detallada, ya que ayudó a identificar áreas de mejora o ajustes que podrían haber sido necesarios para hacer los resultados más aplicables o alineados con las necesidades específicas de la municipalidad.

Fases de Evaluación y Mitigación de Vulnerabilidades en la Infraestructura Tecnológica de la Municipalidad de San Juan Bautista

En las Fases I y II de la evaluación de seguridad informática de la Municipalidad Distrital de San Juan Bautista, se estableció un análisis exhaustivo de la infraestructura tecnológica existente, utilizando la metodología NIST SP 800-115 y herramientas de Hacking Ético como Nmap, OWASP ZAP, Nikto y Shodan.

En la Fase I: Planificación, se definió el alcance del proyecto, que abarcó la evaluación de computadoras personales, laptops y una red gestionada por MikroTik, con el objetivo de identificar vulnerabilidades y proponer medidas correctivas. Además, se preparó un entorno controlado de pruebas utilizando Kali Linux y diversas herramientas especializadas para analizar la seguridad de los sistemas.

En la Fase II: Descubrimiento, se realizaron actividades de reconocimiento pasivo y activo para identificar vectores de ataque. El uso de Shodan y BuiltWith permitió obtener información sobre la página web de la municipalidad, detectando puertos abiertos como POP3 en el puerto 110. Posteriormente, el reconocimiento activo mediante Nmap reveló puertos y servicios activos en los servidores, como FTP y HTTP, lo que permitió identificar configuraciones inseguras que podrían ser explotadas por atacantes. Este análisis detallado de la infraestructura tecnológica subraya la necesidad urgente de mejorar y reforzar la seguridad en los sistemas evaluados.

En la Fase III, se realizó un escaneo exhaustivo de vulnerabilidades que reveló diversos riesgos en la infraestructura de la Municipalidad de San Juan Bautista, especialmente relacionados con puertos abiertos, servicios mal configurados y versiones de software desactualizadas. Se identificaron vulnerabilidades críticas y medias en sus aplicaciones web, como la exposición de información personal, falta de protección contra ataques CSRF, y configuraciones incorrectas que podrían permitir inyecciones de código malicioso.

En las Fases VI se ha realizado un análisis exhaustivo de las vulnerabilidades detectadas en la infraestructura y aplicaciones de la Municipalidad de San Juan Bautista. Los resultados mostraron riesgos de alto y medio nivel, tales como la divulgación de información personal, la ausencia de protección contra ataques CSRF, y configuraciones de seguridad inadecuadas. Para cada vulnerabilidad identificada, se han propuesto medidas de mitigación claras, como la implementación de encriptación, la mejora de las

configuraciones de seguridad web y la adopción de políticas estrictas de acceso y autenticación.

Capítulo V
Conclusiones y Recomendaciones

5.1. Conclusiones

A. De acuerdo con el marco metodológico establecido en el capítulo II, se logró determinar la información relevante de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, utilizando la metodología NIST SP 800-115, combinada con herramientas de Hacking Ético como Nmap, OWASP ZAP y Nikto. Como resultado, se identificaron los principales activos tecnológicos de la municipalidad, tales como servidor web, redes gestionadas por MikroTik, computadoras y laptops personales, cuyos resultados se exponen en el capítulo IV en las secciones 4.1 y 4.2. Estos activos, debido a su naturaleza sensible, requieren la implementación de medidas de seguridad adicionales para garantizar su protección frente a amenazas externas e internas, así como para asegurar la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica municipal.

B. Siguiendo el marco teórico expuesto en el Capítulo II, se procedió a la identificación y análisis de las vulnerabilidades presentes en los sistemas informáticos de la Municipalidad, utilizando procedimientos de escaneo activo y pasivo detallados en el Capítulo IV, específicamente en la Sección 4.2.1 y 4.2.2 y en la Fase III. Durante este proceso, se detectaron varias vulnerabilidades críticas, entre las que destacan la divulgación de información personal identificable (PII Disclosure), la ausencia de tokens Anti-CSRF, la divulgación de errores de aplicación, la falta de políticas de Content Security Policy (CSP) y configuraciones inseguras en servicios críticos. Los resultados de estas vulnerabilidades se presentan y detallan en las Tablas 2, 3, 4, 5,6 y 7 del Capítulo IV, proporcionando una visión clara de los riesgos identificados y las áreas que requieren intervención para mejorar la seguridad de los sistemas.

C. En función de los hallazgos obtenidos y siguiendo los lineamientos de seguridad establecidos en el Capítulo II, se identificaron las vulnerabilidades presentes en la infraestructura tecnológica de la Municipalidad Distrital de San Juan Bautista. A través de este análisis, se propusieron diversas medidas de seguridad informática

para mitigar los riesgos detectados, tales como la implementación de cifrado de datos sensibles, el refuerzo de políticas de autenticación (incluyendo el uso de MFA), la aplicación de tokens Anti-CSRF en formularios, la configuración de encabezados de seguridad en servidores web y la actualización continua de sistemas y aplicaciones. Las recomendaciones específicas para abordar estas vulnerabilidades se detallan en la Sección 5.2, con el objetivo de fortalecer la postura de seguridad de la municipalidad y reducir la exposición a posibles amenazas

5.2. Recomendaciones

5.2.1. Para la página Web de la Municipalidad

A. Divulgación de Información Personal Identificable (PII Disclosure)

Se recomienda implementar cifrado de datos sensibles, como los que contienen información personal identificable (PII), utilizando protocolos como TLS/SSL para proteger los datos en tránsito. Además, es esencial aplicar controles de acceso estrictos a las áreas sensibles de la web, implementando autenticación multifactor (MFA) y restringiendo el acceso a datos solo a usuarios autorizados. Por último, se sugiere realizar auditorías de seguridad periódicas para evaluar posibles brechas y mejorar la protección de los datos.

B. Ausencia de Tokens Anti-CSRF

Se recomienda implementar tokens Anti-CSRF en todos los formularios y peticiones sensibles para prevenir que un atacante pueda realizar acciones no autorizadas en nombre de los usuarios. También se debe configurar el encabezado de seguridad SameSite en las cookies para prevenir el envío de cookies en solicitudes de sitios de origen cruzado (cross-site).

C. Divulgación de Errores de Aplicación (Application Error Disclosure)

Se recomienda configurar mensajes de error genéricos para evitar que los atacantes obtengan detalles sobre el sistema que podrían usar para explotar vulnerabilidades. Además, se debe registrar los detalles técnicos solo en los logs del servidor, asegurando que los errores no se filtren en la interfaz de usuario, y mejorar el manejo de errores para garantizar que no se revelen datos sensibles en las respuestas de la aplicación.

D. Encabezado Content Security Policy (CSP) No Configurado

Es esencial configurar el encabezado Content-Security-Policy (CSP) para restringir el origen de los recursos que pueden ser cargados por la web. Además, se recomienda deshabilitar la ejecución de scripts en línea, lo que ayuda a prevenir ataques de Cross-Site Scripting (XSS). Esto incrementará significativamente la protección contra la inyección de contenido malicioso.

E. Mala Configuración de Cross-Domain

Es importante limitar los orígenes permitidos en CORS (Cross-Origin Resource Sharing) para evitar que sitios no autorizados puedan interactuar con la aplicación web. Además, se debe evitar el uso de "*" como origen permitido, y asegurarse de que todas las APIs tengan mecanismos de autenticación y validación de acceso adecuados para prevenir accesos no autorizados.

5.2.2. Para las Computadoras y Laptops de la Municipalidad

A. Antivirus desactualizados

Se recomienda actualizar los antivirus en todas las computadoras y laptops, asegurando que estén configurados para realizar escaneos de seguridad periódicos y detectar amenazas emergentes.

B. Contraseñas inseguras

Es fundamental establecer políticas de contraseñas seguras que incluyan longitud mínima, complejidad y la prohibición de contraseñas predecibles como combinaciones de números y nombres. Además, se debe implementar autenticación multifactor (MFA) en todos los accesos sensibles.

C. Falta de cifrado de datos

Se recomienda implementar cifrado de datos sensibles en todos los dispositivos de la municipalidad, utilizando tecnologías como BitLocker (para Windows) para proteger la información de ser interceptada o robada.

D. Actualización de software deficiente

Es esencial mantener actualizados todos los sistemas operativos, aplicaciones y software antivirus de las computadoras y laptops. Se recomienda implementar una estrategia de gestión de parches para asegurar que se apliquen las actualizaciones de seguridad oportunas.

E. Accesos no autorizados a través de dispositivos USB

Se recomienda deshabilitar los puertos USB no necesarios y aplicar políticas estrictas de acceso USB, permitiendo solo el uso de dispositivos autorizados. Además, se deben realizar escaneos periódicos de los dispositivos USB para detectar posibles amenazas.

F. Falta de autenticación multifactor

Se debe implementar autenticación multifactor (MFA) en todos los sistemas críticos de la municipalidad para garantizar que incluso si las contraseñas se ven comprometidas, el acceso no autorizado sea bloqueado.

G. Acceso a información sensible por personal no autorizado

Es crucial implementar controles de acceso estrictos para garantizar que solo el personal autorizado tenga acceso a datos sensibles. Se recomienda el uso de políticas de acceso basado en roles (RBAC) y revisiones periódicas de los permisos otorgados.

H. Configuración incorrecta de firewalls

Se recomienda revisar y configurar correctamente los firewalls de las computadoras y laptops, asegurando que solo el tráfico necesario sea permitido y bloqueando accesos no autorizados a recursos internos.

I. Software no licenciado o pirata

Se debe implementar una política de software licenciado, prohibiendo el uso de programas no autorizados o piratas. Además, se recomienda realizar auditorías periódicas para verificar el cumplimiento de esta política.

J. Uso de contraseñas por defecto en dispositivos IoT

Es importante cambiar las contraseñas predeterminadas de todos los dispositivos IoT conectados a la red, como impresoras y cámaras de seguridad, y asegurarse de que estas contraseñas sean fuertes y únicas.

K. Falta de segmentación de red

Se recomienda segmentar la red de manera adecuada para aislar los sistemas críticos y protegerlos de accesos no autorizados. Se recomienda también revisar y fortalecer las configuraciones de firewalls y sistemas de acceso remoto para limitar las posibles brechas de seguridad.

L. Proveedor externo

Es fundamental realizar una evaluación de seguridad de todos los proveedores externos, asegurando que cumplan con las mejores prácticas de seguridad. Además, se recomienda implementar controles de acceso y auditorías para las interacciones con estos proveedores.

M. Mal manejo de permisos y roles

Se recomienda establecer un sistema de gestión adecuada de permisos basado en el principio de menor privilegio y realizar revisiones periódicas de los permisos otorgados para garantizar que solo los usuarios autorizados tengan acceso a la información sensible.

N. Recomendación para el riesgo de FTP abierto

Se recomienda cerrar el puerto FTP o, en su defecto, configurar un firewall para restringir el acceso a este puerto solo a direcciones IP autorizadas. Si es necesario mantener la funcionalidad de transferencia de archivos, se debe reemplazar FTP con protocolos más seguros como SFTP o FTPS, que proporcionan cifrado en la transferencia de archivos. Además, se deben realizar auditorías de seguridad periódicas para identificar puertos innecesarios y asegurar que no existan vulnerabilidades abiertas que puedan ser explotadas. También se sugiere monitorear el tráfico de la red para detectar intentos de acceso no autorizado.

O. Falta de formación y concientización en seguridad

Es fundamental implementar programas de capacitación en ciberseguridad para todos los empleados de la municipalidad, abarcando temas como phishing, malware, gestión de contraseñas, y el uso seguro de los sistemas. La capacitación continua reducirá el riesgo de errores humanos y mejorará la postura de seguridad organizacional.

5.2.3. Para Routers MikroTik de la Municipalidad

A. Falta de protección en el puerto FTP

Se recomienda cerrar el puerto FTP o, en su defecto, configurar un firewall para limitar el acceso a este puerto solo a direcciones IP autorizadas. Adicionalmente, se debe usar protocolos más seguros como SFTP o FTPS en lugar de FTP para proteger las transferencias de archivos.

B. Falta de Gestión de Parcheo de Software

Es fundamental actualizar el firmware del router MikroTik de manera regular, aplicando los parches de seguridad correspondientes. Se recomienda establecer un procedimiento de gestión de parches para asegurar que las vulnerabilidades conocidas sean corregidas oportunamente.

C. Falta de autenticación segura

Se recomienda configurar autenticación segura en los servicios del router MikroTik, como FTP y otros servicios de administración, mediante el uso de contraseñas fuertes y únicas. También es esencial habilitar autenticación multifactor (MFA) en los accesos a la interfaz de administración del router para fortalecer la seguridad.

5.3. Propuesta de validación de la efectividad de las medidas de mitigación

5.3.1. Evaluación de la efectividad de las medidas de mitigación:

Para asegurar que las medidas propuestas sean efectivas, se recomienda implementar un proceso de validación post-implementación que incluya las siguientes etapas:

- **Pruebas de penetración posteriores:** Después de la implementación de las medidas, realizar nuevas pruebas de penetración (pentesting) utilizando las mismas herramientas y técnicas empleadas en el análisis original. Esto permitirá verificar si las vulnerabilidades previamente identificadas han sido efectivamente mitigadas.
- **Escaneos regulares de vulnerabilidades:** Realizar escaneos regulares de vulnerabilidades utilizando herramientas como OWASP ZAP, Nikto, y Nmap para asegurar que las configuraciones de seguridad y las medidas implementadas sigan siendo efectivas frente a amenazas emergentes.
- **Monitoreo y auditorías continuas**: Implementar un sistema de monitoreo en tiempo real para detectar comportamientos anómalos o ataques que intenten explotar vulnerabilidades aún no identificadas. También, realizar auditorías periódicas de los sistemas y redes, que incluyan análisis de logs, accesos no autorizados y configuraciones de seguridad.

- **Revisión de políticas y protocolos:** Revisar y ajustar las políticas de seguridad y las reglas de firewall (WAF) basadas en los resultados de las auditorías y pruebas, asegurando que se mantengan alineadas con las mejores prácticas y las amenazas más recientes.

La investigación realizada responde al objetivo general establecido al desarrollar un proceso integral de análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista. A través de las fases de evaluación descritas en los capítulos anteriores, se utilizó la metodología NIST SP 800-115 combinada con herramientas y técnicas de Hacking Ético, como Nmap, OWASP ZAP, Nikto, y Shodan, para identificar y evaluar vulnerabilidades en los sistemas, redes y dispositivos tecnológicos de la municipalidad.

El análisis realizado permitió detectar diversas vulnerabilidades críticas, como la divulgación de información personal identificable, la ausencia de protección contra ataques CSRF, y configuraciones inseguras en servicios clave. Posteriormente, se propusieron medidas de seguridad, como la implementación de cifrado de datos sensibles, la adopción de autenticación multifactor (MFA), y el refuerzo de políticas de seguridad en aplicaciones web y sistemas internos.

Además, la investigación contribuyó al establecimiento de normativas y regulaciones en materia de seguridad informática al proponer prácticas de actualización constante de sistemas, auditorías periódicas de seguridad y capacitación en ciberseguridad para el personal de la municipalidad. Con ello, se busca minimizar los riesgos asociados a la infraestructura tecnológica existente y fortalecer su capacidad para enfrentar amenazas cibernéticas. En resumen, el proceso no solo identificó y evaluó vulnerabilidades, sino que también estableció bases sólidas para la mejora continua de la seguridad informática en la Municipalidad Distrital de San Juan Bautista.

Bibliografía

Almeyda, A., Torres, R., y Arias, A. (2016). *Análisis de vulnerabilidades: una herramienta para* Albújar, J. C. (2015). *Empresas con servicios de seguridad informática incrementan su productividad hasta en 30%*. Diario Gestión.

la protección de activos críticos. Revista de investigación Academia Journals, 10, 13-25.

Ariganello, E. (2019). *Modelo de referencia OSI. Recuperado el 11 de octubre del 2020* de https://aprenderedes.com/2019/05/modelo-de-referencia-osi/.

Bermeo, C. (2017). *Implementación de Hacking Ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Peru S.A.C., Tumbes.* Tesis de Pregrado, Perú.

Carthern, C., Wilson, W., Rivera, N., & Bedwell, R. (2015). *Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA*. Springer Science Business Media New York, EEUU.

Chávez, P. (2011). *Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergente.* Tesis de Pregrado, Escuela Politécnica Nacional, Quito, Ecuador.

Crúz, V. Y. (2017*). Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final,* 3, 505–516.

De la Torre, C. (2017). *La mayor vulnerabilidad de un sistema son los usuarios*. Ambit.com.

Digital, B. (mayo de 2017). *Metodología de Pruebas de Intrusión en la NIST SP 800-115*. Obtenido de https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebasde-intrusion-en-la-nist-sp-800-115/

Diario El Peruano (09 marzo, 2020). *Perú entre países más inseguros en línea en América Latina.* Recuperado de https://elperuano.pe/noticia-peru-entre-paisesmasinseguros-linea-america-latina-90806.aspx.

Durand, A. (2019). *Evaluación de técnicas de Ethical Hacking para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa prestadora de servicios*. Tesis de Pregrado, Universidad Señor de Sipán, Pimentel, Perú.

Easttom, C. (2014). *Network Defense and Countermeasures:* Principles and Practices, Second Edition. Pearson IT Certification.

FasesHackingEtico. (2019). Obtenido de https://ehack.info/las-fases-del-hackingetico/

FasesDelHackingÉtico. (2014). Obtenido de https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

Gontharet, F., & Testing, P. (2015). *ISSAF Methodology Analysis and Critical Evaluation.*

González, B. H. R., & Montesino, P. R. (2018). *Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web.* Revista Cubana de Ciencias Informáticas.

Gonzales, Sánchez, y Soriano. (2013). *Pentesting con Kali.* Recuperado de file:///C:/Users/LARED/Downloads/0xword-Pentesting-Con-Kali-Linux_v6.pdf.

Gómez, H. J. A. (2015*). Introducción al Hacking Ético de sistemas y redes*. Ucys, 1–39.

Gutiérrez, P. (2019). *Hacker's WhiteBook. Edición While Suit Hacking.* Monterrey, México.

HackingÉtico. (s.f.). Obtenido de https://www.internetglosario.com/1131/Hackingetico.html

Hernández, B., Baquero, y Gil, C. (2018). *Hacking ético en dispositivos móviles: consideraciones y usos prácticos.*

Hernández Sampieri, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación (6ta Ed.).* México, D.F., México: McGraw Hill Interamericana.

Hernández, B. (2001). *Técnicas estadísticas de investigación social. España:* Diaz de Santos S.A.

Hernández, R., Fernández, C., & Baptista, P. (2014*). Metodología de la investigación (6ª ed.)*. México: McGraw-Hill.

Hernández, L., & Mejía, J. (2015). *Guía de Ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web.* Recuperado de https://www.redalyc.org/articulo.oa?id=512251501005.

Huilca, N. (2012). *Hacking Ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del cantón Cevallos.* Tesis de Pregrado, Universidad Técnica de Ambato, Ecuador.

Hurtado, M., & Mendaño, L. (2016). *Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado*. Tesis de Maestría, Quito, 2016. Recuperado de: https://bibdigital.epn.edu.ec/handle/15000/16836

Joyanes, A. L. (2015). *Ciberseguridad: retos y amenazas a la seguridad nacional en el Ciberespacio.* Imprenta Del Ministerio de Defensa.

Kaspersky (2023). *Ciber Amenaza Mapa En Tiempo Real. Estadística histórica mundial.* Recuperado de https://cybermap.kaspersky.com/es/stats/#country=4&type=ids&period=w.

Kizza, J. M. (2015). *Guide to Computer Network Security (3ra Ed.).* Springer.

Kumar, S. (2018). *Ataques de piratería, métodos, técnicas y sus medidas de protección.*

Kurose, J. F., & Ross, K. W. (2017). *Redes de computadoras: un enfoque descendente basado en Internet (7ma ed.)*. Pearson.

Laudon, K. C., & Laudon, J. P. (2016). *Management Information Systems: Managing the Digital Firm (14th ed.).* Pearson.

López, A. R. (2017). *Sistema de Gestión de la Seguridad Informática*. Fundación Universitaria Del Área Andina (Bogotá). https://doi.org/978-958-5455-74-0.

López, S. R. (2015). *Propuesta de implementación de una metodología de auditoría 137 de seguridad informática.* Universidad Autónoma de Madrid, 61.

López, R. (2015). *Propuesta de implementación de una metodología de auditoría de seguridad informática.* Universidad Autónoma de Madrid. Recuperado de: https://repositorio.uam.es/handle/10486/668900

Lund, A. C. (2018). *El sudeste asiático: La región en ascenso.*

Macías, B. (2021). *Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red wifi de universidad estatal del sur de Manabí.* Tesis de Pregrado. Ecuador: Universidad Estatal del Sur de Manabí.

McNab, C. (2004). *Network Security Assessment:* Know Your Network. O'Reilly Media.

Mammar, A., Cavalli, A., & Jimenez, W. (2011). *Using testing techniques for vulnerability detection in C programs.* Testing Software and Systems, 80–96. Recuperado de http://link.springer.com/chapter/10.1007/978-3-642-24580-0_7

Medina Rojas, E. F. (s.f.). *Hacking Ético: Una herramienta para la seguridad informática.*

Mohammed M, Alani (2014*). Guide to OSI and TCP/IP Models (4ta Edición). Springer* Cham Heidelberg New York Dordrecht London.

Muñoz, J. (2016). *Seguridad Organizacional.* Recuperado de https://www.seguritecnia.es/tecnologias-y-servicios/seguridadorganizacional_20160910.html.

Niño, N. R. (2018). *Modelo de un Sistema de Gestión de Seguridad de Información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática* - INEI Filial Lambayeque. Universidad Nacional de Pedro Ruíz Gallo.

O'Reilly, T. (2005). *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software.* O'Reilly Media.

Orlando, A. (2018). *Método de inclusión de hacking ético en el proceso de testing de software.* Tesis de Maestría, Buenos Aires, Argentina.

Plinio, P. F. (2012). *Metodología para la Detección de Vulnerabilidades en Redes de Datos.* Scielo Peru.

QuéEsElHackingEtico. (s.f.). Obtenido de https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-elhacking-ético

Rahalkar, S. A. (2016*). Certified Ethical Hacker (CEH) Foundation Guide.* Edition ed. Pune.

Anexos

Anexo 1. Matriz de consistencia

Título: Análisis de vulnerabilidades de los sistemas informáticos de la municipalidad distrital de San Juan Bautista, 2024

PROBLEMA	OBJETIVO	VARIABLES	METODOLOGIA DE INVESTIGACION
PROBLEMA PRINCIPAL ¿Cuáles son los resultados del proceso de análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023? **PROBLEMAS ESPECÍFICOS** a. ¿Cuál es la información	**OBJETIVO PRINCIPAL** Desarrollar el proceso de análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023. Utilizando la metodología OWASP, herramientas y técnicas de Hacking Ético, con el propósito, de identificar, evaluar, las vulnerabilidades y proponer medidas de seguridad; y la finalidad de establecer normativas y regulaciones en materia de seguridad informática y minimizar los riesgos. **OBJETIVOS ESPECÍFICOS**	**VARIABLE DE INTERES** Análisis de vulnerabilidades **VARIABLES DESCRIPTIVAS** Recopilación de la información Identificación y análisis de vulnerabilidades Medidas de seguridad informática.	**TIPO DE INVESTIGACIÓN** • Aplicada. **NIVEL DE INVESTIGACIÓN** • Descriptiva **DISEÑO** • No experimental **POBLACIÓN** La población estuvo compuesta por los sistemas informáticos: ➢ 1 Red Mikrotik.

relevante de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023? b. ¿Cuáles son las vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista ,2023? c. ¿Cuáles son las medidas de seguridad informática para mitigar las	a. Determinar la información relevante de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023. b. Identificar y analizar las vulnerabilidades de los sistemas informáticos en la Municipalidad Distrital de San Juan Bautista, 2023. c. Plantear medidas de seguridad informática para la mitigación de vulnerabilidades en los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023.		➢ 5 Router. ➢ 6 Switch. ➢ 1 Servidor de la página web de la Municipalidad. ➢ Equipos Informáticos: o 140 computadoras personales. o 15 laptops. **MUESTRA** Se utilizó el Muestreo no probabilístico, muestreo por juicio de experto. La muestra incluyó a todos los elementos de la población objetivo. ➢ 5 computadoras personales: o 2 computadoras de la Oficina de Gestión de Recursos Humanos o 2 computadoras de Gerencia de Recaudación y Administración Tributaria o 1 computadoras de la Oficina TIC. ➢ 3 laptops: o 1 laptop de Gerencia Municipal

vulnerabilidades en los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023?			○ 2 laptops de Oficina General de Planeamiento y Presupuesto. ➢ 1 servidor de la página web. ➢ 1 red administrada con un dispositivo MikroTik. **TÉCNICA** Revisión documental automatizada **INSTRUMENTOS** ➢ Sistema Operativo Kali Linux ○ Nmap ○ Owasp Zap ○ Nikto ○ SQLMap ○ Shodan

Yo: Edgar Eusebio Sulca Contreras, Identificado con DNI: 28297611 en mi calidad de Encargado de Informática del área de Informática de Oficina de Administración y Finanzas, de la Municipalidad Distrital San Juan Bautista, con R.U.C N° 20143114911, ubicada en la ciudad de Huamanga, Departamento de Ayacucho.

OTORGO LA AUTORIZACIÓN,

Al señor Ramiro Núñez Pérez, identificado con DNI N° 44106817, Bachiller de la Universidad Nacional San Cristóbal de Huamanga, Carrera profesional Ingeniería de Sistemas, para utilice la siguiente información:

- Equipos informáticos.
- Red informática (Topología).
- Sistemas de Información (Páginas web, servidores, apps).

Con la finalidad de que pueda desarrollar su Tesis de Investigación, cuyo título es **"ANÁLISIS DE VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA, 2023".**

Trabajo de investigación profesional para optar al grado de Título Profesional.

MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA
GERENCIA DE ADMINISTRACIÓN Y FINANZAS
Edgar E. Sulca Contreras
ESPECIALISTA EN TECNOLOGÍA DE LA INFORMACIÓN (E)

Firma y sello del Representante del área

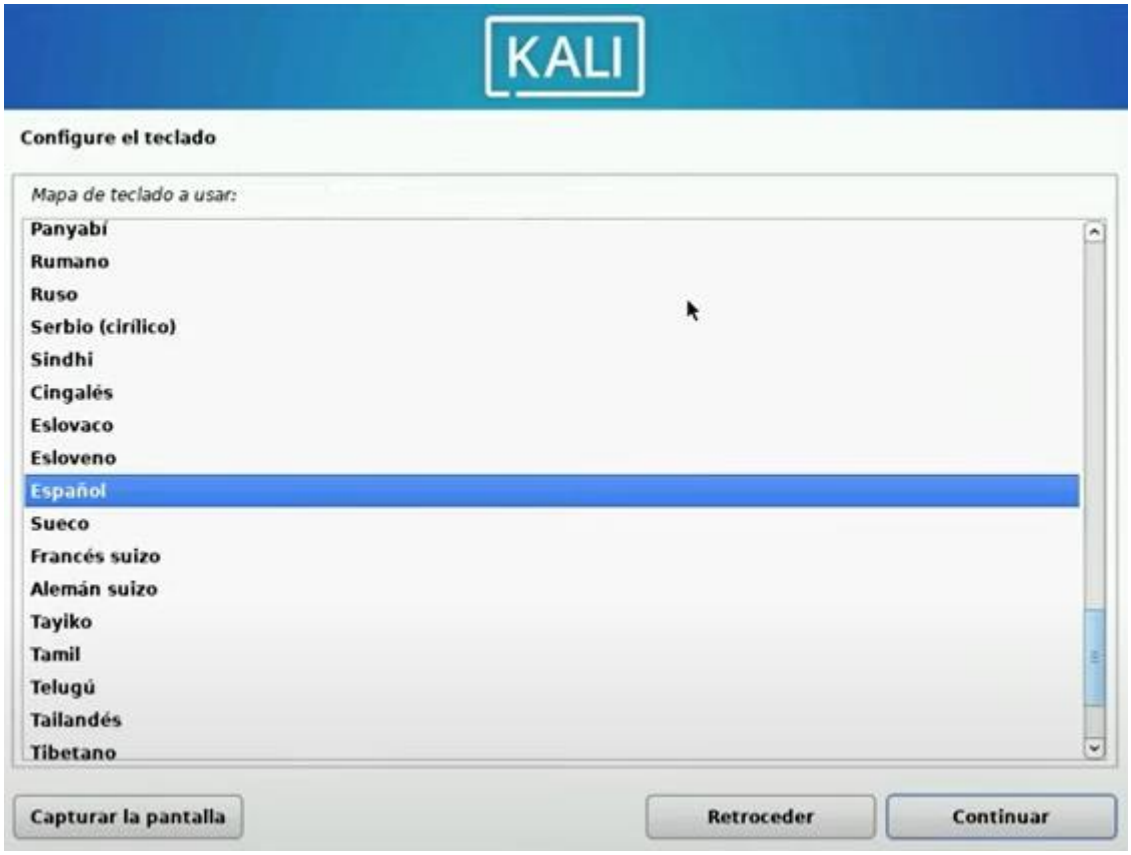
DNI: 28297611

Anexo B: Instalación de Kali Linux

Instalación de Kali Linux

Configuración del idioma del sistema español

Configuración de la ubicación o zona horaria, Perú.



Configuración el método de ingreso del teclado

Configuración el nombre del equipo

Configuración del nombre de dominio

Configuramos los usuarios y contraseña

Configuramos la contraseña

Seleccionamos la partición del disco

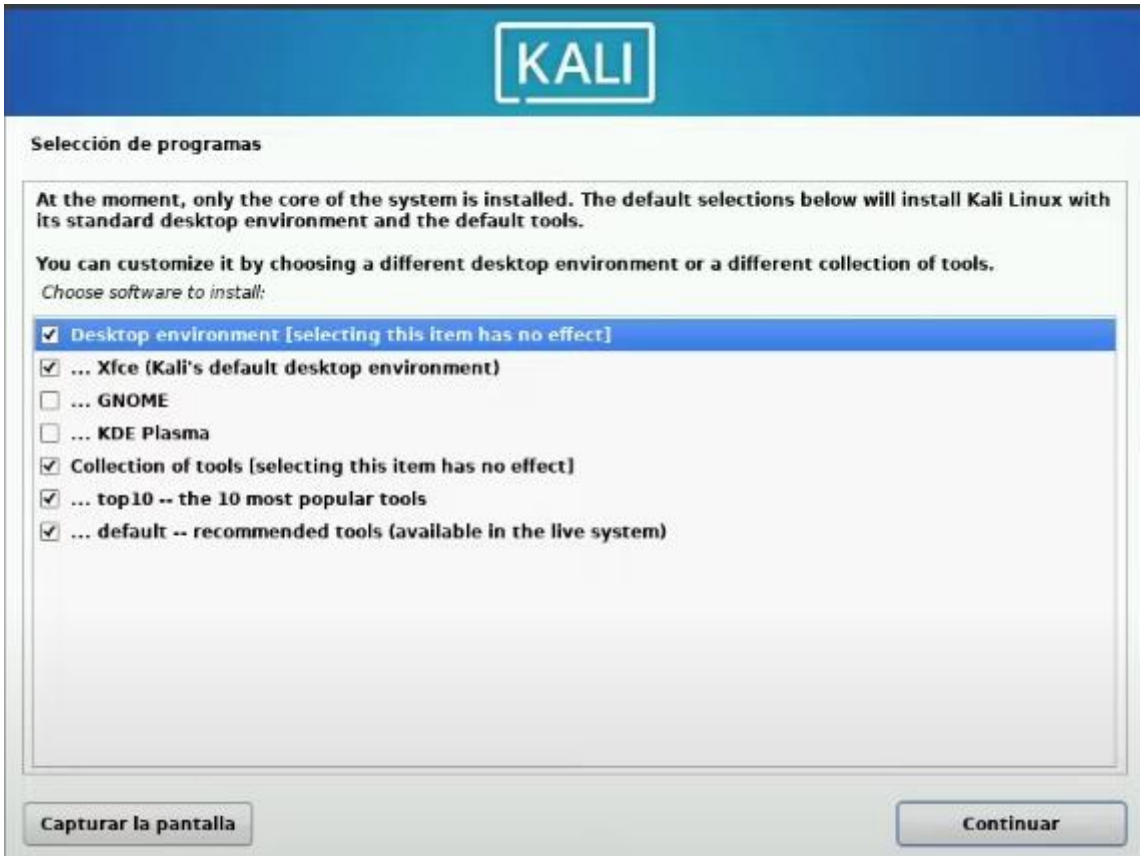
Elegimos el disco a particionar

Elegimos el Esquema del particionado

Finalización del particionado de disco

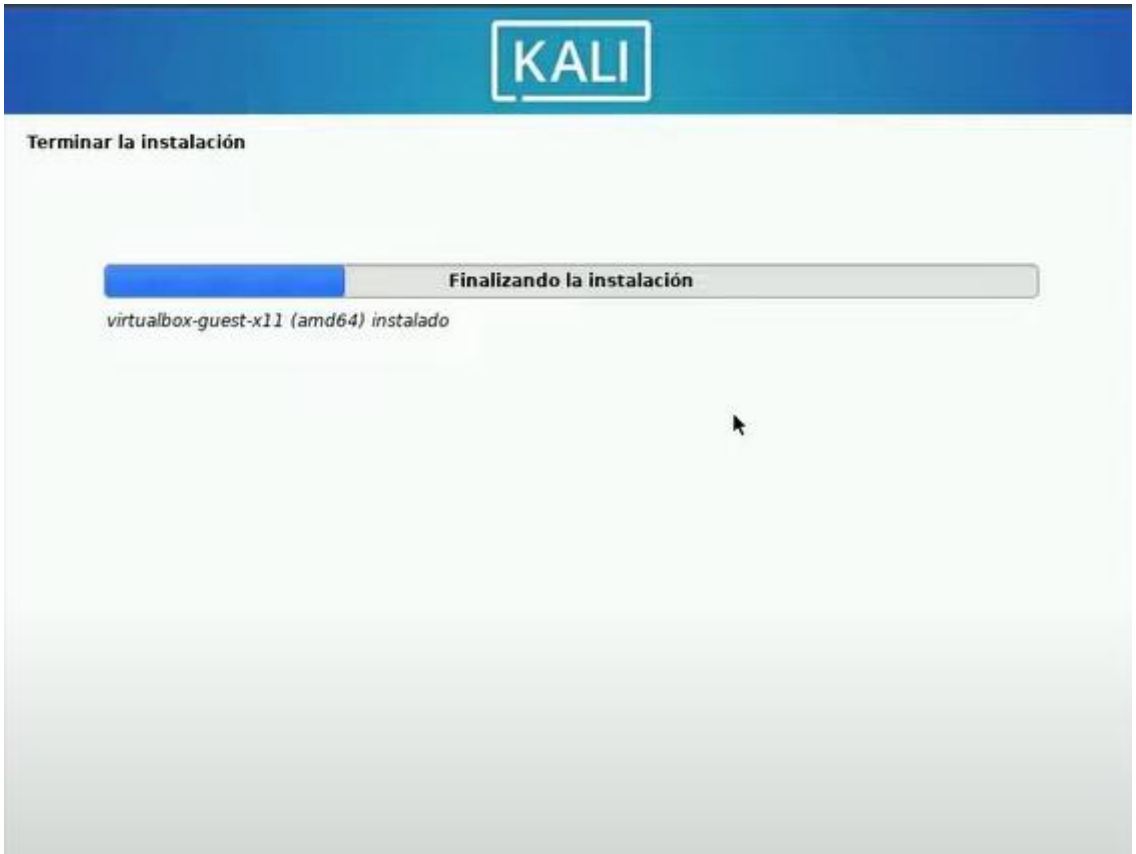
Formateamos el disco seleccionado

Seleccione programas



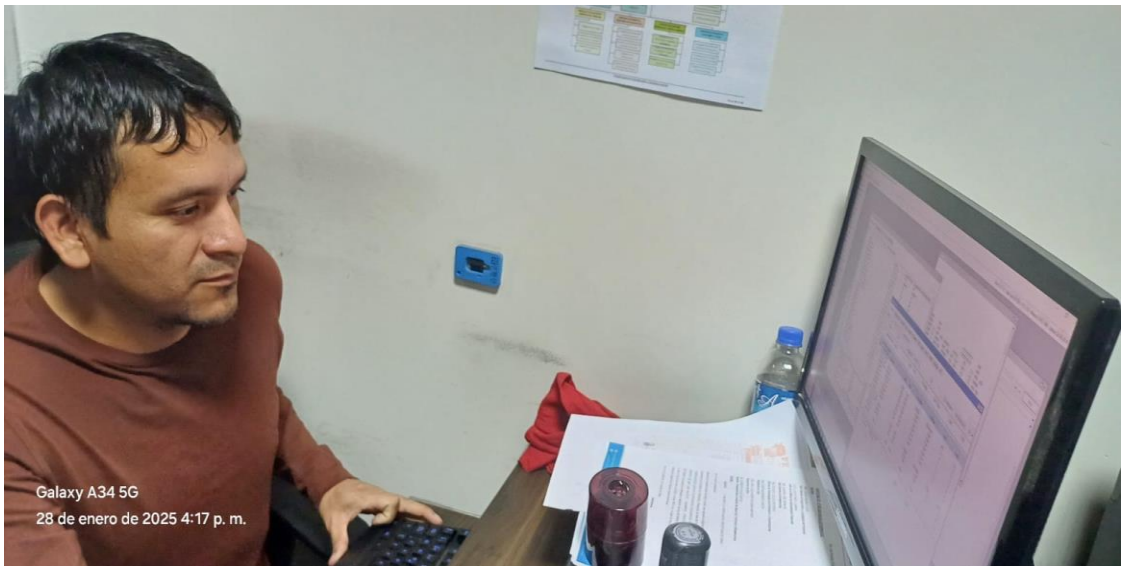
Instalador de cargador de arranque

Instalando el sistema

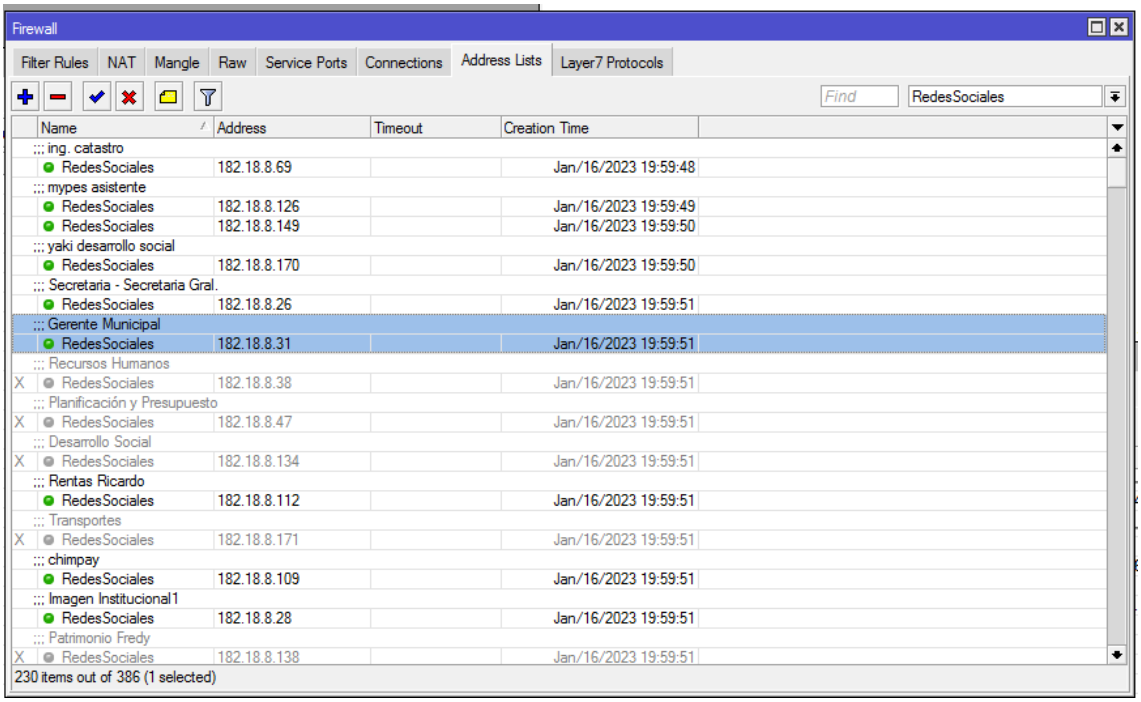


Finalización de la instalación de Kali Linux, iniciamos sesión

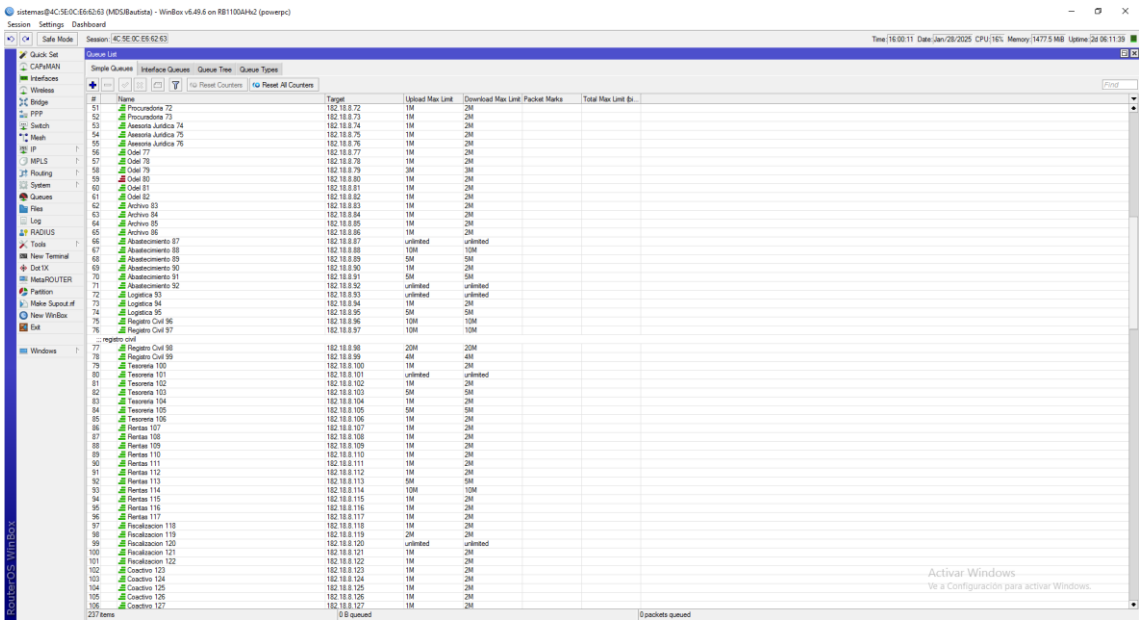
Anexo C: Evidencias Fotográficas de Acceso a MikroTik



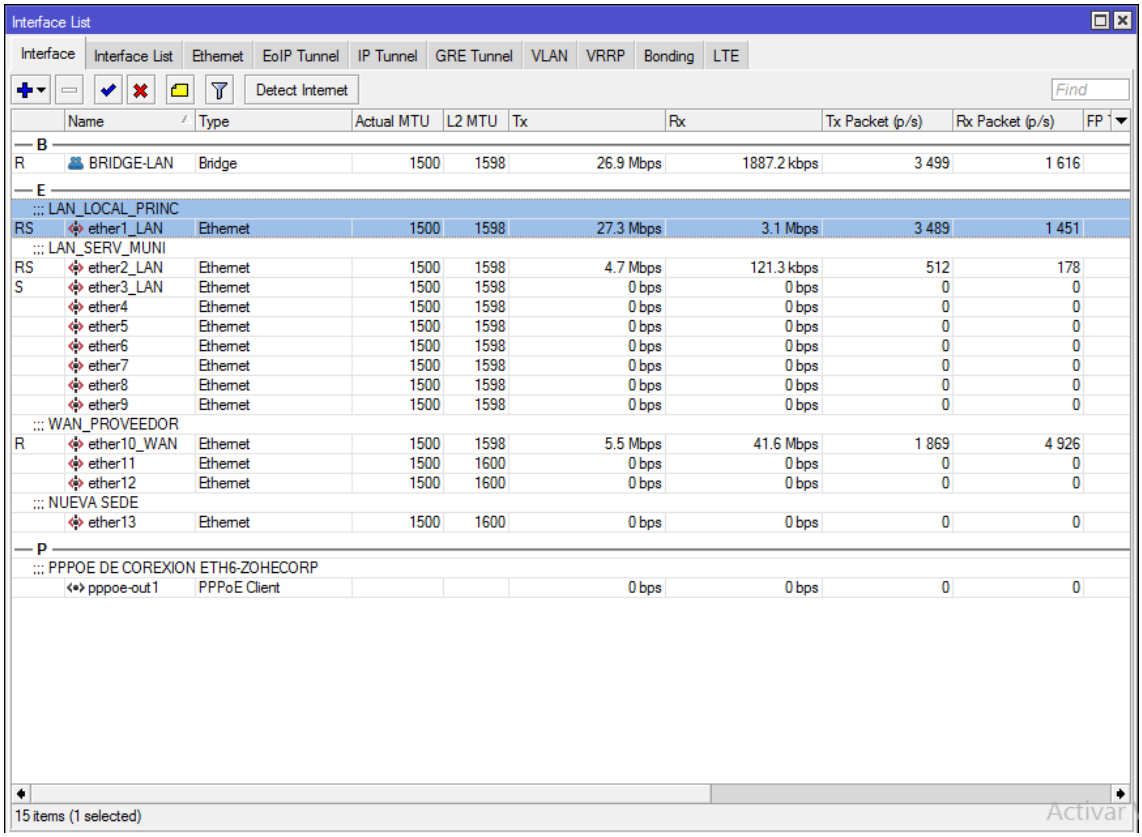
Bloqueo a redes sociales



Capacidad de internet por usuario

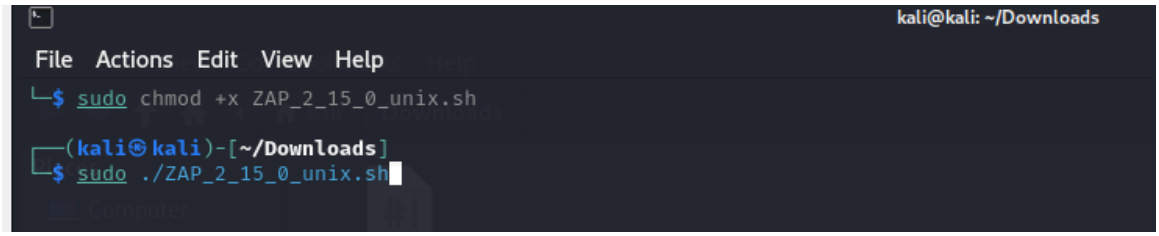


Internet por área

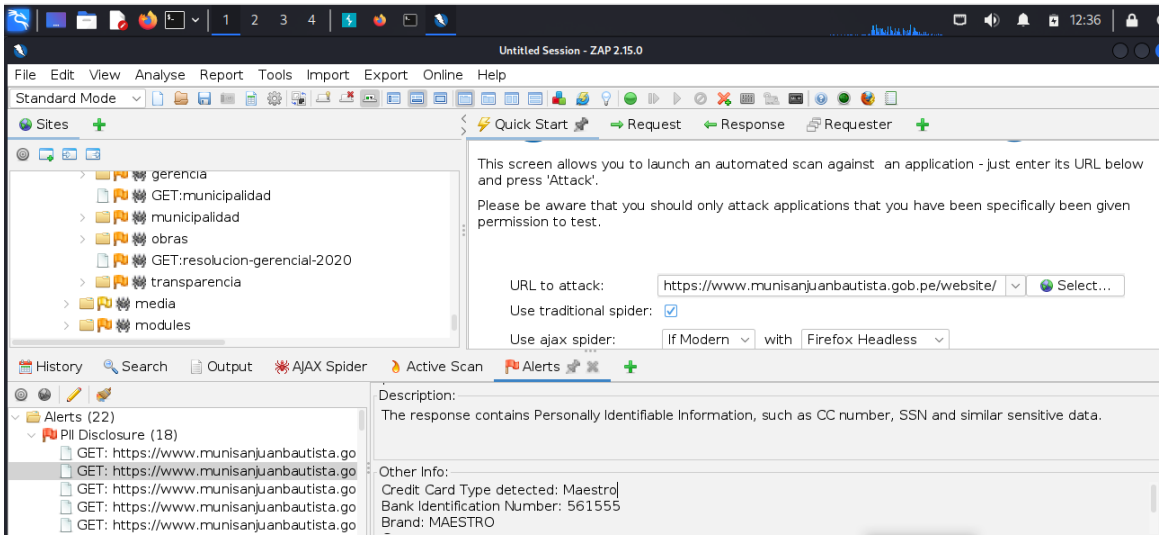


Anexo D. Pruebas de Penetración.

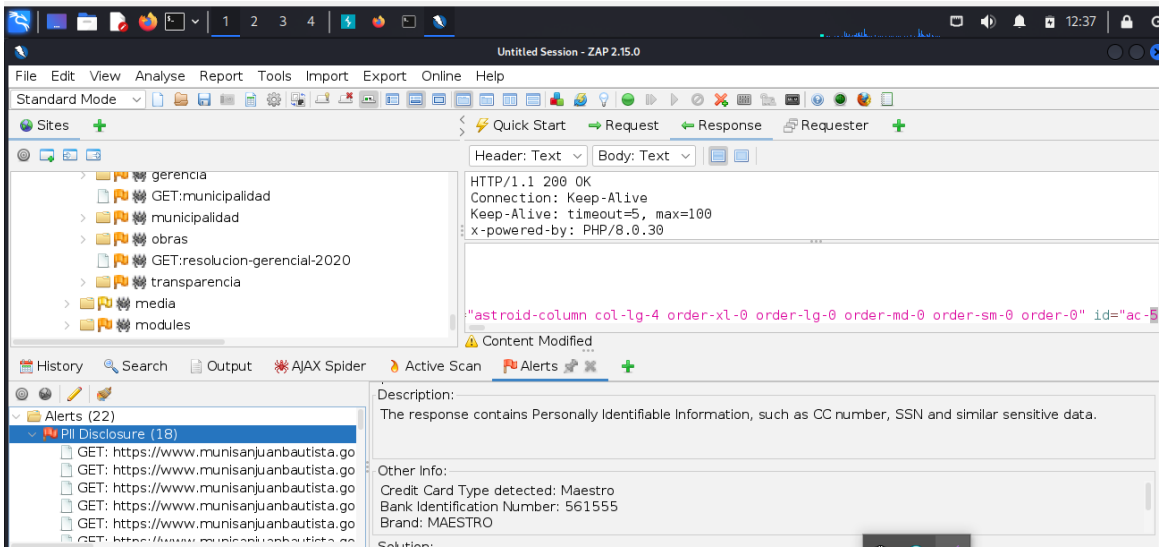
Instalación de OWASP ZAP



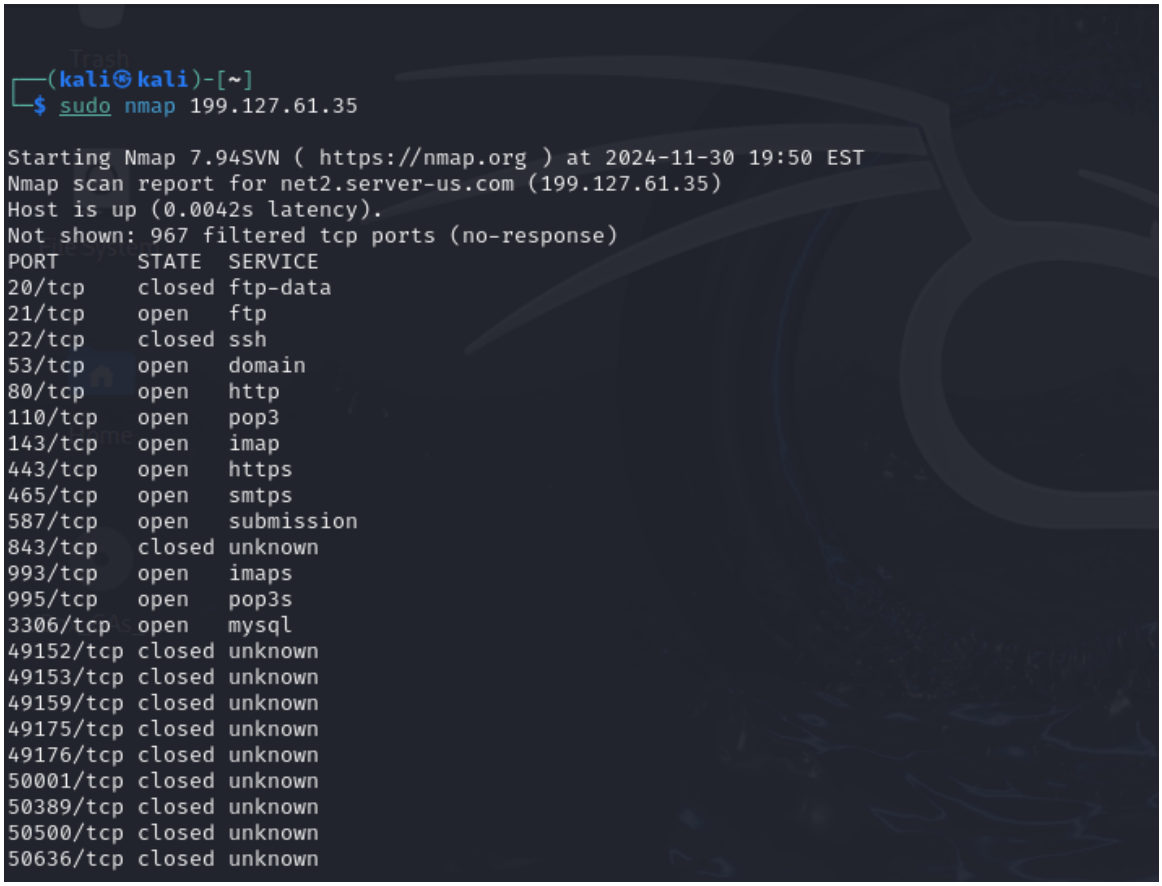
Desarrollo de haking etico con OWASP ZAP



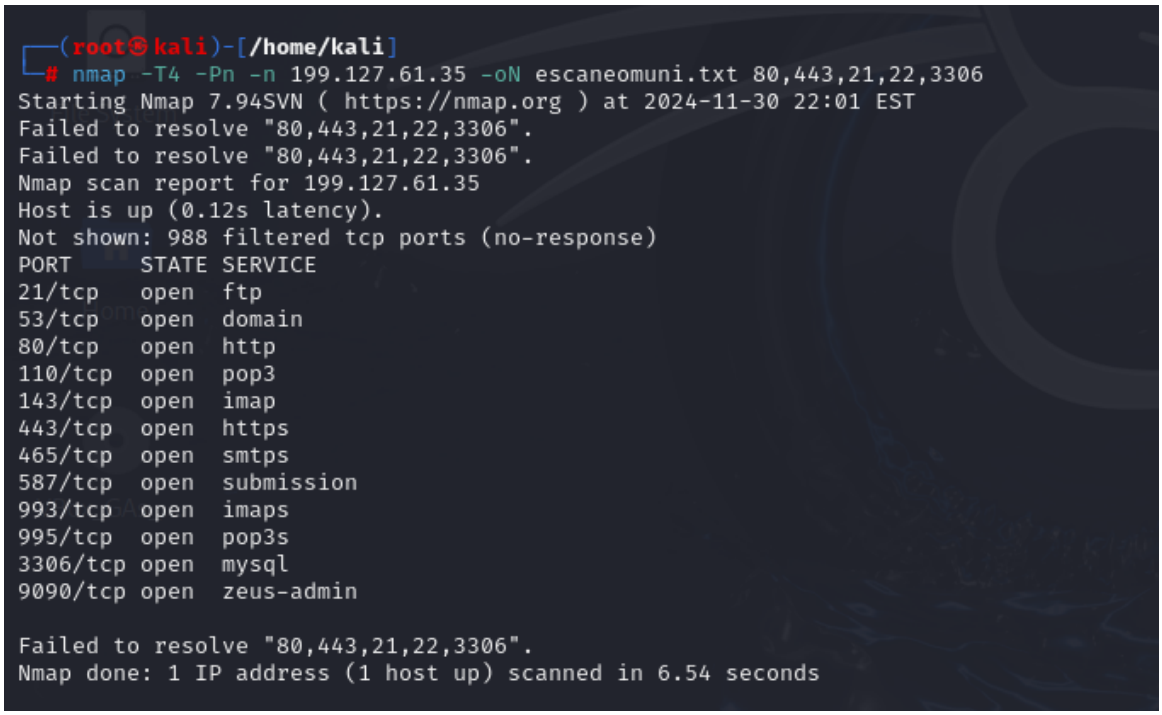
Resultado de análisis con OWASP ZAP



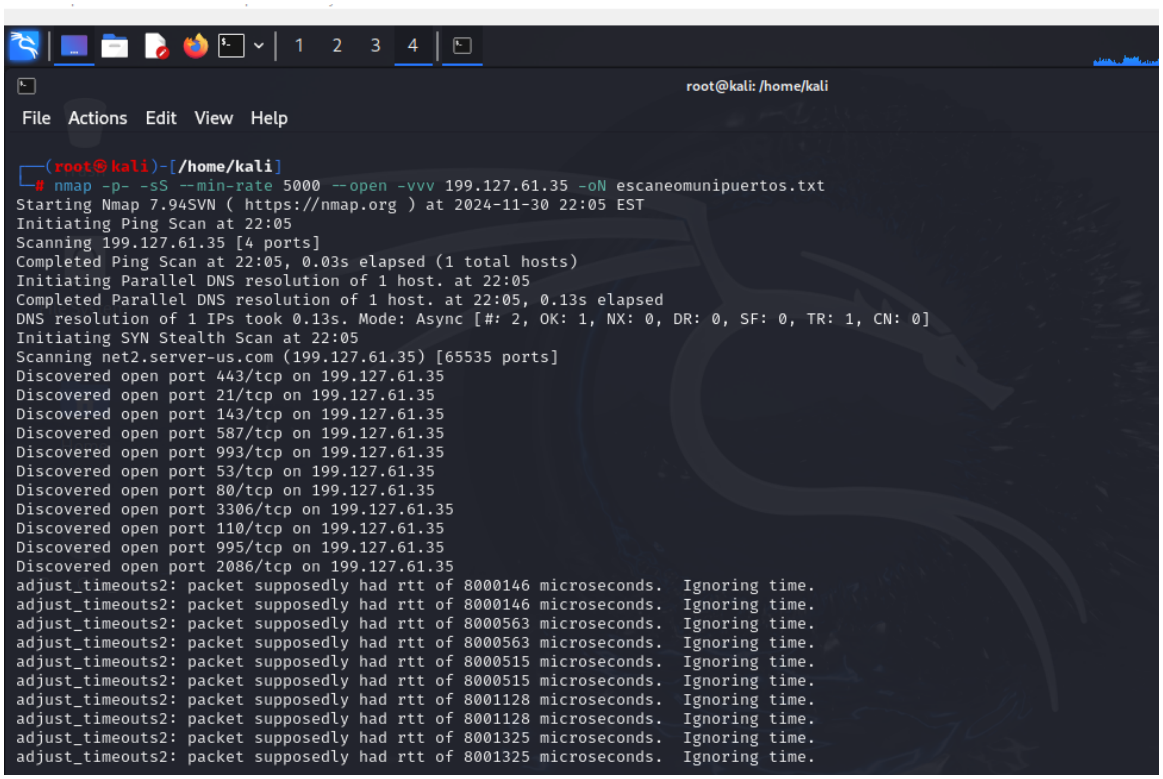
Análisis de vulnerabilidad con NMAP



Resultado de análisis con Nmap



Escaneo de puerto con NMAP



Puerto 21 (FTP)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV -p 21 --script ftp-anon,ftp-syst 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:02 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds

┌──(root㉿kali)-[/home/kali]
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script ftp-anon -p 21 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:20 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
```

Puerto 53 (DNS)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script=dns-recursion -p 53 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:05 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# dig @199.127.61.35 https://munisanjuanbautista.gob.pe/

; <<>> DiG 9.20.0-Debian <<>> @199.127.61.35 https://munisanjuanbautista.gob.pe/
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 12473
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;https://munisanjuanbautista.gob.pe/. IN        A

;; Query time: 108 msec
;; SERVER: 199.127.61.35#53(199.127.61.35) (UDP)
;; WHEN: Wed Dec 11 14:21:58 EST 2024
;; MSG SIZE  rcvd: 64
```

Puerto 80 (HTTP)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV -p 80 --script=http-title,http-headers 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:05 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.014s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    LiteSpeed
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Connection: close
|     content-type: text/html
|     date: Wed, 11 Dec 2024 19:06:06 GMT
|     server: LiteSpeed
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta http-equiv="Content-type" content="text/html; charset=utf-8">
|     <meta http-equiv="Cache-control" content="no-cache">
|     <meta http-equiv="Pragma" content="no-cache">
|     <meta http-equiv="Expires" content="0">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>404 Not Found</title>
|     <style type="text/css">
|     body {
|     font-family: Arial, Helvetica, sans-serif;
|     font-size: 14px;
|     line-height: 1.428571429;
|     background-color: #ffffff;
```

Puertos 110 y 995 (POP3 y POP3S)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV -p 110,995 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:08 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT    STATE SERVICE VERSION
110/tcp open  pop3    Dovecot pop3d
995/tcp open  pop3s?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.13 seconds
```

Puertos 143 y 993 (IMAP e IMAPS)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV -p 143,993 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:10 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT    STATE SERVICE VERSION
143/tcp open  imap    Dovecot imapd
993/tcp open  imaps?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

Puerto 443 (HTTPS)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script ssl-enum-ciphers -p 443 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:14 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     cipher preference: client
|_  least strength: A

Nmap done: 1 IP address (1 host up) scanned in 4.18 seconds
```

Puerto 587 (SMTP con STARTTLS)

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV --script smtp-commands -p 587 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:15 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT    STATE SERVICE VERSION
587/tcp open  smtp    Exim smtpd 4.97.1
| smtp-commands: net2.server-us.com Hello net2.server-us.com [38.250.155.66], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LO
P
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
```

Puerto 3306 (MySQL)

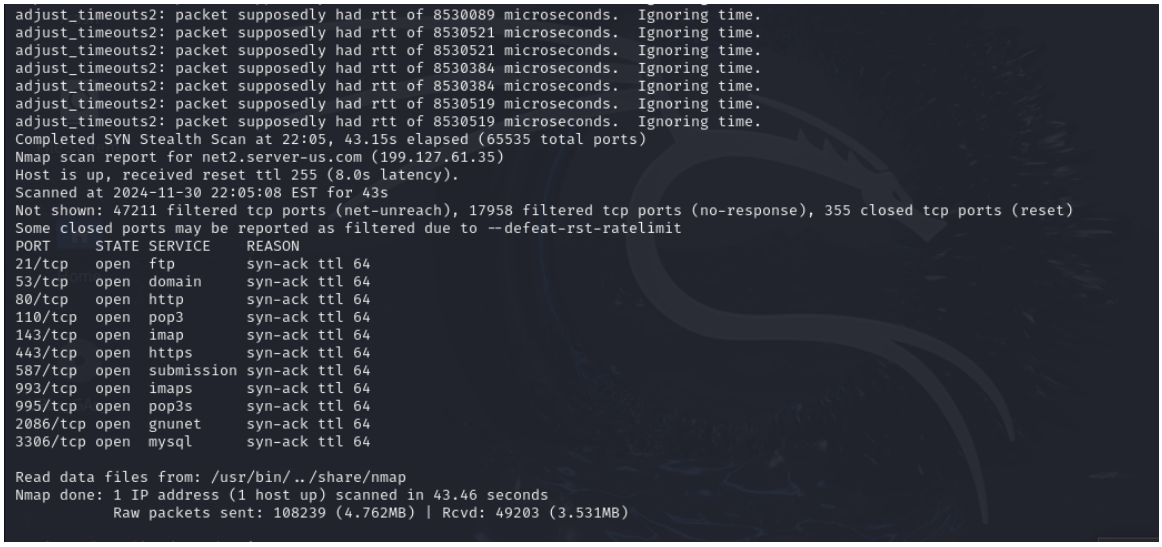
```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV -p 3306 --script mysql-info 199.127.61.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:16 EST
Nmap scan report for net2.server-us.com (199.127.61.35)
Host is up (0.027s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.5-10.6.19-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.6.19-MariaDB
|   Thread ID: 6020858
|   Capabilities flags: 63486
|   Some Capabilities: DontAllowDatabaseTableColumn, SupportsTransactions, LongColumnFlag, IgnoreSpaceBeforeParenthesis, ODBCClient, Speaks41ProtocolNew, Speak
s41ProtocolOld, IgnoreSigpipes, FoundRows, ConnectWithDatabase, InteractiveClient, Support41Auth, SupportsCompression, SupportsLoadDataLocal, SupportsAuthPlugi
ns, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: Q0;u_\1z8G=9H?Co){Qd
|_  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

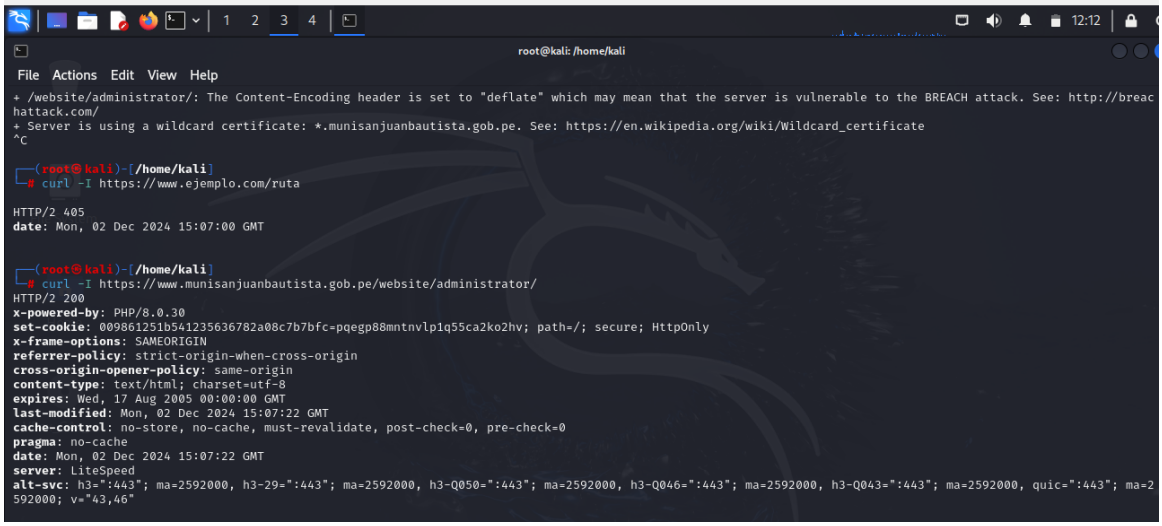
Escaneo de todo servicio con NAMP



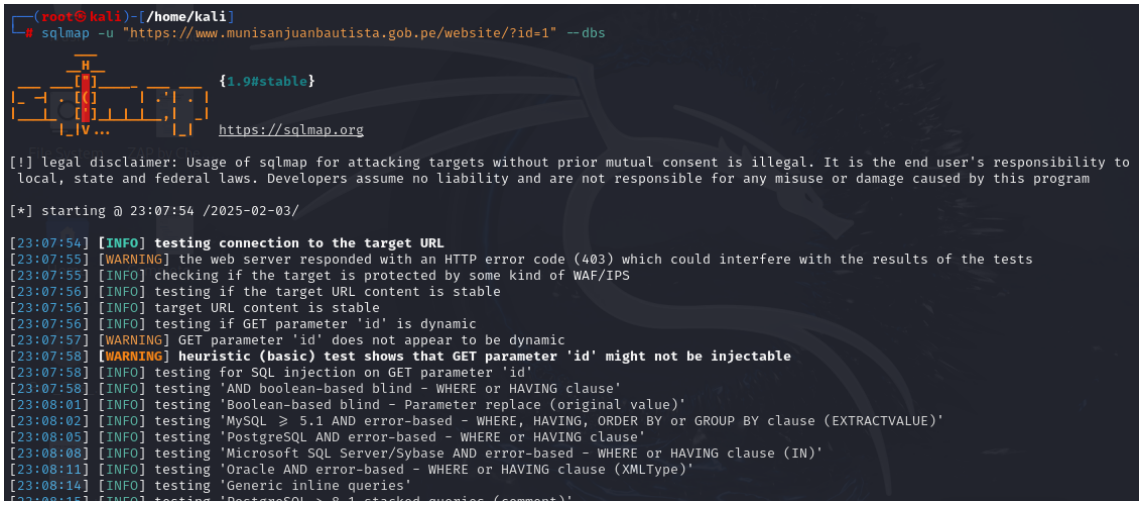
Escaneo de servicio FTP con NMAP

Análisis de vulnerabilidad con NIKTO

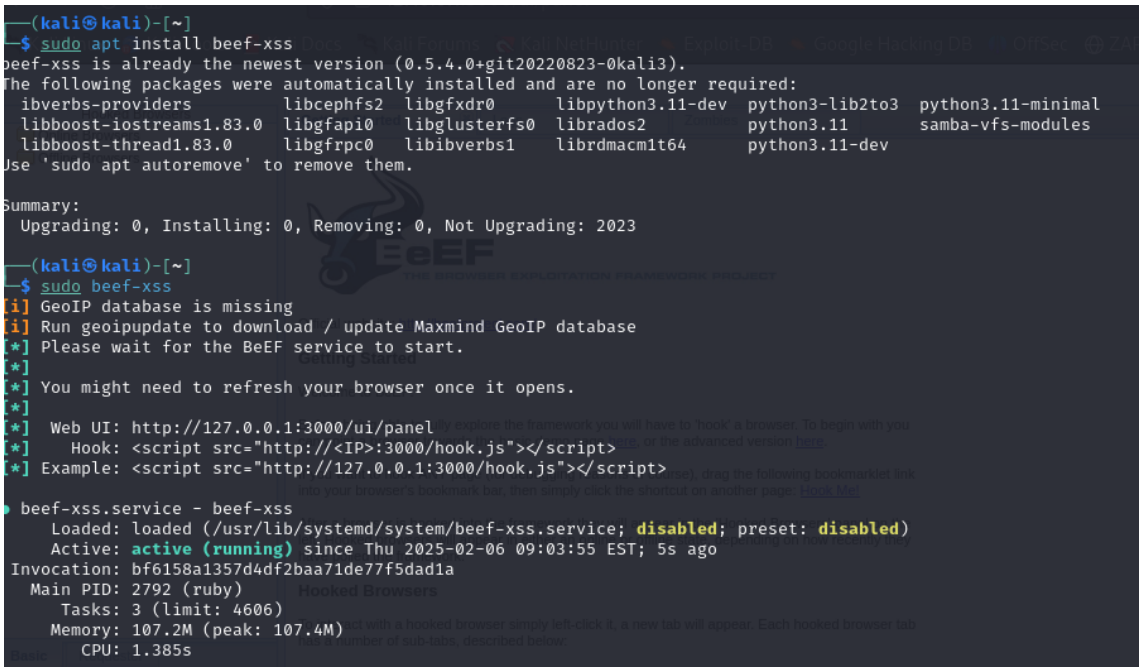
Usar (curl) para ver los encabezados HTTP con NIKTO



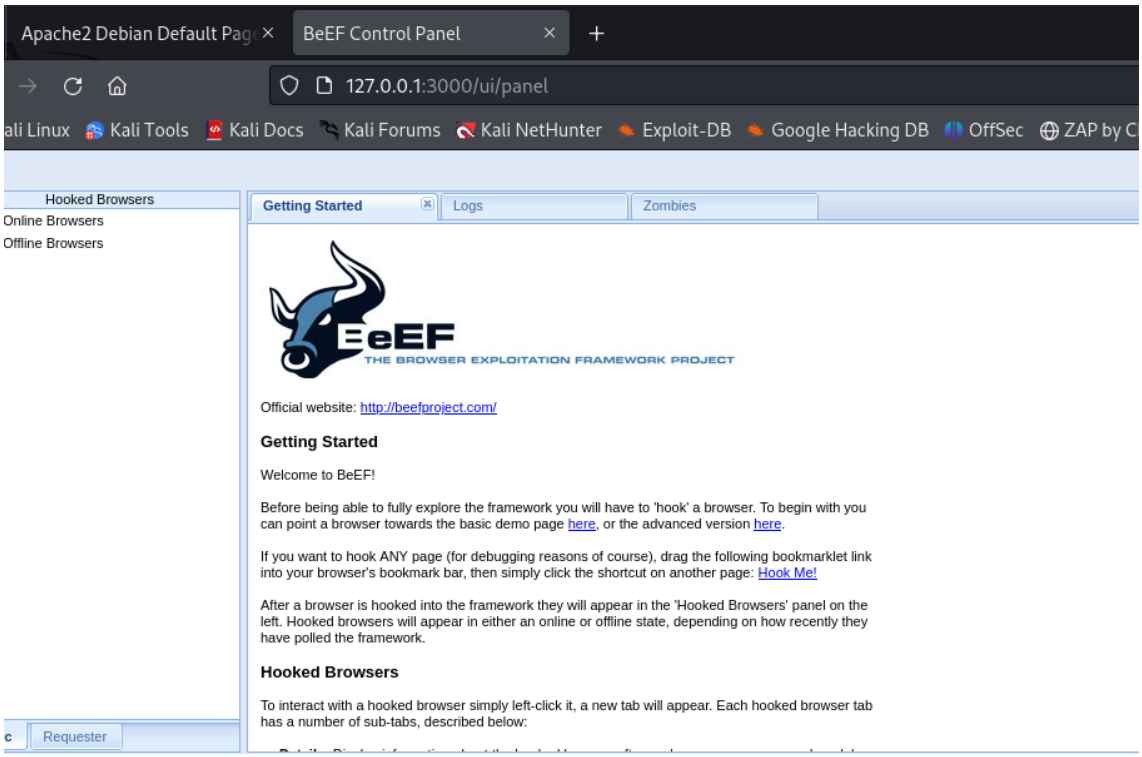
Análisis de vulnerabilidad con SQL inyección



Analisis de vulnerabilidad con Beef



Pantalla principal de Beef



UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ACTA DE SUSTENTACIÓN DE TESIS N° 023-2025-FIMGC

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

En la Universidad Nacional de San Cristóbal de Huamanga de la ciudad de Ayacucho, en cumplimiento a la **RESOLUCIÓN DECANAL No 200-2025-FIMGC-D**, a los **ocho días del mes de agosto 2025**, siendo las **10:00 a.m.**, reunidos en el **Auditorio de la Escuela Profesional de Ingeniería de Minas**, bajo la presidencia del **Mg. Ing. José Ernesto Estrada Cárdenas** y los miembros: **Mtra. Elinar CARRILLO RIVEROS, Mg. Ing. Karel PERALTA SOTOMAYOR y Dr. Manuel Avelino LAGOS BARZOLA** actuando como secretario docente el **MSc. Ing. Saul Walter RETAMOZO FERNÁNDEZ**, para proceder a la sustentación de tesis para optar el **Título Profesional de Ingeniero de Sistemas**, del bachiller:

RAMIRO NUÑEZ PEREZ

Quien presentó la tesis denominada:

Análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023

Los señores miembros del jurado, luego de expuesta la tesis y absueltas las preguntas, deliberaron y declararon:

Aprobado con dieciséis (16)

Siendo las **10:40 a.m.** del día **8 de agosto de 2025**, culmina el acto de sustentación de tesis, y en conformidad con lo actuado, los miembros del jurado firman al pie del presente.

MSc. Ing. José Ernesto Estrada Cárdenas
Presidente

Mtra. Elinar CARRILLO RIVEROS
Miembro

Mg. Ing. Karel PERALTA SOTOMAYOR
Miembro

Dr. Manuel Avelino LAGOS BARZOLA
Miembro - Asesor

MSc. Saul Walter RETAMOZO FERNANDEZ
Secretario docente de la FIMGC

FACULTAD DE INGENIERÍA
DE MINAS Y CIVIL
Av. Independencia S/N
Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

turnitin

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA Nº 025-2025-KPS-FIMGC/UNSCH

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado con el software Turnitin, en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la **Resolución de Consejo Universitario Nº 039-2021-UNSCH-CU**, Reglamento de Originalidad de Trabajos de Investigación de la Universidad Nacional San Cristóbal de Huamanga y **Resolución Decanal Nº 697-2024-FIMGC-D**, deja constancia de originalidad de trabajo de investigación, que el/la Sr./Srta.

Nombres y Apellidos	:	Ramiro Nuñez Perez
Escuela Profesional	:	INGENIERÍA DE SISTEMAS
Título de la Tesis	:	Análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023
Evaluación de la Originalidad	:	**13%** Índice de Similitud
Identificador de la entrega	:	2760076362

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

En señal de conformidad y verificación se firma la presente constancia

Ayacucho, 24 de setiembre de 2025

FIRMA DIGITAL

Firmado digitalmente por: PERALTA SOTOMAYOR Karel FAU 20143660754 soft
Motivo: Soy el autor del documento
Fecha: 05/05/2026 12:03:37-0500

Con depósito para Sustentación y Tramites
C.c. Archivo

FACULTAD DE INGENIERIA DE MINAS, GEOLOGIA Y CIVIL
Av. Independencia S/N Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

Análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023

por Ramiro Nuñez Perez

Fecha de entrega: 23-sept-2025 05:04p. m. (UTC-0500)

Identificador de la entrega: 2760076362

Nombre del archivo: MEMORANDO_N_500-2025-CERTIFICADO_DE_ORIGINALIDAD-_RAMIRO_NUÑEZ_PEREZ.pdf (7.27M)

Total de palabras: 31232

Total de caracteres: 184413

Análisis de vulnerabilidades de los sistemas informáticos de la Municipalidad Distrital de San Juan Bautista, 2023

INFORME DE ORIGINALIDAD

13%	12%	5%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.utn.edu.ec Fuente de Internet	2%
2	hdl.handle.net Fuente de Internet	2%
3	repositorio.uss.edu.pe Fuente de Internet	2%
4	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	1%
5	repositorio.unsch.edu.pe Fuente de Internet	1%
6	Submitted to CORPORACIÓN UNIVERSITARIA IBEROAMERICANA Trabajo del estudiante	1%
7	archive.org Fuente de Internet	1%
8	repositorio.unap.edu.pe Fuente de Internet	<1%

9	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
10	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	<1 %
11	Submitted to Universidad Abierta para Adultos Trabajo del estudiante	<1 %
12	repository.unad.edu.co Fuente de Internet	<1 %
13	repositorio.ucv.edu.pe Fuente de Internet	<1 %
14	www.coursehero.com Fuente de Internet	<1 %
15	repositorio.ug.edu.ec Fuente de Internet	<1 %
16	repositorio.upt.edu.pe Fuente de Internet	<1 %
17	repositorio.uladech.edu.pe Fuente de Internet	<1 %
18	Sandra Rodriguez Trigo. "La profesión de la gestión cultural en España: análisis interdisciplinario sobre su evolución, formación y adaptación en la era digital	<1 %

postpandemia", Universitat Politecnica de Valencia, 2024
Publicación

19	Submitted to Universidad Nacional del Centro del Peru Trabajo del estudiante	<1 %
20	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
21	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	<1 %
22	repositorio.unesum.edu.ec Fuente de Internet	<1 %
23	Jaramillo Jaramillo, Fabian Cristóbal. "Propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador.", Universidad Católica de Cuenca (Ecuador) Publicación	<1 %
24	Submitted to Universidad Nacional de Educación a Distancia Trabajo del estudiante	<1 %
25	atica.web.uah.es Fuente de Internet	<1 %

26	cimat.repositorioinstitucional.mx Fuente de Internet	<1 %
27	guardianproject.gitlab.io Fuente de Internet	<1 %
28	ciberseguridad.club Fuente de Internet	<1 %
29	repositorio.upse.edu.ec Fuente de Internet	<1 %
30	repositorio.utelesup.edu.pe Fuente de Internet	<1 %
31	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1 %
32	Submitted to University of Bradford Trabajo del estudiante	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		