



**UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE  
ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.**

**PROCESO DE TITULACIÓN**

**ABRIL 2022 – SEPTIEMBRE 2022**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA  
PRÁCTICA**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO EN SISTEMAS  
DE INFORMACIÓN**

**TEMA:**

**ANÁLISIS COMPARATIVO ENTRE LOS SISTEMAS OPERATIVOS  
WINDOWS XP Y KALI LINUX PARA EL ATAQUE Y PREVENCIÓN DE SU  
CIBERSEGURIDAD.**

**ESTUDIANTE:**

**WILMAN EMANUELLE VILLACIS SILVA**

**TUTOR:**

**ING. ENRIQUE DELGADO**

**AÑO 2022**

# CONTENIDO

PLANTEAMIENTO DEL PROBLEMA	3
JUSTIFICACIÓN	5
OBJETIVOS	6
LÍNEAS DE INVESTIGACIÓN	7
MARCO CONCEPTUAL	8
TABLA COMPARATIVA	19
MARCO METODOLÓGICO	20
RESULTADOS	21
DISCUSIÓN DE RESULTADOS	22
CONCLUSIONES	24
RECOMENDACIONES	25
REFERENCIAS	26
ANEXOS	28

## **PLANTEAMIENTO DEL PROBLEMA**

Muchos de los estudiantes no conocen completamente los sistemas operativos que se están utilizando, ni las herramientas que este posee, y como podrían utilizarlo de la mejor manera para sus clases y el estudio, por tal motivo el presente tema ayudara a los estudiantes a conocer sobre estos sistemas operativos.

El problema radica en que los estudiantes de la Universidad Técnica de Babahoyo, en la carrera de sistemas y sistemas de información no investigan sobre los sistemas que se van a utilizar en las materias.

En la actualidad los estudiantes de sistemas de información están cursando la materia de seguridad en computación, donde se utiliza los sistemas operativos Kali Linux y Windows XP, para atacar a otros sistemas o dispositivos mediante aplicaciones que se utilizan.

El poco conocimiento sobre la seguridad informática para los estudiantes, o personas que estén relacionadas, puede ser contraproducente para sí mismo, causándole daños, y ser vulnerable a posibles ataques. El sistema operativo comercial denominado Windows XP, tiene sus ventajas y vulnerabilidades que pueden ayudar al usuario y también puede evitar ser vulnerables a diversos ataques que puedan suceder, el sistema operativo de software libre Kali Linux, tiene muchas ventajas al tener su código libre ayudando así a los usuarios.

Con este estudio de caso se pretende que los usuarios y estudiantes de la Universidad Técnica de Babahoyo conozcan sobre los sistemas que se están utilizando, ayudándolos a tener un mayor desempeño y conocimiento al usarlos, Además de conocer herramientas que les permitan conocer y aprenden sobre los diversos ataques que pueden hacer, y las vulnerabilidades que tienen al ser usados.

En la materia de seguridad al computador, se pudo observar que muchos de los estudiantes tenían poco o nulo conocimiento sobre los sistemas operativos que se están utilizando, por tal motivo los estudiantes desconocían las herramientas que se podían utilizar al momento de hacer alguna actividad o trabajo.

Con el paso del tiempo, las tecnologías y sistemas han ido evolucionando y también los ataques y las vulnerabilidades informáticas, junto con las herramientas que muchos de nosotros desconocemos.

## **JUSTIFICACION**

El presente estudio comparativo se enfoca en los ataques y vulnerabilidades que tiene el sistema operativo comercial Windows XP y Kali Linux, de tal manera en que los estudiantes de la Universidad técnica de Babahoyo y los usuarios de estos sistemas conozcan las herramientas que estos sistemas poseen, adquiriendo conocimientos que no tenían y que pueden utilizar al momento de realizar alguna tarea o trabajo.

Actualmente los estudiantes que están cursando la materia de seguridad en computación en la Universidad Técnica de Babahoyo no conocen las herramientas que estos sistemas operativos tienen por lo cual momento de practicar o utilizar van con menos conocimientos y sin aprovechar por completo estos sistemas.

En el sistema operativo Kali Linux existen herramientas que nos permiten hacer ataques a otros sistemas o dispositivos, así también existen amenazas que pueden tener al usar dichas herramientas por no tener un mayor conocimiento de estas. También existen herramientas que nos permite conocer sobre las vulnerabilidades que tiene nuestros sistemas, dando una información detallada.

En la actualidad los usuarios no pueden usar herramientas de ataques sin conocerlas o estudiarlas, por tal motivo que esto provocaría vulnerabilidades y estar indefenso hacia posibles ataques y delitos en su ciberseguridad.

## **OBJETIVOS**

### **OBJETIVO GENERAL:**

- Analizar sobre los ataques y vulnerabilidades de los sistemas operativos Windows XP y Kali Linux.

### **OBJETIVOS ESPECIFICOS:**

- Examinar los sistemas operativos Windows XP y Kali Linux.
- Determinar las posibles vulnerabilidades que tienen estos sistemas.
- Conocer los diferentes ataques que se pueden hacer en los sistemas operativos.

## **LINEAS DE INVESTIGACION**

### **LÍNEA DE INVESTIGACIÓN**

Sistemas de información y comunicación, emprendimiento e innovación.

### **SUBLINEA DE INVESTIGACIÓN**

Redes y tecnologías inteligentes de software y hardware.

En el presente estudio de caso análisis comparativo entre los sistemas operativos Windows XP y Kali Linux para el ataque y prevención de su ciberseguridad está relacionado con los sistemas de información y también está relacionado con las redes y tecnologías de software.

Está relacionado con los sistemas de información debido a que se analizaran y compararan dos sistemas operativos, y este proyecto también se encuentra con la sublinea de redes y tecnologías, porque se hará manejo de las tecnologías, tanto hardware como software.

## MARCO CONCEPTUAL

### DEFINICION DE LOS SISTEMAS OPERATIVOS.

El sistema operativo más conocido como sistema operativo es un programa que actúa como intercesor entre la computadora y el usuario. El sistema operativo tiene diversas funciones como llegar a ser gestionar la memoria secundaria y los dispositivos de entrada y salida para los usuarios.

Un sistema operativo es un conjunto de programas que nos permiten administrar la memoria, el disco, los medios de almacenamiento de información y los diversos periféricos o recursos de nuestra computadora, como el teclado, el ratón, la impresora, la tarjeta de red. Los periféricos usan un controlador o controladores y son desarrollados por todos los fabricantes de computadoras. (Ramos, 2019)

Encontramos diferentes sistemas operativos como Windows, Linux, MAS OS, en sus diferentes versiones.

Dentro de las tareas que realiza el sistema operativo en particular, se encarga de administrar la memoria de nuestro sistema y la carga de los diferentes programas, para esto cada programa tiene una prioridad o jerarquía y dependiendo de ella serán los recursos de nuestro sistema.

El sistema operativo también se encarga de los procesos en ejecución. Llamamos a la carga en la memoria de nuestro programa de proceso, si no está cargada en la memoria de nuestro programa, pero "no se está ejecutando". El sistema operativo es el software que coordina y dirige todos los servicios y aplicaciones que el usuario utiliza en una computadora, por lo que es el más importante y fundamental. Son programas que permiten y controlan los aspectos más básicos del sistema.



Los sistemas operativos permiten que otros programas los utilicen para respaldar su funcionamiento. Por tanto, desde el sistema utilizado, se pueden instalar unos programas y otros no. Son parte esencial del funcionamiento de los sistemas informáticos y la pieza central del software en la cadena de procesos, porque establecen las condiciones mínimas para que todo funcione.

## **SISTEMA OPERATIVO WINDOWS XP**

Su nombre en clave era Whistler durante la fase de desarrollo y su nombre oficial proviene del término inglés eXPerience. Este sistema operativo, que sucedió a Windows 2000 y su antecesor Windows Vista, fue el más utilizado en el mundo.

Hay adaptaciones para diferentes entornos, como computadoras domésticas, portátiles y miniportátiles. Los usuarios elogiaron la interfaz gráfica de Windows XP, que promueve un uso más simplificado en comparación con otros sistemas operativos. En cambio, entre las críticas más frecuentes están sus vulnerabilidades de seguridad y la integración del navegador Internet Explorer y Windows Media Player (lo que puede considerarse un abuso del dominio de mercado de Microsoft y un ataque a la libre competencia).

Otra de las novedades de Windows XP es la inclusión del sistema Windows Genuine Advantage, que se encarga de verificar si la copia es original o falsificada. Cuando el programa falla en el proceso de validación, se advierte al usuario. (Aller, 2020)

El 8 de abril de 2014, se suspendió Windows XP. Esto significaba que, a partir de ese momento, los usuarios que cuenten con el mencionado sistema operativo en sus equipos no podrán contar con más actualizaciones de seguridad, correcciones de errores del sistema o parches de diversa índole.

Este hecho implicaba básicamente que el equipo con Windows XP instalado queda desprotegido y más expuesto a vulnerabilidades. (C,2019)

## **VENTAJAS.**

El Windows XP tiene diversas ventajas entre las cuales encontramos su fácil instalación, lo entendible y comprendido que es a la hora de utilizar, tiene diversas facilidades por las cuales podemos terminar o llegar más fácil a ciertas ventanas o aplicaciones lo cual nos permite trabajar con más rapidez, facilidades a la hora de mover y copiar, algunas de las ventajas son:

- Instalación simple.
- Uso comercial.
- Programas atractivos de diseño web y diseño gráfico sin mucha información sobre ellos.
- Programación visual, orientada a objetos y estructurada

## **DESVENTAJAS**

Algunas de las desventajas de Windows XP pueden ser:

- Muchos errores (errores de código).
- Amenaza constante de infecciones virales.
- Bloque de pantalla azul y otras pantallas publicitarias.
- Uso excesivo de recursos si desea instalar programas sofisticados.

## **VULNERABILIDADES.**

Puede presentar diversas vulnerabilidades las cuales llegan a contarse como desventajas que presenta este sistema, puede llegar a ser muy fácil que se infecte de algún virus. (Noriega, 2020)

## **SISTEMA OPERATIVO KALI LINUX**

Kali Linux es una distribución de Linux basada en Debian diseñada específicamente para una amplia variedad de problemas de seguridad, como análisis de red, ataques inalámbricos, análisis forense y otros que mencionaremos más adelante. (Altube, 2021)

Linux es probablemente el sistema operativo de código abierto más popular y personalizable del mundo. Gracias a sus miles de funciones y amplia configuración, este sistema se puede adaptar a cualquier entorno de trabajo, tanto personal como profesional. Una de las distribuciones más valiosas por su aporte a la seguridad es Kali Linux. Esta distribución ofrece muchas funciones de administración y análisis de red, así como análisis forense informático. (Jesus, 2022)

Existen herramientas para realizar todas estas pruebas y análisis de seguridad. Fue desarrollado en base a una reescritura de BackTrap, otra distribución de Linux para usos similares, por Mati Aharoni y Devon Kearns de Offensive Security.

Kali Linux se encuentra entre las distribuciones de seguridad de Linux más utilizadas porque es una de las mejores para uso personal y profesional, brindando paquetes de herramientas como Foremost, Wireshark, Maltigo as-Aircrack-ng, Kismet y más para los usuarios. Probablemente esté familiarizado con algunas de estas herramientas, especialmente Wireshark, que tiene un artículo interesante en nuestro blog que habla de ello. Kali Linux cuenta con multitud de herramientas, a nivel gráfico y, sobre todo, de mando, lo que lo convierte en un sistema muy completo, ya sea para defensores que buscan un sistema más seguro, como para atacantes que buscan que los datos sean tan valiosos como las cuentas, contraseñas, y otros datos personales.

Entre todo lo que se puede hacer con Kali Linux, destacamos varias características:

- Colección de información análisis de vulnerabilidades ataques inalámbricos.  
Aplicaciones web
- Herramientas forenses
- Seguimiento y Pesca
- Ataques de contraseña
- Ingeniería inversa
- Herramientas de información piratería informática

Kali Linux es una distribución enfocada a la seguridad informática, por lo que puedes ejecutar todo tipo de herramientas para probar la seguridad de tus sistemas y redes. Esto no significa que cuando ejecute Kali Linux en su computadora, aparecerá un gran botón en el medio de la pantalla que convertirá su computadora en una máquina de eludir la seguridad. (UDS Enterprime Team, 2020)

Kali Linux es una plataforma la cual abarca una gran cantidad de herramientas como es capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

## **OPENVAS**

OpenVAS es un escáner de vulnerabilidades de código abierto muy útil que nos permite encontrar fallas de seguridad e información detallada sobre vulnerabilidades que pueden ser explotadas para comprometer la confidencialidad, disponibilidad e integridad de los datos almacenados y procesados en nuestras computadoras. (Araya, 2021)

También es un escáner de vulnerabilidades multiplataforma de código abierto con una aplicación web que nos permite buscar vulnerabilidades en una o más computadoras dentro de una red.

## **ESCANER DE VULNERABILIDADES**

Es un software que nos permite identificar vulnerabilidades conocidas en los diferentes servicios o aplicaciones instaladas en los equipos informáticos de una empresa. Estos escáneres funcionan comparando los servicios y sus versiones instaladas en nuestros equipos con la propia base de datos del escáner, que contiene todas las versiones de los servicios que han identificado algún tipo de vulnerabilidad hasta el momento. Al final del escaneo, se muestra un informe que contiene la información con todos los agujeros de seguridad encontrados.

El escaneo de vulnerabilidades es un proceso automatizado que escanea aspectos de una red, aplicación o dispositivo en busca de fallas de seguridad. Escanear en busca de vulnerabilidades de seguridad es algo que debe hacerse regularmente para garantizar que la información y las aplicaciones permanezcan seguras. (Cartara, 2020)

## **LEGION**

Legion una herramienta de prueba de penetración de red fácil de usar, altamente extensible y semiautomatizada que ayuda en el descubrimiento, exploración y explotación de sistemas de información. Legion, una bifurcación de Sparta SECFORCE, es un marco de prueba de red semiautomático de código abierto que ayuda en el descubrimiento, exploración y explotación de sistemas de información. Legion es desarrollado y mantenido por GoVanguard.

Reconocimiento y escaneo automático con NMAP, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer y más (con casi 100 scripts programados automáticamente) Interfaz gráfica fácil de usar con menús y paneles ricos en contexto que permiten a los pentesters encontrar y explotar rápidamente los vectores de ataque en los hosts.

La funcionalidad modular permite a los usuarios personalizar fácilmente Legion y llamar automáticamente a sus propios scripts/herramientas Escaneo altamente personalizable para evasión de IPS como un ninja Detección automática de CPE (Common Platform Enumeration) y CVE (Common Vulnerability and Exposures) Guardado automático de resultados de proyectos y tareas en tiempo real.

## **ATAQUES INFORMATICOS**

En un contexto cada vez más digital y con iniciativas innovadoras con las tecnologías de la información, se está desarrollando una economía digital que conecta a diferentes actores de la sociedad, para crear nuevos ecosistemas de negocios donde se pueden lograr oportunidades, utilidades y experiencias sin precedentes para diferentes intereses. grupos En este sentido, la inseguridad digital, manifestada en ciberataques, se configura como un impuesto progresivo que grava la confianza digital de los consumidores y genera áreas de incertidumbre. (J & M, 2020)

En consecuencia, este artículo desarrolla una reflexión conceptual sobre este nuevo impuesto progresivo, así como algunas ideas para concretar su elusión en un entorno cada vez más digital y tecnológico.

En computadoras y redes informáticas, un ataque es un intento de exponer, alterar, interrumpir, destruir, destruir un activo para obtener acceso no autorizado o utilizar un activo. Un ciberataque o ataque informático es cualquier maniobra ofensiva de explotación intencionada que tiene por objeto tomar el control, desestabilizar o dañar un sistema informático (ordenador, red privada, etc.). Un atacante es una persona u organización que intenta hacerse con el control de un sistema informático para utilizarlo con fines malintencionados, robar información o dañar a su objetivo. (Bello, 2021)

Un ciberataque utiliza códigos maliciosos para corromper códigos, datos privados o algoritmos, generando consecuencias que vulneran la seguridad de los sistemas de información.

Por ello, es cada vez más importante implementar estrategias y medidas que reduzcan la posibilidad de sufrir este tipo de ataques, que no solo ponen en peligro la reputación de la empresa sino también su funcionamiento, la relación con clientes y proveedores, además de generar pérdidas, ingresos e incluso nuevas oportunidades de negocio. (Jimenez, 2022)

## **VULNERABILIDADES INFORMATICAS**

Todo lo construye un hombre vulnerable a algo. Los sistemas de información, incluso los mejor protegidos, tienen muchas vulnerabilidades que pueden ser aprovechadas por intrusos o atacantes.

En informática, una vulnerabilidad es una debilidad existente en un sistema que una persona malintencionada puede utilizar para comprometer su seguridad. Una vulnerabilidad informática se considera cualquier debilidad en el software o hardware que puede ser aprovechada por un ataque cibernético para obtener acceso no autorizado a un sistema informático, lo que permite a un atacante comprometer la integridad, disponibilidad o confidencialidad de ese sistema o los datos que contiene. lugares. en riesgo. en peligro de extinción. (Santander, 2021)

Todo esto porque puede acceder a la memoria del sistema, instalar programa maligno y robar, borrar o modificar datos sensibles. Pueden ocurrir debido a fallas de diseño, errores de configuración o procedimientos no robustos. Los más peligrosos son aquellos que permiten al atacante ejecutar código malicioso en el sistema comprometido. Sin embargo, para que un atacante aproveche esta vulnerabilidad, debe poder conectarse al sistema informático y sigue siendo una de las principales razones por las que una

empresa puede experimentar un ataque informático en su sistema.

Las vulnerabilidades son agujeros de seguridad en cualquier organización, ya sea en sistemas, procesos o personas, y son un punto de acceso para que intrusos o atacantes vulneren su seguridad.

## **TIPOS DE VULNERABILIDADES INFORMATICAS**

Junto con el nacimiento de las tecnologías de la información, también nacieron los programas o software que permitían el funcionamiento de estas máquinas primitivas. Si bien estas máquinas procesaban la información con precisión, lo cierto es que los programas que las controlaban eran de desarrollo y diseño humano, por lo que su código era propenso a todo tipo de errores.

A lo largo de los años, los errores de programación han disminuido, gracias en gran parte al hecho de que los lenguajes de programación más nuevos son más flexibles y hay mucha información impresa y en Internet sobre cómo operarlos.

El problema de las vulnerabilidades es un tema que no debe tomarse a la ligera de ninguna manera, porque nos puede traer un buen número de peligros, aunque no utilicemos datos o documentos muy importantes. Este problema es realmente muy grave, y ha sido estudiado y clasificado por infinidad de empresas y organizaciones, algunos tipos pueden ser:

- **Vulnerabilidades de desbordamiento de búfer:** Esta condición es verdadera cuando una aplicación no puede controlar la cantidad de datos copiados en el búfer, por lo que, si esa cantidad excede la capacidad del búfer, los bytes restantes se almacenan en áreas de memoria adyacentes, dejando su escritura original. Este problema se puede aprovechar para ejecutar código que otorga privilegios de root al atacante.



- **Vulnerabilidades de la condición de carrera:** La condición de carrera generalmente se cumple cuando varios procesos acceden a un recurso compartido al mismo tiempo. En este sentido, es un buen ejemplo de variables, cambiando su estado y obteniendo así un valor inesperado.
- **Vulnerabilidades de error de cadena de formato:** La causa subyacente de los llamados errores de cadena de formato es la condición de aceptar sin validar la entrada de datos proporcionada por el usuario. Este es un error de diseño de la aplicación, es decir, proviene de descuidos en su programación. En este sentido, C/C++ es el lenguaje de programación más afectado por este tipo de vulnerabilidad. Es casi seguro que un ataque realizado con este método conduce a la ejecución de código arbitrario y al robo de información y datos del usuario.
- **Vulnerabilidades de secuencias de comandos entre sitios (XSS):** Las vulnerabilidades Cross-Site Scripting (XSS) se utilizan en ataques en los que las condiciones permiten la ejecución de scripts de lenguaje como VBScript o JavaScript. Este tipo de situaciones se pueden encontrar en cualquier aplicación utilizada para mostrar información en cualquier navegador web que no esté debidamente protegido contra estos ataques.
- **Vulnerabilidades de denegación de servicio:** La técnica de denegación de servicio se utiliza para evitar que los usuarios utilicen un servicio, una aplicación o un recurso. Básicamente, lo que provoca un ataque de denegación de servicio es la pérdida de conectividad de red para la víctima del ataque debido al consumo excesivo de ancho de banda de red o recursos adjuntos al sistema informático.
- **Vulnerabilidades complejas de Windows:** Sin duda, esta es una de las vulnerabilidades más famosas y comunes entre los usuarios, especialmente para aquellos que llevan algunos años detrás de un monitor. Esta técnica, también

conocida como “Windows Spoofing”, permite a un atacante mostrar ventanas de notificación y mensajes en el ordenador de la víctima, lo que suele incluir decirnos que hemos ganado un premio o situaciones similares.

## **SEGURIDAD INFORMATICA**

La seguridad informática es un tema central hoy en día para todos los usuarios de equipos informáticos, ya sean de escritorio o móviles, en casa, en la escuela o dentro de una organización. Esto se debe a que el uso y la popularidad de Internet plantea importantes riesgos de seguridad. Internet se utiliza para fines para los que no estaba previsto originalmente. Internet se diseñó originalmente para promover la conectividad, no la seguridad. (Gomez, 2022)

La seguridad informática, también conocida como ciberseguridad, hace referencia a la protección de la información y, en particular, de su tratamiento, para evitar la manipulación de datos y procesos por parte de personas no autorizadas. Su finalidad principal es proteger a las personas y los equipos tecnológicos y datos de daños y amenazas de terceros. Es por ello que esta disciplina en el campo de las tecnologías de la información encargada de proteger la privacidad de los datos dentro de los sistemas informáticos se ha convertido en parte esencial de las operaciones empresariales y comerciales.

Es la disciplina del campo de la tecnología de la información encargada de proteger la privacidad de los datos dentro de los sistemas informáticos, los cuales se han convertido en parte indispensable de las operaciones empresariales y comerciales. (UNIR, 2021)

## TABLA COMPARATIVA

Para hacer esta tabla comparativa con ventajas y desventajas de este sistema, se recopilaron datos de diferentes fuentes en internet.

	WINDOWS XP	KALI LINUX
<b>VENTAJAS</b>	<ul style="list-style-type: none"><li>● Su manejo es muy intuitivo</li><li>● Multiusuario y multitarea</li><li>● Su instalación es sencilla</li><li>● Programación visual orientada a objetos</li></ul>	<ul style="list-style-type: none"><li>● Su uso es gratuito</li><li>● Rara vez es víctima de ciberataques.</li><li>● Pocos errores en su seguridad.</li><li>● Brinda muchas herramientas.</li><li>● Código abierto</li></ul>
<b>DESVENTAJAS</b>	<ul style="list-style-type: none"><li>● Fallos en su seguridad</li><li>● No tiene soporte de Microsoft</li><li>● Gran cantidad de ataques por virus</li><li>● Limitación con la RAM</li><li>● No brinda bloqueo a intrusos.</li></ul>	<ul style="list-style-type: none"><li>● Complicado de usar</li><li>● Su idioma prioritario es las ingles</li><li>● No es para principiantes</li><li>● Varios programas no están disponibles para esta plataforma.</li></ul>

## **MARCO METODOLOGICO**

### **Tipo de investigación.**

En el presente estudio de caso se utilizó la metodología bibliográfica básicamente consiste en la compilación de información en base a lo que ya está publicado, también se utilizó el método cualitativo debido a que se hizo una recolección de datos, mediante una encuesta, también se utilizó la metodología de campo, por que se uso un programa para conocer las vulnerabilidades de Windows.

### **Técnicas e Instrumentos.**

En el presente caso de estudio se utilizó la técnica de encuestas, con los instrumentos de un formulario de Google, debido que se hizo una encuesta a un grupo de 60 estudiantes de la Universidad Técnica de Babahoyo en la carrera de Ingeniería en Sistemas e Ingeniería en sistemas de información con preguntas relacionadas a los ataques y vulnerabilidades de los sistemas operativos Kali Linux y Windows XP, se tomaron 60 estudiantes donde se encuestaron a 10 estudiantes en los cursos de los semestres de octavo ingeniería en sistemas de información y decimo en ingeniería en sistemas, de la sección mañana, tarde y noche, se utilizo OpenVAS como instrumento para conocer las vulnerabilidades.

## RESULTADOS

Gracias a los resultados obtenidos con el método bibliográfica se pudo conocer sobre los ataques existente que tienen estos sistemas debido a las vulnerabilidades que estos poseen también se adquirieron conocimientos sobre las herramientas de los sistemas operativos y como estas ayudarían para prevenir o hacer un ataque informático.

Gracias a la técnica de encuesta donde se realizó 5 preguntas a 60 estudiantes, se llegaron a los resultados que con la primera pregunta al analizar la tabulación se pudo observar que el 95% de los encuestados si han utilizado estos sistemas operativos y solo el 5% no ha utilizado.

En la segunda pregunta se puede observar que en su mayoría no conocen las vulnerabilidades que estos sistemas poseen con un 80% y solo el 20% Si conoce.

En la tercera pregunta se observó que el 53% de los encuestados si ha utilizado estos sistemas para realizar ataques, en cambio el 47% no lo ha hecho.

Analizando los resultados de la cuarta pregunta se llegó a la conclusión de que el 88% de los encuestados no conocen las herramientas que estos sistemas operativos poseen y la minoría con un 12% desconoce estas herramientas.

Según los resultados de la quinta pregunta se llegó a la conclusión de que el 28% de los encuestados fue víctima de algún ataque cibernético, mientras que el 72% no.

Como resultado un sistema operativo de software libre (Kali Linux) es mucho mejor y más protegido que un sistema de software comercial en este caso Windows XP.

Gracias al programa OpenVAS que se utilizo para conocer sobre las vulnerabilidades que este sistema posee, dio como resultado que existe muy poca vulnerabilidad en este sistema.

## DISCUSIÓN DE RESULTADOS

Con los resultados obtenidos con los métodos y técnicas que se utilizaron en este proyecto, es preferible usar un sistema más seguro y de código libre como es el sistema operativo Kali Linux, debido a que este cuenta con muchas herramientas que se pueden utilizar y es mucho más robusto y menos vulnerable que su contraparte el sistema Windows XP.

Con los resultados obtenidos en la encuesta de los 60 estudiantes hay que recalcar que muchos de los estudiantes han utilizado estos sistemas, pero muy pocos conocen sus vulnerabilidades, herramientas, ventajas y desventajas que estas tienen entre sí.

La mayoría de los encuestados ha utilizado estos sistemas operativos, debido a esto, es de vital importancia el análisis de estos sistemas para dar a conocer a los usuarios sobre las características que estos ofrecen.

Una gran mayoría no conoce de las vulnerabilidades que estos sistemas poseen lo cual sería perjudicial tanto para su persona, como para la empresa de donde trabaje, es de vital importancia que los usuarios conozcan estas vulnerabilidades para evitar daños a futuro y ataques por ciberdelincuentes.

Muchos de los estudiantes no conocen las herramientas sobre todas las herramientas que estos sistemas poseen, en especial las del sistema Kali Linux, que cuenta con una gran cantidad de herramientas, que sirven para diversas cosas, y es muy importantes conocerlas en caso de que su uso se requiera.

También existe una parte de los encuestados que han sido víctima de algún ataque por parte de algún ciberdelincuente, esto podría reflejarse a que la mayoría de las personas no conocía sobre las vulnerabilidades que estos sistemas poseen, o también por desconocer sobre los ataques que puedan existen en el uso de las nuevas tecnologías que

han surgido a lo largo de los años.

En lo personal elegiría un sistema más protegido y que tenga menos vulnerabilidades para diversas acciones y que me ayudarían a estar más protegido con los ciberdelincuentes que cada día aumentan más.

## CONCLUSIONES

Una vez hecho el análisis se determina que el sistema operativo Windows XP al ser un sistema de software comercial, es más vulnerable a errores y a su ciberseguridad, debido a que hace mucho tiempo esta descontinuado por lo que ya no recibe actualizaciones ni parches, en cambio Kali Linux al ser un sistema de código libre, es muy poco probable que sea víctima de algún ataque por ciberdelincuentes, es mucho más seguro.

Mediante el análisis realizado, se llegó a la conclusión de que el sistema operativo Kali Linux es menos vulnerable, debido a que es mucho más robusto, mientras Windows XP es mucho más indefenso, los usuarios que utilizan ese sistema, están más desprotegidos.

Gracias al análisis de estos sistemas operativos se llegó a la conclusión de que Kali Linux es un sistema que nos permite utilizar muchas herramientas y aplicaciones de ataque que Windows XP.



## **RECOMENDACIONES**

Es recomendable que, si vas a usar el sistema operativo para entretenimiento o eres un principiante con estas tecnologías, es mejor elegir el sistema Windows XP, mientras que, si tu uso es para guardar datos importantes, querer estar más en incognito o seguro al momento de navegar por el internet y hacer diversas pruebas de ataques, y vulnerabilidades, se recomienda escoger Kali Linux.

Es recomendable analizar las vulnerabilidades que tienen estos sistemas para conocer y determinar que no vas a estar desprotegido frente a ciberataques, se recomienda usar Kali Linux al ser un software más robusto.

Si lo que te interesa es simular ataques, saber más sobre ciberseguridad, ataques informáticos, poner en práctica tus conocimientos, se recomienda usar Kali Linux, por su gran variedad de herramientas y aplicaciones que tiene para ataques.

## REFERENCIAS

- Aller, A. (20 de 12 de 2020). *Windows XP, uno de los mejores sistemas operativos de Microsoft*. Obtenido de Profesional Reviuw: <https://www.profesionalreview.com/2020/12/20/historia-windows-xp/>
- Altube, R. (05 de 11 de 2021). *Kali Linux: Que es y características principales*. Obtenido de Open Webinars: <https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/>
- Araya, J. (16 de 02 de 2021). *Guia de instalacion de OpenVas en Kali Linux*. Obtenido de SpainClouds: <https://www.spainclouds.com/blog/guia-de-instalacion-de-openvas-en-kali-linux>
- Bello, E. (29 de 11 de 2021). *Ciberseguridad*. Obtenido de IEBS: <https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/>
- C, O. (12 de 04 de 2019). *Adios a Windows XP*. Obtenido de TecnoXplora: [https://www.lasexta.com/tecnologia-tecnoxplora/internet/adios-windows-historia-mejor-sistema-operativo-historia-microsoft\\_201904125cb0720d0cf2bee6b3f7b452.html](https://www.lasexta.com/tecnologia-tecnoxplora/internet/adios-windows-historia-mejor-sistema-operativo-historia-microsoft_201904125cb0720d0cf2bee6b3f7b452.html)
- Cartara, J. (05 de 10 de 2020). *Que es un escaneo de vulnerabilidades de seguridad*. Obtenido de BLOG: <https://www.cyberseguridad.com.mx/que-es-un-escaneo-de-vulnerabilidades-de-seguridad/>
- J, J., & M, C. (26 de 11 de 2020). *Ciberataques*. Obtenido de ACIS: <https://sistemas.acis.org.co/index.php/sistemas/article/view/129>
- Jesus. (02 de 08 de 2022). *Kali Linux Para Principiantes*. Obtenido de Dongee: <https://www.dongee.com/tutoriales/que-es-kali-linux/>
- Jimenez, M. M. (02 de 03 de 2022). *Ataques ciberneticos: causas, tipos y consecuencias*. Obtenido de Pirani: <https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias>
- Noriega, F. A. (13 de 03 de 2020). *Explotar Vulnerabilidades en Windows XP*. Obtenido de Issu: [https://issuu.com/fatimaabigailporrasnoriega/docs/f\\_tima\\_abigail\\_porras\\_noriega-vulnerabilidad\\_windo](https://issuu.com/fatimaabigailporrasnoriega/docs/f_tima_abigail_porras_noriega-vulnerabilidad_windo)
- Ramos, M. d. (2019). *Sistema Operativos Monopuestos*. España. Obtenido de [https://books.google.es/books?hl=es&lr=&id=qt-ZDwAAQBAJ&oi=fnd&pg=PP1&dq=sistemas+operativos&ots=AL\\_I6iZ-AR&sig=T30BcGIAL4ca9jFitx1C80Q#v=onepage&q=sistemas%20operativos&f=false](https://books.google.es/books?hl=es&lr=&id=qt-ZDwAAQBAJ&oi=fnd&pg=PP1&dq=sistemas+operativos&ots=AL_I6iZ-AR&sig=T30BcGIAL4ca9jFitx1C80Q#v=onepage&q=sistemas%20operativos&f=false)
- Gomez, A. (2022). *Auditoria de Seguridad Informatica*. Obtenido de

[https://books.google.es/books?hl=es&lr=&id=No5dEAAAQBAJ&oi=fnd&pg=PA41&dq=seguridad+informatica&ots=RfBH7BMsl0&sig=GD2ACAHRIcuNe4f\\_okL09a2qEOE#v=onepage&q&f=false](https://books.google.es/books?hl=es&lr=&id=No5dEAAAQBAJ&oi=fnd&pg=PA41&dq=seguridad+informatica&ots=RfBH7BMsl0&sig=GD2ACAHRIcuNe4f_okL09a2qEOE#v=onepage&q&f=false)

Santander. (02 de 10 de 2021). *Que es una vulnerabilidad informatica*. Obtenido de Santander: <https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.>

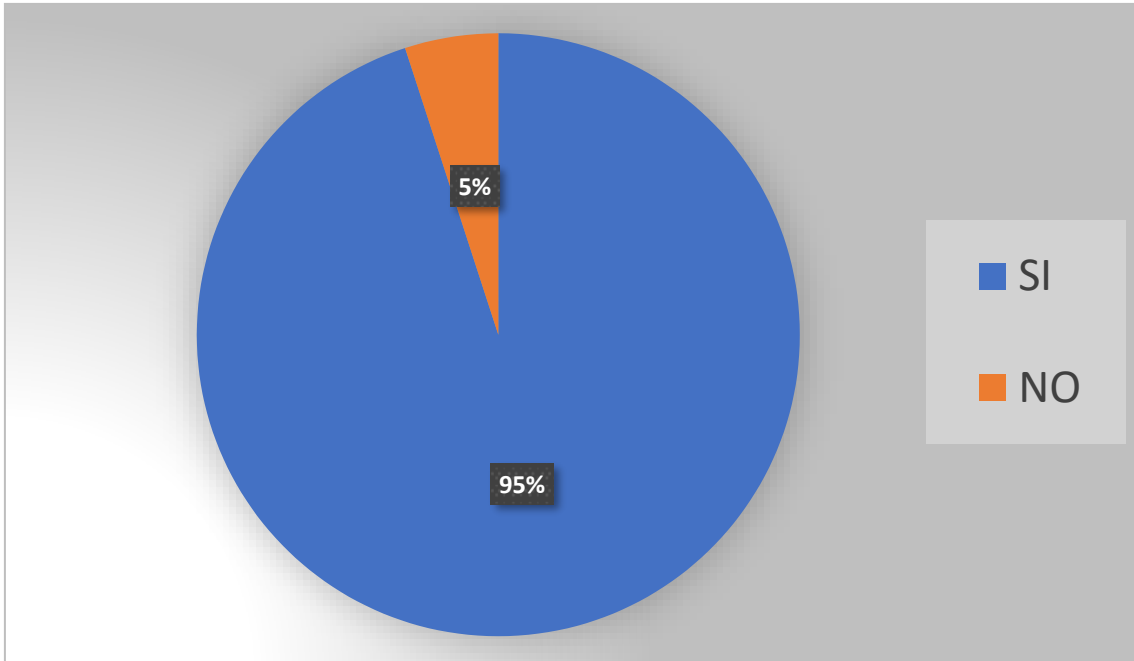
UDS Enterprime Team. (09 de 10 de 2020). *Kali Linux*. Obtenido de UDS Enterprime : <https://www.udsenderprise.com/es/blog/2020/10/09/kali-linux-instala-utilizar-distro-hacking-etico/>

UNIR. (15 de 06 de 2021). *QUE ES LA SEGURIDAD INFORMATICA Y CUALES SON SUS TIPOS*. Obtenido de UNIR: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>

**ANEXOS**  
**ANEXO DE RESULTADOS DE LAS ENCUESTAS.**

**Figura 1**

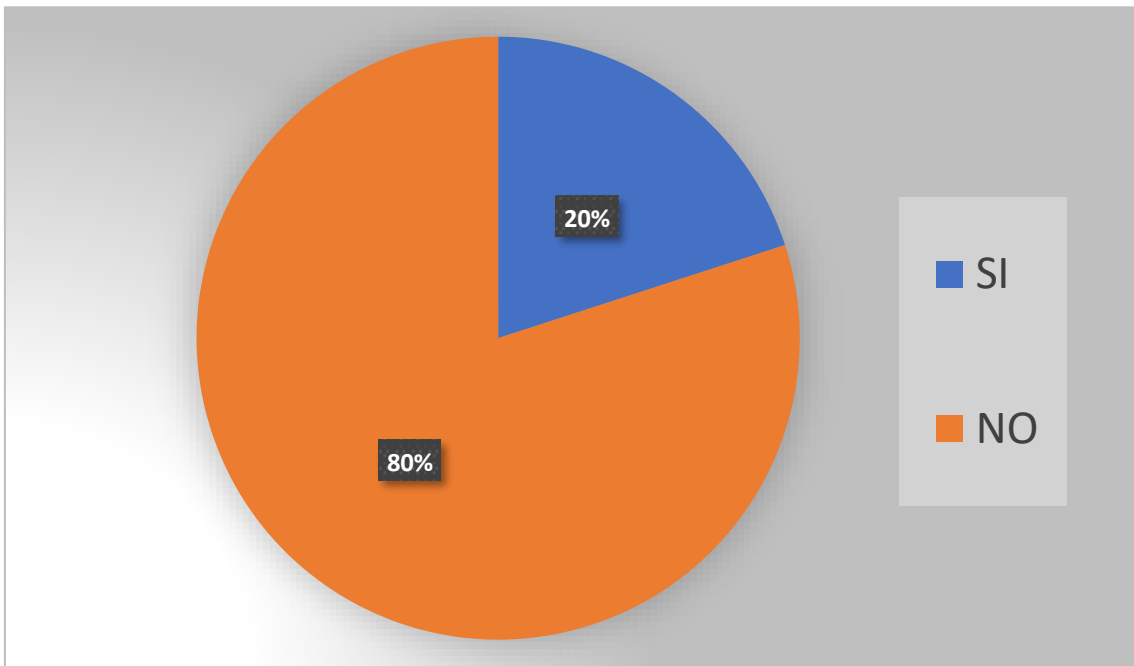
**¿Ha utilizado los sistemas Windows o Kali Linux?**



**Nota:** Al analizar el grafico se puede observar que el 95% de los encuestados si han utilizado estos sistemas operativos y solo el 5% no ha utilizado.

**Figura 2**

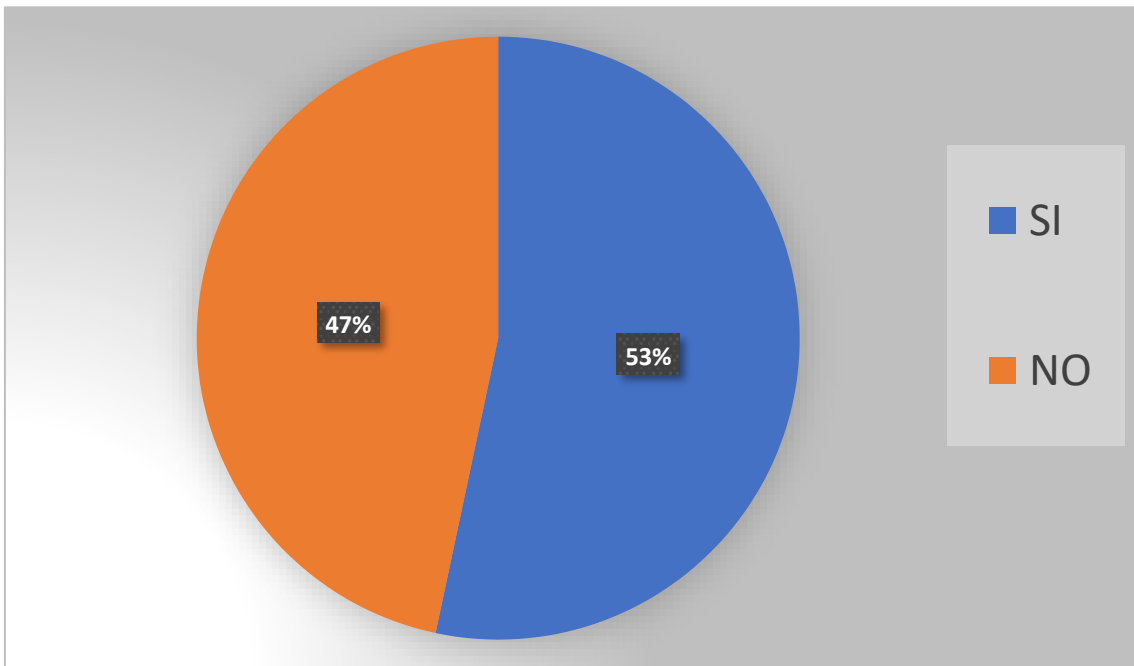
**¿Conoce sobre las vulnerabilidades de estos sistemas?**



**Nota:** En el siguiente grafico se puede observar que en su mayoría no conocen las vulnerabilidades que estos sistemas poseen con un 80% y solo el 20% Si conoce.

**Figura 3**

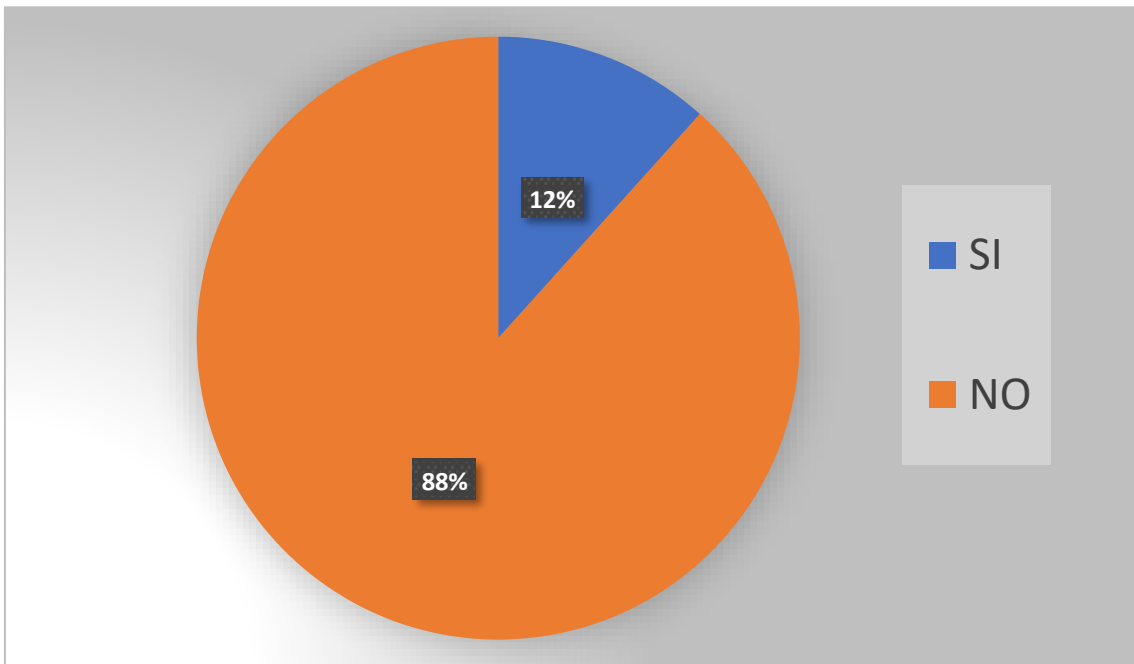
**¿Ha utilizado estos sistemas para realizar ataques informáticos en clases?**



**Nota:** Se puede observar en el grafico que el 53% de los encuestados si ha utilizado estos sistemas para realizar ataques, en cambio el 47% no lo ha hecho.

**Figura 4**

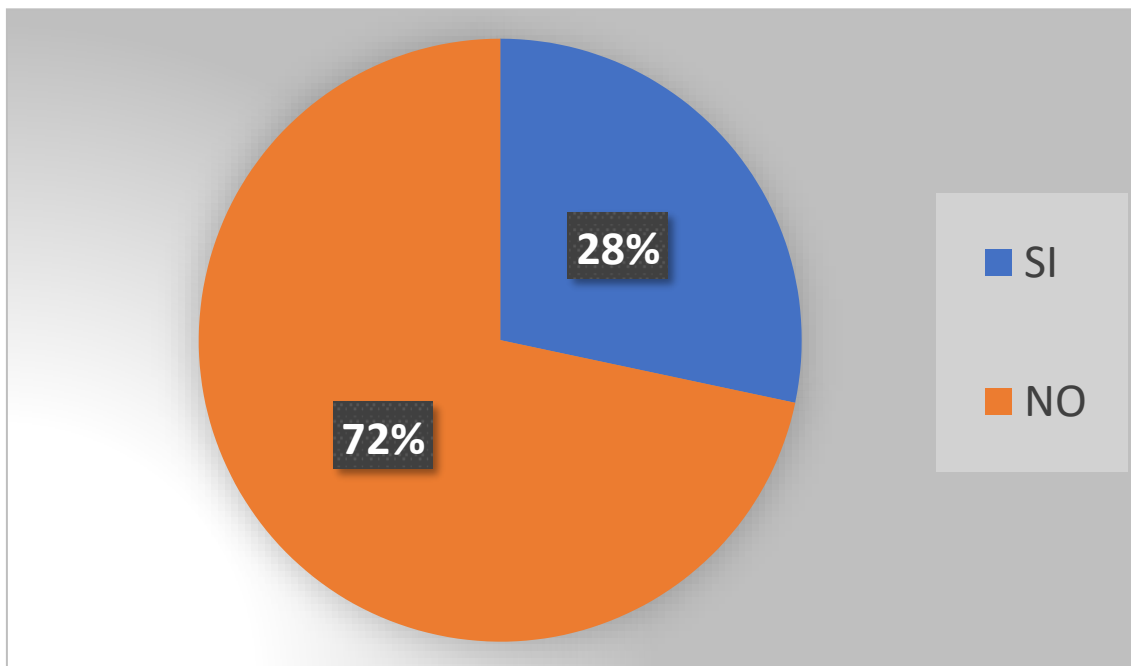
**¿Conoce las herramientas que estos sistemas poseen?**



**Nota:** Analizando el grafico se llegó a la conclusión de que el 88% de los encuestados no conocen las herramientas que estos sistemas operativos poseen y la minoría con un 12% desconoce estas herramientas.

**Figura 5**

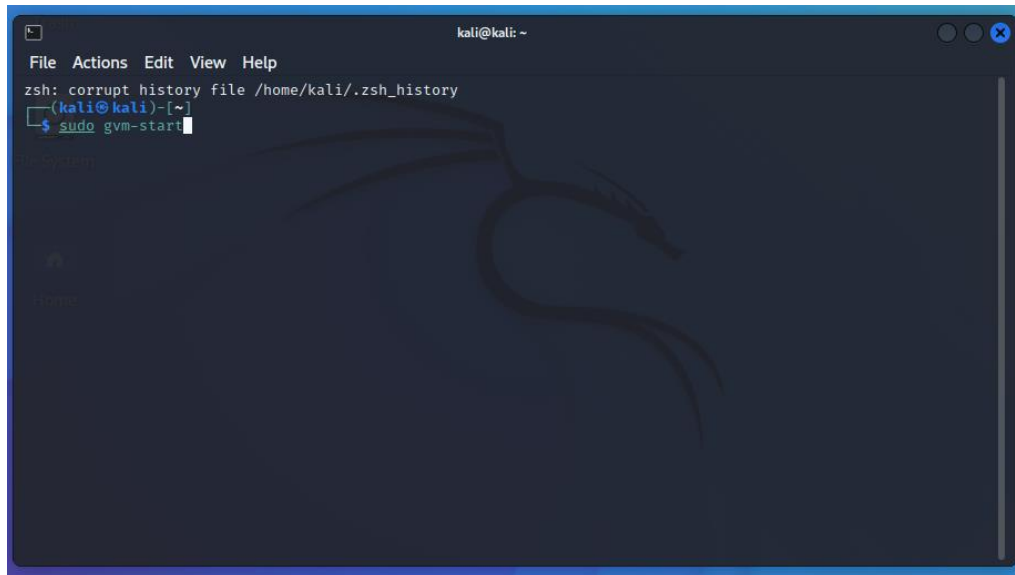
**¿Ha sido víctima de algún ataque informático?**



**Nota:** Según el grafico mostrado se llegó a la conclusión de que el 28% de los encuestados fue víctima de algún ataque cibernético, mientras que el 72% no.

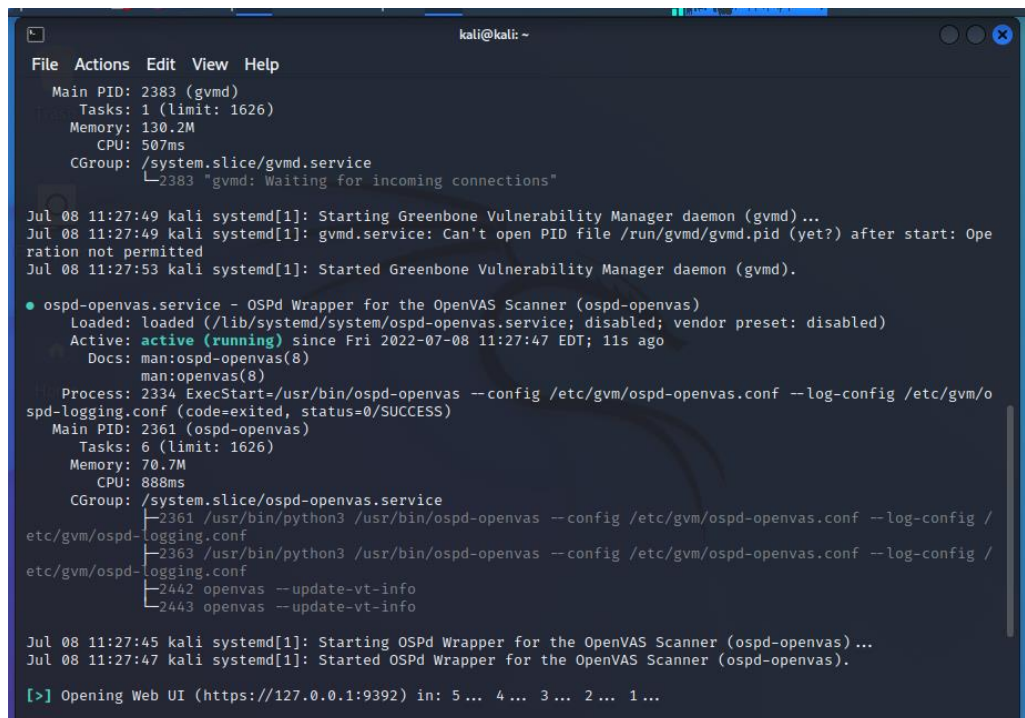


## INICIAR OPENVAS Y CONOCER LAS VULNERABILIDADES DE LOS SISTEMAS



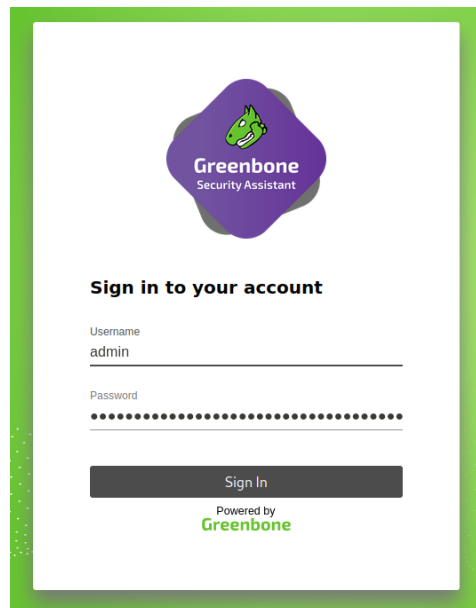
```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)~  
└─$ sudo gvm-start
```

## SE INSTALA OPENVAS EN KALI LINUX

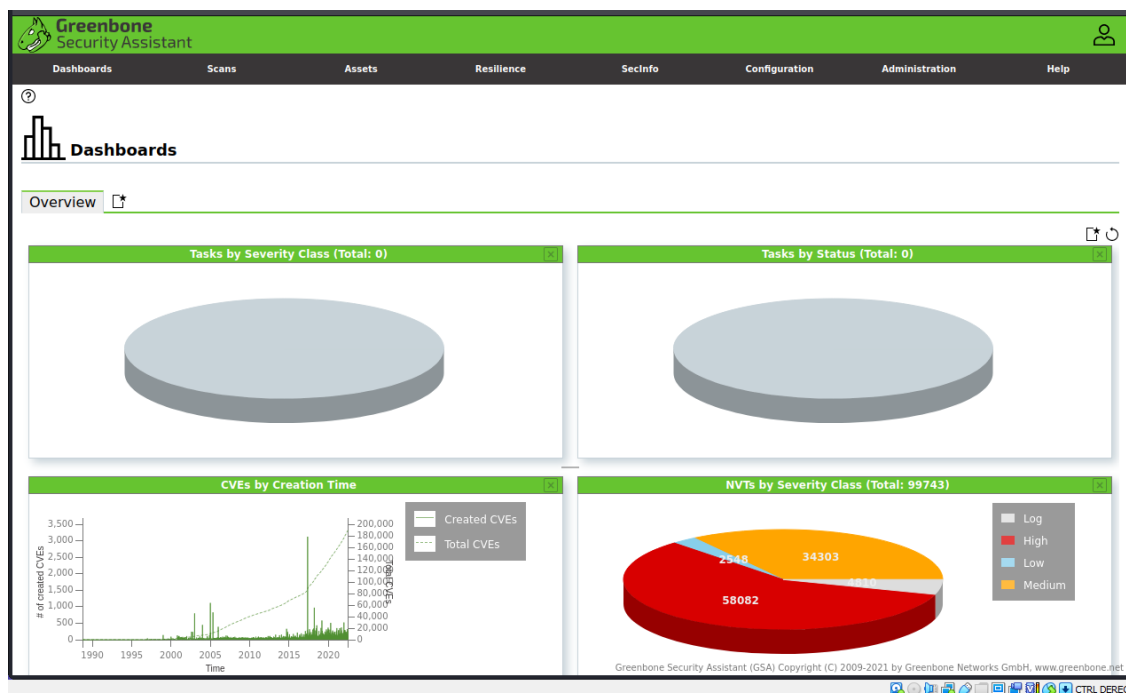


```
kali@kali: ~  
File Actions Edit View Help  
Main PID: 2383 (gvmd)  
Tasks: 1 (limit: 1626)  
Memory: 130.2M  
CPU: 507ms  
CGroup: /system.slice/gvmd.service  
└─2383 "gvmd: Waiting for incoming connections"  
  
Jul 08 11:27:49 kali systemd[1]: Starting Greenbone Vulnerability Manager daemon (gvmd) ...  
Jul 08 11:27:49 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: Operation not permitted  
Jul 08 11:27:53 kali systemd[1]: Started Greenbone Vulnerability Manager daemon (gvmd).  
  
● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)  
Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; vendor preset: disabled)  
Active: active (running) since Fri 2022-07-08 11:27:47 EDT; 11s ago  
Docs: man:openvas(8)  
man:openvas(8)  
Process: 2334 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)  
Main PID: 2361 (ospd-openvas)  
Tasks: 6 (limit: 1626)  
Memory: 70.7M  
CPU: 888ms  
CGroup: /system.slice/ospd-openvas.service  
└─2361 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf  
└─2363 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf  
└─2442 openvas --update-vt-info  
└─2443 openvas --update-vt-info  
  
Jul 08 11:27:45 kali systemd[1]: Starting OSPd Wrapper for the OpenVAS Scanner (ospd-openvas) ...  
Jul 08 11:27:47 kali systemd[1]: Started OSPd Wrapper for the OpenVAS Scanner (ospd-openvas).  
  
[>] Opening Web UI (https://127.0.0.1:9392) in: 5 ... 4 ... 3 ... 2 ... 1 ...
```

SE ABRE OPENVAS EN EL NAVEGADOR DESPUES DE HABER DESCARDO



INTERFAZ DEL PROGRAMA



## CONOCEMOS LA IP DE NUESTRO SISTEMA

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)~  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 172.16.51.13 netmask 255.255.252.0 broadcast 172.16.51.255  
inet6 fe80::a00:27ff:fedc:4c36 prefixlen 64 scopeid 0<20<link>  
ether 08:00:27:dc:4c:36 txqueuelen 1000 (Ethernet)  
RX packets 24164 bytes 2615747 (2.4 MiB)  
RX errors 0 dropped 750 overruns 0 frame 0  
TX packets 928 bytes 117548 (114.7 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0<10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 3596 bytes 6788782 (6.4 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 3596 bytes 6788782 (6.4 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)~
```

## CON LA IP QUE YA CONOCEMOS LA UTILIZAMOS PARA CONOCER LAS VULNERABILIDADES

The screenshot shows a web-based interface for a vulnerability scanner. At the top, there is a navigation bar with icons and a search filter. Below this, a header displays the report title: "Report: Fri, Jul 8, 2022 2:34 PM UTC" with a progress indicator at 93%. A sub-header shows the scan ID: "10221270-236f-4496-b7d5-3a334036886a" and other metadata like "Created: Fri, Jul 8, 2022 2:35 PM UTC".

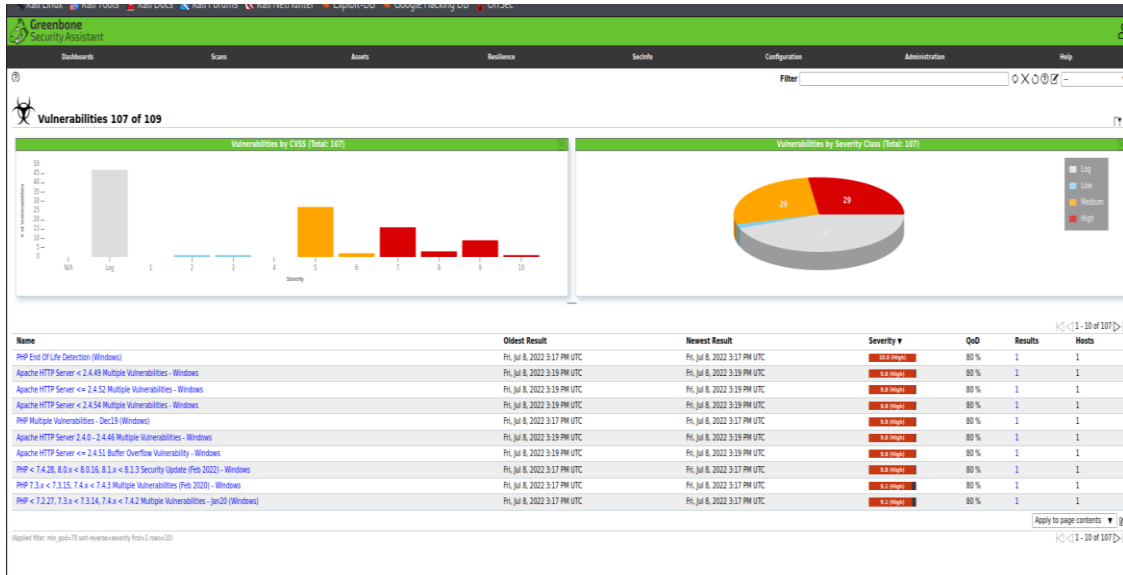
The main content area features a horizontal menu with tabs: "Information", "Results (87 of 476)", "Hosts (15 of 47)", "Ports (5 of 17)", "Applications (5 of 5)", "Operating Systems (3 of 4)", "CVEs (54 of 54)", "Closed CVEs (101 of 101)", "TLS Certificates (2 of 2)", "Error Messages (4 of 4)", and "User Tags (0)".

Under the "Information" tab, the following details are visible:

- Task Name: Immediate scan of IP 172.16.49.25/24
- Scan Time: Fri, Jul 8, 2022 2:35 PM UTC
- Scan Status: 93% (indicated by a green progress bar)
- Hosts scanned: 47
- Filter: apply\_overrides=0 levels=html min\_opd=70
- Timezone: Coordinated Universal Time (UTC)

At the bottom right of the interface, there is a small footer: "Copyright © 2013-2022 by Core Security Technologies, Inc. All rights reserved. www.coresecurity.com".

# DESPUES DE ESPERAR UNOS MINUTOS NOS VA A APARECER DE FORMA DETALLADA LAS VULNERABILIDADES QUE TIENE NUESTRO SISTEMA



**Report: Fri, Jul 8, 2022 2:34 PM UTC**

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
PHP End Of Life Detection (Windows)	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
Apache HTTP Server < 2.4.51 Buffer Overflow Vulnerability - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
PHP Multiple Vulnerabilities - Dec23 (Windows)	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Apache HTTP Server < 2.4.48 Multiple Vulnerabilities - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Apache HTTP Server < 2.4.52 Multiple Vulnerabilities - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
PHP 7.3.x < 7.3.25, 7.4.x < 7.4.3 Multiple Vulnerabilities (Feb 2020) - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
PHP < 7.2.21, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
PHP 7.3.x < 7.3.25, 7.4.x < 7.4.4 Multiple Vulnerabilities - Mar20 (Windows)	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
Apache HTTP Server 2.4.7 - 2.4.53 Multiple Vulnerabilities - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4012389)	High	95%	172.16.49.222		445tcp	Fri, Jul 8, 2022 3:26 PM UTC
Windows Multiple Vulnerabilities (Feb 2022) - Windows	High	80%	172.16.49.48		3396tcp	Fri, Jul 8, 2022 2:47 PM UTC
PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jan 2022) - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:17 PM UTC
Windows OS Vulnerability (MS02-25630) - Windows	High	80%	172.16.49.48		3396tcp	Fri, Jul 8, 2022 2:47 PM UTC
Windows Multiple Vulnerabilities (April 2022) - Windows	High	80%	172.16.49.48		3396tcp	Fri, Jul 8, 2022 2:47 PM UTC
Windows Multiple Vulnerabilities (April 2022) - Windows	High	80%	172.16.49.48		3396tcp	Fri, Jul 8, 2022 2:47 PM UTC
Apache HTTP Server 2.4.20 - 2.4.44 Multiple Vulnerabilities (Windows)	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Apache HTTP Server 2.4.41 - 2.4.46 NULL Pointer Dereference Vulnerability - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	High	99%	172.16.49.200		445tcp	Fri, Jul 8, 2022 3:26 PM UTC
Apache HTTP Server 2.4.36 - 2.4.49 OS Vulnerability - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC
Apache HTTP Server 2.4.17 - 2.4.49 'mod_proxy' HTTP2 Request Smuggling Vulnerability - Windows	High	80%	172.16.49.48		6093tcp	Fri, Jul 8, 2022 3:19 PM UTC



**Greenbone Security Assistant**

[Dashboards](#)
[Scans](#)
[Assets](#)
[Resilience](#)
[Security](#)
[Configuration](#)
[Administration](#)
[Help](#)

[PHP Live Detection \(Windows\)](#)
1.5
100%
172.26.49.48
80%
172.26.49.48
8092/tcp
Fri, Jul 8, 2022 3:17 PM UTC

[Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows](#)
1.5
100%
172.26.49.48
80%
172.26.49.48
8092/tcp
Fri, Jul 8, 2022 3:19 PM UTC

---

**Summary**

Apache HTTP Server is prone to a buffer overflow vulnerability.

**Detection Result**

Installed version: 2.4.43  
 Fixed version: 2.4.52  
 Install location  
 path / port: 8092/tcp

**Product Detection Result**

Product: cpe:/a:apache:http\_server:2.4.43  
 Method: Apache HTTP Server Detection Consolidation (OD: 1.3.6.1.4.1.25623.1.0.117320)  
 Log [View details of product detection](#)

**Insight**

A carefully crafted request body can cause a buffer overflow in the mod\_lua multipart parser (parsebody()) called from Lua scripts.

**Detection Method**

Checks if a vulnerable version is present on the target host.

Details: [Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows OD: 1.3.6.1.4.1.25623.1.0.117857](#)  
 Version used: 2021-12-29T12:12:57Z

**Affected Software/OS**

Apache HTTP Server versions through 2.4.51.

**Solution**

**Solution Type:** 0 Vendorfix  
 Update to version 2.4.52 or later.

**References**

CVE [CVE-2021-44790](#)  
 CERT [DPN-2021-11136](#)  
[DPN-2021-11135](#)  
[DPN-CERT-2022-1114](#)  
[DPN-2021-11137](#)

Greenbone Security Assistant (SSA) Copyright © 2004-2021 by Greenbone Networks GmbH. [www.greenbone.net](#)

# CASO DE ESTUDIO Villacis Wilman

8%  
Similitudes



< 1% Texto entre comillas  
0% similitudes entre comillas  
1% Idioma no reconocido

Nombre del documento: CASO DE ESTUDIO Villacis Wilman.docx  
Tamaño del documento original: 32,98 ko

Depositante: FREDY MAXIMILIANO JORDAN CORDONES  
Fecha de depósito: 12/8/2022  
Tipo de carga: interface  
fecha de fin de análisis: 12/8/2022

Número de palabras: 4802  
Número de caracteres: 32.358

Ubicación de las similitudes en el documento:



## Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<a href="https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/">www.tecnologia-informatica.com</a>   Todo sobre Vulnerabilidades informáticas: Cómo... https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/	4%		Palabras idénticas : 4% (216 palabras)
2	<a href="https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/">openwebinars.net</a>   Kali Linux: Qué es y características principales   OpenWebinars https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/	2%		Palabras idénticas : 2% (119 palabras)
3	<a href="https://www.greyhelmet.net/2019/04/legion-entorno-semiautomatico-de.html">www.greyhelmet.net</a>   Legion entorno semiautomático de pruebas de penetración d... https://www.greyhelmet.net/2019/04/legion-entorno-semiautomatico-de.html	2%		Palabras idénticas : 2% (87 palabras)
4	<a href="https://sistemas.acis.org.co/index.php/sistemas/article/view/129">sistemas.acis.org.co</a>   Ciberataques   Revista Sistemas https://sistemas.acis.org.co/index.php/sistemas/article/view/129	1%		Palabras idénticas : 1% (53 palabras)
5	<a href="https://www.cyberseguridad.com.mx/que-es-un-escaneo-de-vulnerabilidades-de-seguridad/">www.cyberseguridad.com.mx</a>   ¿Qué es un escaneo de vulnerabilidades de segurid... https://www.cyberseguridad.com.mx/que-es-un-escaneo-de-vulnerabilidades-de-seguridad/	< 1%		Palabras idénticas : < 1% (45 palabras)

## Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<a href="https://kolibers.com/blog/openvas.html">kolibers.com</a>   Openvas - Escáner de vulnerabilidades de código abierto. https://kolibers.com/blog/openvas.html	< 1%		Palabras idénticas : < 1% (37 palabras)
2	<a href="https://www.scielo.org.mx/scielo.php?script=sci_arttext&amp;pid=S2007-36072018000200005">www.scielo.org.mx</a>   Concientización y capacitación para incrementar la seguridad i... https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200005	< 1%		Palabras idénticas : < 1% (25 palabras)
3	CASO EDDER CASTILLO LEON.docx   CASO EDDER CASTILLO #04e5cf El documento proviene de mi grupo	< 1%		Palabras idénticas : < 1% (18 palabras)
4	Documento de otro usuario   Tarea 10 - Modelo de Seguridad Informática(3... #0728c6 El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (11 palabras)
5	<a href="https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En+informática,+una+vulner...">www.bancosantander.es</a>   Qué es una vulnerabilidad informática - Banco Santander https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En+informática,+una+vulner...	< 1%		Palabras idénticas : < 1% (12 palabras)

## Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

- <https://www.profesionalreview.com/2020/12/20/historia-windows-xp/>
- <https://www.iwebschool.com/blog/ciberseguridad-ataques-tecnologia/>
- [https://www.lasexta.com/tecnologia-tecnoplora/internet/adios-windows-historia-mejor-sistema-operativo-historia-microsoft\\_201904125cb0720d0cf2bee6b3f7b452.html](https://www.lasexta.com/tecnologia-tecnoplora/internet/adios-windows-historia-mejor-sistema-operativo-historia-microsoft_201904125cb0720d0cf2bee6b3f7b452.html)
- [https://issuu.com/fatimaabigailporrasnoriega/docs/f\\_tima\\_abigail\\_porras\\_noriega-vulnerabilidad\\_windo](https://issuu.com/fatimaabigailporrasnoriega/docs/f_tima_abigail_porras_noriega-vulnerabilidad_windo)
- <https://www.udsenderprise.com/es/blog/2020/10/09/kali-linux-instala-utilizar-distro-hacking-etico/>