UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL 2024 – AGOSTO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACIÓN

TEMA:

COMPARACIÓN DE LA EFICACIA DE LOS SISTEMAS OPERATIVOS KALI LINUX Y PARROT OS EN LA SEGURIDAD DE REDES EN LA UNIDAD EDUCATIVA BABAHOYO

ESTUDIANTE:

CESAR ARIEL CARREÑO NARANJO

TUTOR:

ING. ANDY BAYAS

AÑO 2024

ÍNDICE

RESUMEN

La seguridad de la información hoy en día es crucial debido al aumento de amenazas cibernéticas como malware, ransomware y ataques de phishing. La protección de datos y sistemas requiere una combinación de medidas preventivas y reactivas, incluyendo el uso de firewalls, antivirus y sistemas operativos para la seguridad de redes, además la actualización constante de software que ayuda a mitigar riesgos.

La seguridad de redes es un campo que se enfoca en proteger la integridad, confidencialidad y disponibilidad de la información y los recursos en una red informática. Implica una serie de prácticas, herramientas y tecnologías diseñadas para prevenir, detectar y responder a amenazas y ataques cibernéticos.

Kali Linux y Parrot OS son dos sistemas operativos populares en el ámbito de la seguridad de redes, cada uno con sus características distintivas. Kali Linux es conocido por su enfoque en pruebas de penetración y análisis de seguridad. Viene con una amplia gama de herramientas preinstaladas que permiten realizar auditorías exhaustivas de redes y sistemas.

Por otro lado, Parrot OS ofrece una suite similar de herramientas para seguridad y privacidad, pero con un enfoque adicional en la protección de la identidad y el análisis forense. Parrot OS proporciona una interfaz de usuario amigable y un entorno de trabajo optimizado para análisis forense y desarrollo de software. Destaca por su enfoque en la privacidad f, que enmascara el tráfico de red, y su integración con herramientas de análisis avanzado.

Palabras claves: Seguridad de la información, Kali Linux, Parrot Os, Seguridad de redes, amenazas cibernéticas.

SUMMARY

Information security is crucial today due to the rise of cyber threats such as malware, ransomware, and phishing attacks. Protecting data and systems requires a combination of preventive and reactive measures, including the use of firewalls, antivirus, and operating systems for network security, as well as constantly updating software that helps mitigate risks.

Network security is a field that focuses on protecting the integrity, confidentiality, and availability of information and resources on a computer network. It involves a series of practices, tools, and technologies designed to prevent, detect, and respond to cyber threats and attacks.

Kali Linux and Parrot OS are two popular operating systems in the network security arena, each with its distinctive features. Kali Linux is known for its focus on penetration testing and security analysis. It comes with a wide range of pre-installed tools that allow for thorough network and system audits.

On the other hand, Parrot OS offers a similar suite of tools for security and privacy, but with an added focus on identity protection and forensic analysis. Parrot OS provides a friendly user interface and an optimized working environment for forensic analysis and software development. It stands out for its focus on privacy, which masks network traffic, and its integration with advanced analysis tools.

Keywords: Information security, Kali Linux, Parrot OS, Network security, cyber threats.

PLANTEAMIENTO DEL PROBLEMA

La Unidad Educativa Babahoyo al igual que muchas instituciones educativas, enfrenta desafíos constantes en cuanto a la seguridad de sus redes informáticas. Con el aumento de amenazas cibernéticas y la necesidad de proteger datos sensibles de estudiantes, docentes y personal administrativo, la elección del sistema operativo adecuado para pruebas de penetración y auditorias de seguridad es crucial. Kali Linux y Parrot Os son dos sistemas operativos ampliamente reconocidos en el ámbito de la ciberseguridad, cada uno con características específicas que podrían influir en la protección y defensa de las redes de la Unidad Educativa Babahoyo.

En la actual era digital, el aumento global de técnicas de cibercrimen motivadas por fines lucrativos ha expuesto a las instituciones educativas a diversas amenazas. Esto se debe en parte a la poca atención destinada a la seguridad de la información, lo que resulta en un descuido en el mantenimiento de servidores, aplicaciones y software. Además, existen casos donde los equipo y sistemas utilizados son versiones obsoletas, aumentando aún más la vulnerabilidad de las instituciones frente a estos riesgos emergentes.

Las redes informáticas de las instituciones educativas, como la Unidad Educativa Babahoyo, enfrentan diversas amenazas a su seguridad como programas maliciosos, vulnerabilidades de software, entre otros.

La seguridad de la red es una de las consideraciones más importantes en el campo de la seguridad de la información hoy en día con la expansión de las dependencias de los sistemas de información en las instituciones educativas, la falta de medidas de seguridad en la infraestructura TI puede causar daños críticos que no son deseables para los procesos de la información académica.

El propósito de la seguridad de la red es principalmente evitar daños por el mal uso de los datos. Hay una serie de problemas potenciales que pueden ocurrir si la seguridad de la red no se implementa correctamente.

La falta de seguridad en la gestión de datos en las instituciones educativas puede impactar negativamente en la efectividad del proceso educativo y la administración escolar. Además, la correcta dirección estratégica en la gestión educativa y la educativa y la comunicación con los padres y la comunidad educativa puede verse comprometida por la falta de protección de la información. Esto podría resultar en la violación de la privacidad y confidencialidad de los datos dentro de la institución educativa.

Por lo tanto, es crucial que todo administrador de red implemente políticas rigurosas para prevenir posibles pérdidas, sin importar el tamaño o la naturaleza de la red. Estas políticas constituyen un conjunto de normas, regulaciones y procedimientos diseñados por el administrador o equipo de administradores de red para prevenir y supervisar accesos no autorizados, uso indebido, corrección, prevención de cambios y restricción del acceso a recursos informáticos y redes accesibles.

JUSTIFICACIÓN

En un entorno educativo como el de la Unidad Educativa Babahoyo, la seguridad de la información es prioritaria. La integridad de los datos personales, registros académicos y comunicaciones internas debe ser protegidas contra posibles vulnerabilidades y ataques maliciosos. La elección entre Kali Linux y Parrot Os no solo beneficia la capacidad de detectar y mitigar amenazas, sino también la eficiencia operativa y la facilidad de uso para el personal técnico encargado de la seguridad informática.

La Unidad Educativa Babahoyo, al igual que muchas instituciones educativas en la actualidad, depende en gran medida de su red informática para el desarrollo de sus actividades académicas y administrativas. Sin embargo, esta misma red se ha convertido en un blanco atractivo para los ciberdelincuentes, quienes buscan explotar vulnerabilidades para obtener acceso a información confidencial, interrumpir el funcionamiento de los sistemas o incluso tomar el control de dispositivos.

El uso de sistemas operativos especializados como Kali Linux y Parrot Os, si bien son herramientas valiosas para pruebas de penetración y análisis de seguridad, también introduce nuevos riesgos si no se implementan las medidas de control adecuadas. Es por ello que el presente estudio de caso tiene como objetivo exponer los argumentos que respaldan la necesidad de establecer un enfoque integral para la seguridad de redes en la Unidad Educativa Babahoyo, tomando en consideración el uso responsable de dichos sistemas operativos.

OBJETIVOS

Objetivo General

Comparar la eficiencia en la seguridad de redes entre los sistemas operativos Kali Linux y Parrot Os, para la protección de la infraestructura informática de la Unidad Educativa Babahoyo incluyendo la disponibilidad de documentación.

Objetivos Específicos

Evaluar las características de seguridad y las herramientas integradas en Kali Linux y Parrot Os.

Comparar la facilidad de la configuración de ambos sistemas operativos en el entorno educativo de la Unidad Educativa **Babahoyo**.

Analizar el rendimiento y la estabilidad de Kali Linux y Parrot Os en escenarios prácticos dentro del contexto de la Unidad Educativa Babahoyo.

LÍNEAS DE INVESTIGACIÓN

El presente caso de estudio está vinculado con la línea de investigación “Sistemas de información y comunicación, emprendimiento e innovación “. Además, está relacionada con la sublínea de redes y tecnologías inteligentes de software y hardware, que son coordinadas por la oficina de titulación de la facultad.

La relación de la línea de investigación con la investigación del caso es que aborda la seguridad de la información en infraestructuras tecnológicas. Este tema se conecta directamente con los sistemas de información y comunicación, así como el manejo de equipos informáticos para mejorar continuamente la seguridad.

En cuanto a la sublínea de investigación esta se relaciona debido a que la mayoría de los ciberataques se realizan a través de redes, infectando sistemas informáticos con aplicaciones maliciosas y comprometiendo datos críticos de las instituciones educativas, lo que afecta seriamente al personal administrado, docentes y estudiantes.

Además, es importante destacar dentro de la sublínea de investigación que las redes informáticas tienen como objetivo transportar datos, compartir recursos e información y para proporcionar servicios. Estos procesos son factibles debido a la interconexión de los equipos que conforman las redes. Es crucial garantizar la seguridad de la información que se transmite a través de la red, ya que ciertas áreas de la red pueden ser vulnerables.

Un administrador de sistemas de información se centra en optimizar la red de una empresa, garantizando el correcto funcionamiento de los sistemas informáticos y recursos en línea. Por otro lado, un especialista en ciberseguridad se dedica principalmente a identificar puntos débiles y vulnerabilidades en el sistema de seguridad de una red.

MARCO CONCEPTUAL

Sistemas Operativos

En el estudio realizado por (Albo Castro, 2020) indica que los sistemas operativos se reconocen ampliamente como un tipo de software diseñado para gestionar eficazmente los diversos componentes físicos de un sistema informático. Además de esta función fundamental de administración de hardware, los sistemas operativos también actúan como facilitadores esenciales entre los usuarios y el equipo, proporcionando un entorno donde las aplicaciones pueden ejecutarse de manera eficiente y permitiendo a los usuarios interactuar con el hardware de manera intuitiva y productiva. (p.3)

De igual manera (Bastidas García et al., 2023) da conocer que los sistemas operativos cumplen dos funciones fundamentales que son independientes entre sí: primero, proporcionan a los programadores de aplicaciones (y a las propias aplicaciones) un conjunto de hardware; segundo, administran eficazmente estos recursos de hardware. (p.10)

En base a esto expresamos que los sistemas operativos son programas o software que actúan como intermediarios entre el hardware de una computadora y los programas de aplicación. Son esenciales para que una computadora funcione, ya que gestionan los recursos del sistema, proporcionan interfaces para que los usuarios interactúen con la máquina y coordinan las actividades de los programas.

Por otro lado, los sistemas operativos son responsables de gestionar eficazmente todos los recursos de hardware disponibles en el sistema. Esto incluye la asignación de memoria, la gestión del procesador (CPU), la administración del almacenamiento y la gestión de dispositivos periféricos. La eficiencia en esta gestión es crucial para maximizar el rendimiento del sistema y asegurar que cada aplicación tenga acceso a los recursos necesarios sin interferir con otras aplicaciones en ejecución.

Clasificación

Según (Fernández Iglesias, 2023) nos dice que los sistemas operativos se pueden dividir en varios tipos como:

Sistemas de procesamiento por lotes: Estos sistemas operativos están diseñados para realizar tareas en grandes lotes sin requerir la interacción del usuario durante el procesamiento. Las tareas se agrupan y se procesan secuencialmente. Por ejemplo: IBM OS/360, MVS (Multiple Virtual Storage).

Sistema de asignación de tiempo: Permite que varios usuarios interactúen con el sistema simultáneamente compartiendo el tiempo de CPU. Cada usuario tiene la impresión de que tiene acceso exclusivo al equipo. Por ejemplo: UNIX, Multic.

Sistema operativo distribuido: Administran un grupo de computadoras independientes y las presentan como si fueran un sistema coherente. Los recursos y tareas se distribuyen entre diferentes nodos de la red. Por ejemplo: Amoeba, Plan 9, Google Fuchsia.

Sistema operativo en red: Proporciona servicios y recursos a través de una red, permitiendo a los usuarios acceder a recursos compartidos como archivos, impresoras y aplicaciones desde cualquier dispositivo conectado a la red. Por ejemplo: Novell NetWare, Windows Server, UNIX/Linux con NFS.

Sistema operativo en tiempo real: Están diseñados para resolver problemas en tiempo real bajo estrictas restricciones de tiempo. Las solicitudes deben cumplir plazos estrictos, lo que es importante para los sistemas integrados y los controles industriales. Por ejemplo: VxWorks, QNX, RTLinux.

Sistema operativo móvil: Optimizados para dispositivos móviles como teléfonos inteligentes y tabletas, estos sistemas operativos administran los recursos de manera

eficiente al tiempo que brindan interfaces táctiles y conectividad mejorada. Por ejemplo: Android, iOS, Windows Phone.

Cada tipo de sistema operativo está diseñado para un propósito específico. Por ejemplo, los sistemas operativos de escritorio están diseñados para computadoras personales y estaciones de trabajo. (p.4)

Se ejecutan en Windows, macOS y Linux. Proporcionan una interfaz gráfica de usuario y admiten muchas aplicaciones. Por otro lado, el sistema operativo de servidor. está diseñado para servidores y centros de datos como Windows Server, Linux Server y muchos otros sistemas operativos basados en Unix (por ejemplo, RedHat, Fedora, FreeBSD, Solaris, etc.). Ofrecen funciones como soporte multiusuario, acceso remoto y administración de recursos.

Kali Linux

Historia

Kali Linux es una distribución de Linux basada en Debian diseñada pensando en el pentesting. Anteriormente, Kali Linux se distribuía con el nombre "BackTrack", este nombre es una combinación de tres distribuciones de pentesting de Linux: IWHAX, WHOPPIX y Auditor.

BackTrack es uno de los sistemas más famosos de la distribución de Linux, como lo demuestra la cantidad de descargas que han alcanzado más de 4 millones desde BackTrack 4. Kali Linux 1.0 se lanzó el 12 de marzo de 2013. Cinco días después, se lanzó la versión 1.0.1 y para ese momento Kali se había descargado más de 90.000 veces.

Kali Linux 2.0 se lanzó el 11 de agosto de 2015. El objetivo de esta distribución es mejorar la experiencia del usuario final manteniendo la funcionalidad completa de las versiones anteriores. Una de las principales mejoras incluidas en Kali Linux 2.0 es el paso a la distribución continua. Esto significa que los desarrolladores de Kali Linux actualizan los paquetes a medida que se actualizan, proporcionando a los usuarios una plataforma estable y actualizada periódicamente.

Según (Vargas et al., 2020) Kali tiene un menú muy amplio con más de 300 herramientas para pentesting y otros. Se puede dividir en las siguientes categorías:

Recopilación de información (son herramientas se centran en la recopilación de datos que proporcionan información sobre los objetivos, especialmente herramientas de DNS, dominio e IP. Nmap en este Tipo);

Aplicación web (herramienta de análisis web red a nivel de servidor. Głoso y w3af para encontrar vulnerabilidades en sitios web);

Ataque de contraseña (herramienta para descifrar contraseñas, también conocida como Utilizan ataques de fuerza bruta o de diccionario para encontrar contraseñas. Acceso correcto a formularios o sistemas);

Ataques inalámbricos (herramientas Permiten analizar la red y diagnosticar su seguridad para poder conectarse a la red. red inalámbrica (WLAN) y pueden llevar a cabo una serie de ataques, especialmente escuchas se transmite información);

Herramienta de explotación (Metasploit Un entorno multiplataforma escrito en Ruby que abstrae tareas comunes invasión, ofreciendo un diseño modular en el que se pueden combinar e integrar diferentes tipos de ataques victoria);

Sniffing/spoofing (usando Wireshark y Ettercap puedes ver el tráfico de red) puede proporcionar acceso a información sensible y algunos otros tipos de ataques;

Ingeniería inversa (Ollydbg es uno de los mejores depuradores que puede ayudar entender la función de los archivos en el sistema como parte del proceso ingeniería inversa);

Forense (existen varias herramientas de análisis forense del sistema, es decir, puedes analizar directamente el estado del sistema cuando ocurre un incidente en particular; también puedes identificar acciones pasadas o archivos ocultos dentro del mismo, entre otros). (p.324)

Concepto

Según el estudio realizado por (Vinueza Gualotuña, 2021) nos dice que Kali Linux es una distribución de pruebas de seguridad informática que se utiliza para pruebas de penetración avanzadas. Incluye una variedad de herramientas para realizar tareas de seguridad de la información, incluida la informática forense, pruebas de penetración e ingeniería social. Está desarrollado, fundado y mantenido por Offensive Security, una empresa de formación en seguridad de la información. (p.4)

En base a esta información se puede decir que Kali Linux está diseñado específicamente para actividades relacionadas con la ciberseguridad, con un enfoque destacado en pruebas de penetración avanzadas. Esta especialización implica que la distribución esté optimizada y equipada con las herramientas necesarias para evaluar y fortalecer la seguridad de los sistemas y redes**.**

Además, incluye una amplia variedad de herramientas dirigidas a diversas áreas de la seguridad de la información. Estas herramientas van desde la informática forense hasta las pruebas de penetración y la ingeniería social, cubriendo así diferentes aspectos de la evaluación de la ciberseguridad.

El hecho de que Kali Linux sea desarrollado, fundado y mantenido una reconocida empresa especializada en capacitación en seguridad de la información, brinda credibilidad y confianza en la calidad y relevancia de la distribución. Esta asociación indica un compromiso con altos estándares en términos de herramientas y metodologías de seguridad.

Ventajas

Kali Linux viene con muchas herramientas de seguridad y pruebas de penetración preinstaladas, lo que lo convierte en una opción ideal para los profesionales de pruebas de penetración y ciberseguridad.

Debido a su popularidad en la comunidad de la ciberseguridad, Kali Linux tiene una gran base de usuarios activos y una comunidad sólida. Esto significa que puede encontrar fácilmente ayuda, tutoriales y recursos en línea.

Las actualizaciones periódicas, incluidas nuevas herramientas y actualizaciones de las herramientas existentes, son importantes para mantenerse actualizado con las últimas técnicas y vulnerabilidades de seguridad.

Esta es una excelente opción para los desarrolladores que necesitan realizar pruebas de seguridad de sus aplicaciones y sistemas antes de la implementación.

Aunque Kali Linux se centra principalmente en la seguridad, es una distribución de Linux completa que se puede personalizar y utilizar para fines generales como cualquier otra distribución.

Desventajas

Dado que Kali Linux se centra en pruebas de seguridad y penetración, esto puede ser un desafío para los nuevos usuarios de Linux. Para utilizarlo de forma eficaz se requieren conocimientos profundos en administración de sistemas y seguridad informática.

Debido a que contiene herramientas poderosas y potencialmente peligrosas, los usuarios con intenciones maliciosas pueden usarlo de manera inapropiada o ilegal.

A pesar de las importantes mejoras en esta área, Kali Linux puede experimentar problemas de compatibilidad con algunos dispositivos nuevos debido a ciertos controladores y configuraciones requeridas por las herramientas de seguridad. Actualizado con frecuencia.

Si bien las actualizaciones son beneficiosas desde una perspectiva de seguridad, pueden interrumpir su flujo de trabajo si no se administran adecuadamente, especialmente en entornos de producción.

Algunas herramientas y servicios incluidos pueden consumir importantes recursos informáticos, lo que puede afectar el rendimiento de sistemas más antiguos o limitados.

Parrot Os

Historia

El primer lanzamiento público tuvo lugar el 10 de abril de 2013, gracias al trabajo de Lorenzo Faletra, quien continúa liderando el desarrollo. Inicialmente desarrollado en Frozenbox (un foro comunitario creado por el propio creador de Parrot), el proyecto ha reunido a una comunidad de desarrolladores de código abierto, expertos en seguridad profesionales, defensores de los derechos digitales y entusiastas de Linux de todo el mundo. El proyecto tiene su sede en Palermo, Italia, y está gestionado por Parrot Security CIC, una empresa pública registrada en el Reino Unido.

Incluye un arsenal móvil completo de soluciones de seguridad informática y análisis forense digital. También incluye todo lo que se necesita para crear programas o proteger la privacidad mientras se navega por la web. Parrot está disponible en tres ediciones principales: Security, Home y Architect Edition, incluso como máquina virtual (Virtual Box, Parallels y VMware), en Raspberry Pi y en Docker.

A partir de la versión 5.0 LTS, regresa el soporte para la plataforma ARM (arm64 y Armhf) y algunas imágenes también están disponibles para placas como la Raspberry Pi. El sistema operativo viene con el entorno de escritorio MATE de forma predeterminada, pero se pueden instalar otros DE.

Concepto

Según (Cabañas Pérez, 2022) Parrot Os es una distribución GNU/Linux basada en Debian. Está destinado principalmente a pentesting, informática forense y criptografía. Basado en los puntos de referencia de Debian, tiene las últimas versiones de las herramientas incluidas y también cuenta con una importante comunidad de usuarios. Si surgen problemas, podemos pedir ayuda a otros usuarios. (p.30)

Con respecto a la información dada acerca de Parrot Os, esta es una opción sólida para quienes se especializan en pentesting. Al estar basado en Debian, hereda la estabilidad y el soporte de una de las distribuciones GNU/Linux más confiables. Además, al ofrecer las últimas versiones de herramientas importantes para estas áreas, como pruebas de penetración y análisis forense, garantiza que los usuarios siempre tendrán acceso a la funcionalidad más avanzada y actualizada.

La comunidad activa de Parrot OS es otra gran ventaja. La capacidad de conectarse con otros usuarios experimentados puede resultar invaluable cuando se encuentran problemas técnicos o se busca orientación. Esta red de apoyo no sólo proporciona ayuda práctica, sino que también fomenta el intercambio de conocimientos y la colaboración entre expertos en el campo.

Ventajas

Parrot OS está diseñado teniendo en cuenta la privacidad y el anonimato e incluye herramientas como Tor integrado y un entorno seguro para la navegación web anónima.

A diferencia de Kali Linux, Parrot OS tiene una interfaz de usuario amigable y atractiva, lo que lo hace más accesible para los usuarios que prefieren una experiencia más intuitiva y menos técnica.

AL igual que Kali Linux, Parrot OS tiene una comunidad activa de usuarios y desarrolladores que brindan soporte, tutoriales y recursos útiles.

Aunque se centra principalmente en la seguridad y la privacidad, es una distribución de Linux completa que se puede personalizar y utilizar para fines generales.

Desventajas

Aunque incluye potentes herramientas de seguridad y privacidad, es posible que tenga menos herramientas diseñadas específicamente para pruebas de penetración avanzadas que Kali Linux.

Al igual que Kali Linux, Parrot OS puede requerir una curva de aprendizaje intensa para los usuarios nuevos en Linux y el espacio de la ciberseguridad.

Como cualquier distribución de Linux, puede experimentar problemas de compatibilidad con cierto hardware nuevo, especialmente aquellos que requieren ciertos controladores.

Debido a sus capacidades mejoradas de anonimato y privacidad, Parrot OS, como Kali Linux, puede estar sujeto a un uso inapropiado o ilegal por parte de usuarios malintencionados.

Aunque se actualiza periódicamente para mejorar la seguridad y agregar nuevas funciones, las actualizaciones frecuentes a veces pueden causar problemas de estabilidad si no se usan correctamente.

Ciberseguridad

Según (Mendivil Caldentey, 2022) la ciberseguridad se ha convertido en una de las áreas TI que más atención y esfuerzo ha recibido en los últimos años, tanto para dar respuesta a la demanda, a la constante evolución y complejidad de los ataques y amenazas a la sociedad, como para desarrollar continuamente las tecnologías propias. En este entorno, el factor humano es decisivo en las actividades de educación y formación, y la ciberseguridad es un componente clave que requiere una continua profundización, actualización y mejora. (p.208)

Por otro lado (Orozco Bonilla, 2021) dice que la ciberseguridad incluye un conjunto de herramientas, controles de seguridad, políticas, enfoques de gestión de riesgos, operaciones, capacitación, mejores prácticas, seguridad y tecnologías diseñadas para proteger el entorno digital de la organización. Esta área incluye muchos elementos utilizados para proteger y controlar el ciberespacio interno. En comparación con la seguridad de la información, ambos campos tienen aplicaciones diferentes pero complementarias y son importantes a nivel estratégico. (p.4)

En base a dicha información se puede decir que la ciberseguridad se ha convertido en un campo crucial en la tecnología de la información debido a la creciente sofisticación y frecuencia de los ciberataques. Esta atención y los esfuerzos invertidos son necesarios para proteger a la sociedad de las amenazas digitales en constante evolución.

La ciberseguridad no es solo un tema técnico importante sino también un campo estratégico que requiere atención inmediata y constante, capacitación adecuada y un enfoque integral para proteger completamente la infraestructura y los activos digitales de la organización.

Análisis de Vulnerabilidades

En el estudio realizado por (Mora Zambrano, 2024) dice que el análisis de vulnerabilidades a pesar de su flexibilidad y movilidad, sigue siendo un importante desafío para la seguridad. Se necesitan técnicas como el análisis de registros, las pruebas de penetración, las pruebas de seguridad y el monitoreo continuo para identificar amenazas potenciales. (p.1)

Estas pueden incluir vulnerabilidades de protocolo, configuraciones incorrectas y fallas de dispositivos. Para minimizar este riesgo, se debe implementar protocolos de seguridad sólidos, actualizar el firmware periódicamente y realizar personalizaciones. Además, la capacitación de los usuarios y el monitoreo en tiempo real son aspectos clave para protegerse contra ataques. En resumen, al aprovechar estrategias de análisis integrales y soluciones proactivas, las instituciones educativas pueden proteger la integridad de los datos y la seguridad de sus redes.

El análisis de vulnerabilidades es un proceso crucial en la seguridad informática que se enfoca en identificar y evaluar debilidades en sistemas, redes y aplicaciones que podrían ser explotadas por atacantes. Estos son los aspectos claves que se realizan en este proceso: recopilación de información, identificación de vulnerabilidades, evaluación de riesgos, informe de resultados, mitigación, monitoreo continuo y cumplimiento y normativas.

Firewall

Según (Mora Bandera & Villero Contreras, 2019) informan que actualmente los firewalls juegan un papel importante en la seguridad informática de las redes empresariales debido a sus características y capacidad para proteger información y datos. Estos factores son importantes, tanto estratégica como operativamente, para cualquier organización que quiera seguir siendo competitiva. (p.1)

Por otro lado (Marín Valencia et al., 2020) da a conocer que es un servicio especializado que filtra información de manera proactiva mediante el monitoreo continuo del contenido publicado en línea. Según las políticas predefinidas de la empresa, determina si bloquear o permitir el tráfico. En el contexto del sistema creado, el firewall actuará como un filtro importante que protegerá la red local del acceso no autorizado y potencialmente peligroso desde el exterior. (p.88)

De acuerdo a la información recopilada acerca de los firewalls o también conocidos como los cortafuegos son piezas clave en la arquitectura de seguridad de las redes empresariales. Actúan como barreras protectoras que controlan y filtran el tráfico entrante y saliente según reglas predefinidas. Esto es crucial para evitar el acceso no autorizado y proteger la integridad de la información y los datos confidenciales de la organización.

Los firewalls desempeñan un papel importante en la seguridad de la red al filtrar el tráfico de manera proactiva y aplicar políticas de seguridad específicas para proteger contra el acceso no autorizado y potencialmente peligroso. Esto resalta su importancia como elemento esencial para proteger los activos digitales y la continuidad organizacional en entornos cibernéticos cada vez más complejos y amenazantes.

Red Informática

Según (Bolívar Díaz & Ayala, 2020) mencionan que una red es un medio que permite el intercambio de información entre personas o grupos de información y servicios. La tecnología de redes informáticas es una herramienta de recopilación que permite a las computadoras intercambiar información y recursos.

Una red informática es un conjunto de dispositivos conectados entre sí para compartir recursos y datos a través de medios de comunicación como cables de red, cables de fibra óptica o conexiones inalámbricas. Estos dispositivos pueden incluir computadoras, servidores, impresoras, dispositivos de almacenamiento y otros periféricos.

El objetivo principal es permitir la comunicación y el intercambio de información entre diferentes dispositivos conectados. Ofrece varias características y beneficios, como compartir archivos y recursos, colaboración en proyectos, comunicación instantánea por correo electrónico o texto y acceso a aplicaciones y servicios distribuidos.

Redes Alámbricas

Las redes alámbricas utilizan cables físicos para la transmisión de datos entre los dispositivos conectados. Ofrecen estabilidad y generalmente mayores velocidades de transferencia en comparación con las redes inalámbricas. Se utilizan en una variedad de entornos, desde redes domésticas hasta redes empresariales grandes.

Redes Inalámbricas

Para (Solórzano Álava et al., 2022) las redes inalámbricas son una tecnología que proporciona buenas velocidades de transferencia de datos y es fácil de instalar y configurar. Sin embargo, esto no garantiza la seguridad de la información transmitida. Por este motivo, cuando se transmite información a través de una red inalámbrica, pueden producirse interferencias, provocando que toda la información llegue de forma irregular y fuera del tiempo de recepción previsto.

Componentes De Una Red Informática

Routers: Dispositivos que enrutan datos entre diferentes redes, por ejemplo, entre una red de área local (LAN) y una red de área amplia (WAN), o entre diferentes redes de área local. Los enrutadores determinan la mejor ruta para los datos y pueden proporcionar funciones adicionales como NAT (traducción de direcciones de red), firewalls y VPN (redes privadas virtuales).

Switches: Dispositivos que conectan varios dispositivos en una red de área local (LAN) y admiten la comunicación entre ellos. Operan en la capa de enlace de datos del modelo OSI, enviando datos solo a un dispositivo de destino específico en lugar de transmitirlos a todos los puertos.

Hubs: Dispositivos centrales que conectan varios dispositivos en la red. Operan en la capa física del modelo OSI y envían datos a todos los dispositivos conectados independientemente del destino específico. Los hubs son menos eficientes que los switches y han sido reemplazados por ellos en la mayoría de los casos.

Access Points (AP): Dispositivos que permiten que los dispositivos inalámbricos se conecten a una red cableada, lo que extiende la cobertura de la red de área local (LAN) a áreas donde los cables no pueden llegar. Los puntos de acceso crean redes Wi-Fi y ayudan a conectar dispositivos móviles.

Computadoras: Dispositivos del usuario final acceden a la red para enviar y recibir datos, ejecutar aplicaciones y realizar tareas específicas. Puede ser una estación de trabajo, una computadora portátil o de escritorio.

Servidores: Las computadoras están diseñadas para compartir servicios, recursos y datos con otros dispositivos en una red. Pueden ejecutar aplicaciones de servidor, administrar bases de datos, almacenar archivos y proporcionar servicios de correo electrónico e Internet.

Impresoras y otros periféricos: Los dispositivos conectados a la red permiten a los usuarios acceder a servicios adicionales. Las impresoras de red permiten que varios usuarios impriman documentos desde diferentes dispositivos. Otros periféricos pueden incluir escáneres, cámaras de seguridad y dispositivos de almacenamiento.

Tipos de Redes

- Redes de área metropolitana (MAN)
- Redes privadas virtuales (VPN)
- **Redes LAN**

Para (Monterrubio-Hernández, 2023) indica que una red de área local (LAN) implica conectar varios dispositivos en una ubicación específica, como un hogar, una escuela o un negocio. Esta conexión permite que los dispositivos compartan recursos y se comuniquen entre sí a través de una red local. Como se mencionó anteriormente, las redes de área local generalmente están ubicadas en áreas relativamente pequeñas, pero no están limitadas en tamaño y pueden incluir muchos dispositivos que utilizan una única conexión de red. (p.1)

La información proporcionada muestra que una red de área local (LAN) es esencial para las comunicaciones internas en ubicaciones específicas, lo que permite compartir recursos y comunicarse de manera eficiente entre dispositivos. La flexibilidad, la escalabilidad y la capacidad de mejorar el rendimiento hacen que las redes de área local sean una infraestructura esencial en una variedad de entornos, desde el hogar hasta la empresa y la educación.

- **Redes WAN**

Según (Pita Tomalá, 2023) una red WAN es una infraestructura informática que cubre una gran área geográfica, a veces a nivel mundial. Estas redes combinan varias redes pequeñas en una sola unidad, lo que permite la comunicación y el intercambio de

recursos entre usuarios en diferentes ubicaciones, a altas velocidades de transmisión y diferentes niveles de datos. Estas conexiones utilizan dispositivos especializados como enrutadores, conmutadores y máscaras de subred para ayudar a conectar múltiples hosts de manera eficiente y segura. (p.10)

Este tipo de red es importante para empresas y organizaciones que operan a nivel global o regional porque proporciona la infraestructura necesaria para conectar de manera efectiva diferentes ubicaciones y facilitar la comunicación y el intercambio de recursos a través de una red local grande y diversa.

Topología de Red

Se llama topología de red al modelo de interconexión según el cual estén dispuestas las relaciones entre clientes y servidores. Existen tres modelos de topología de red:

Lineal o bus. El servidor está al inicio de la red, y los clientes están distribuidos por toda la red, siendo el único canal de comunicación un único canal, llamado bus o backbone.

En estrella. El servidor está en el centro de la red y cada cliente tiene una conexión única, por lo que cualquier comunicación entre máquinas debe pasar primero por ella.

En un anillo o círculo. Todas las máquinas están conectadas en círculo, en contacto con las más cercanas y son iguales, aunque el servidor mantiene su propia jerarquía.

Tabla 1

Cuadro comparativo

Característica	Kali Linux	Parrot OS
Propósito principal	Pruebas de penetración y auditorías de seguridad	Pruebas de penetración, auditorías de seguridad, y privacidad
Desarrollador	Offensive Security	Frozenbox Network
Base	Debian	Debian
Entorno de escritorio	GNOME, Xfce, KDE, LXDE, MATE	MATE, KDE, Xfce
Herramientas incluidas	Gran colección de herramientas para pruebas de penetración, forense y análisis	Amplia colección de herramientas para pruebas de penetración, forense, privacidad, y desarrollo
Rendimiento	Optimizado para pruebas de seguridad	Optimizado para pruebas de seguridad y uso diario
Requisitos de hardware	Mínimos: 1 GHz CPU, 1 GB RAM, 20 GB HDD	Mínimos: 1 GHz CPU, 1 GB RAM, 20 GB HDD
Gestor de paquetes	APT	APT

Soporte para arquitectura	x86, x64, ARM	x86, x64, ARM
Modelo de lanzamiento	Rolling release	Rolling release
Seguridad y privacidad	Algunas herramientas de anonimato	Fuerte enfoque en privacidad y anonimato
Documentación y soporte	Extensa documentación oficial y comunidad activa	Buena documentación oficial y comunidad activa
Facilidad de uso	Orientado a usuarios avanzados	Más amigable para principiantes y usuarios avanzados
Personalización	Alta personalización a través de configuraciones manuales	Alta personalización con herramientas integradas para facilitar ajustes

Fuente: Elaborado Por: *Cesar Carreño N.*

MARCO METODOLÓGICO

En el presente estudio de caso se centra en proporcionar una descripción detallada y precisa de los sistemas operativos Kali Linux y Parrot OS. Como parte de la comparación de eficacia, incluye la recopilación de información sobre las ventajas, desventajas, capacidades y especificaciones de ambos sistemas operativos.

La investigación descriptiva es esencial para construir una base de conocimiento sólida de como aborda la seguridad de redes los sistemas operativos Kali Linux y Parrot OS. Su propósito es proporcionar una descripción detallada y fácil de entender que describa las características, y la funcionalidad de cada sistema. Esto es muy importante para realizar las comparaciones porque permite comprender las capacidades y limitaciones de cada sistema antes de evaluar su efectividad.

Para poder realizar la comparación de la eficacia de los sistemas operativos Kali Linux y Parrot Os en la seguridad de redes también se utilizó la investigación bibliográfica donde debe se centra en recopilar y analizar fuentes existentes que brinda información relevante y oportuna.

La investigación cualitativa nos permite explorar las percepciones y experiencias de los usuarios con Kali Linux y Parrot OS. Este enfoque es importante para comprender la usabilidad y la satisfacción del usuario es por eso que se aplicó la entrevista como una herramienta poderosa para obtener información detallada y profunda sobre la eficacia de los sistemas operativos Kali Linux y Parrot OS.

Se va utilizar una excelente herramienta como lo es las entrevistas que brindan una mirada profunda a las experiencias de los usuarios individuales con Kali Linux y Parrot OS. Brindan la oportunidad de obtener información detallada y matizada sobre cómo los usuarios interactúan con cada sistema operativo.

En la investigación se realizó la entrevista a un maestro y al vicerrector de la Institución Educativa con las siguientes preguntas:

ENTREVISTA

1. ¿Conoce usted acerca de la ciberseguridad?
2. ¿Está de acuerdo en hacer capacitaciones sobre temas de seguridad informática?
3. ¿Cuáles han sido las principales vulnerabilidades que ha identificado en sus sistemas?
4. ¿Qué tipo de ataques ha enfrentado la Institución Educativa en el pasado?
5. ¿Qué medidas de seguridad tiene implementadas para prevenir ataques informáticos?
6. ¿Conoce las principales amenazas y vulnerabilidades que afectan a su infraestructura de red actualmente?
7. ¿Cuántos sistemas operativos diferentes se utiliza en la Institución Educativa?
8. ¿Está familiarizado con Kali Linux y Parrot Os?
9. ¿Estaría dispuesto en hacer capacitaciones sobre el uso de Kali Linux y Parrot Os?
10. ¿Es posible que implemente uno de estos sistemas operativos en la Institución Educativa?

RESULTADOS

A partir del análisis del presente caso de estudio, los resultados obtenidos mediante la aplicación de las estrategias metodológicas permitieron una comprensión clara de la funcionalidad y las limitaciones de cada sistema en el contexto de la ciberseguridad debido a que se proporcionó una descripción precisa y exhaustiva de ambos sistemas, incluyendo sus características, ventajas, desventajas, capacidades y especificaciones técnicas.

En el contexto actual, marcado por un incremento de ataques informáticos, es crucial llevar a cabo capacitaciones específicas para proteger la infraestructura tecnológica. Las charlas y formaciones en ciberseguridad son esenciales para que tanto estudiantes como docentes adquieran el conocimiento necesario para manejar y mitigar riesgos. La educación continua en esta área no solo fortalece la preparación del personal, sino que también contribuye a la creación de un entorno más seguro.

Las entrevistas realizadas identificado detectado dos vulnerabilidades críticas en el sistema de la Institución Educativa. En primer lugar, el uso de software obsoleto representa un riesgo significativo, que las versiones antiguas suelen tener brechas de seguridad que pueden ser explotadas por atacantes. En segundo lugar, la insuficiente segregación de la red interna permite que, en caso de un ataque, la amenaza pueda propagarse fácilmente por todo el sistema. Estas deficiencias no solo exponen a la institución a riesgos inmediatos, sino que también pueden comprometer la integridad de los datos y la seguridad general de la red.

Para abordar estas deficiencias, se sugiere considerar la implementación de sistemas operativos como Kali Linux o Parrot Os. Estas plataformas son conocidas por sus herramientas avanzadas para el análisis de vulnerabilidades, lo que permitiría identificar y mitigar riesgos de manera más efectivas. Adicionalmente, la adopción de estas herramientas podría proporcionar una visión más completa de las debilidades del sistema y contribuir a la protección y fortalecimiento de la infraestructura tecnológica de la institución.

DISCUSIÓN DE RESULTADOS

En base a los resultados obtenidos mediante la tabla de comparación entre Kali Linux y Parrot OS se puede deducir que la elección entre uno de estos sistemas operativos depende en gran medida de las necesidades y del perfil de usuario. Kali Linux cuenta con una rica colección de herramientas especializadas en pruebas de penetración y análisis forense, lo que lo convierte en la opción preferida por los expertos en seguridad y ciberseguridad. Su entorno está pensado para usuarios avanzados, y si bien ofrece una amplia personalización, requiere de un conocimiento profundo para aprovechar al máximo sus capacidades.

Por otro lado, Parrot OS no solo ofrece herramientas de pruebas de seguridad, sino que también pone mucho énfasis en la privacidad y el anonimato, lo que lo hace más versátil para usos cotidianos que necesitan proteger datos personales. La interfaz fácil de usar y las herramientas de configuración integradas lo hacen fácil de usar tanto para usuarios nuevos como experimentados. Además, su enfoque en la privacidad lo convierte en la solución ideal para aquellos que se preocupan por proteger sus datos personales y su anonimato en línea.

En resumen, Kali Linux es la elección correcta para quienes necesitan un entorno robusto y centrado en la seguridad, mientras que Parrot OS ofrece una solución más equilibrada y asequible que combina la ciberseguridad con herramientas seguras y fáciles de usar para el uso diario.

Kali Linux tiene como ventaja que es ampliamente conocido en la comunidad de ciberseguridad por sus numerosas herramientas de seguridad y pruebas de penetración preinstaladas. La integración con herramientas avanzadas y una documentación sólida lo convierten en la opción preferida de los profesionales de la seguridad. Pero la complejidad de Kali Linux puede ser un obstáculo para los usuarios novatos. Su pronunciada curva de

aprendizaje y su enfoque en las pruebas de penetración pueden no ser ideales para todas las necesidades de seguridad en el departamento de educación.

Por otro lado, Parrot OS también ofrece muchas herramientas de seguridad, pero su entorno es más amigable tanto para principiantes como para usuarios experimentados. Además, incluye funciones adicionales de seguridad y privacidad, lo que lo hace más versátil. Aunque es más accesible, puede carecer de las amplias herramientas especializadas que ofrece Kali Linux. Esto puede limitar su eficacia en situaciones de seguridad más complejas.

En la Institución Educativa, el factor decisivo es el nivel de conocimiento técnico del personal y los estudiantes. Aunque Kali Linux ofrece herramientas avanzadas, su complejidad puede ser un gran problema en este entorno. Parrot OS, con su enfoque más amigable para el usuario, puede ser más adecuado para aprender e implementar medidas de seguridad básicas y avanzadas.

La capacidad de proporcionar una capacitación adecuada es esencial. Kali Linux requiere una curva de aprendizaje más profunda, lo que puede ser un obstáculo si los recursos son limitados. La interfaz más intuitiva de Parrot OS puede permitir un aprendizaje más rápido y eficiente, lo que permite a los usuarios dominar las competencias clave en menos tiempo.

La investigación realizada afirma que ambos sistemas operativos son aceptados en la comunidad de seguridad informática, pero su efectividad depende del contexto de uso. La investigación descriptiva nos permite entender que mientras Kali Linux es más adecuado para entornos profesionales con altos requisitos técnicos, Parrot OS ofrece un equilibrio entre funcionalidad y accesibilidad, lo cual es muy importante en el contexto educativo de la Institución Educativa.

CONCLUSIONES

Kali Linux cuenta con muchas herramientas avanzadas de pruebas de seguridad y pruebas de penetración. La documentación es amplia y está bien organizada, lo que facilita que los usuarios avanzados comprendan y utilicen sus funciones. Mientras que Parrot OS si bien también ofrece una variedad significativa de herramientas de seguridad, su enfoque es más accesible y fácil de usar para diferentes niveles de experiencia. Parrot OS incluye funciones adicionales de seguridad y privacidad, lo que lo hace más versátil en entornos educativos.

En Kali Linux la configuración puede ser complicada y requiere un nivel avanzado de conocimiento técnico. Curva de aprendizaje pronunciada, que puede ser un obstáculo en entornos de aprendizaje donde los recursos y el conocimiento pueden ser limitados. Mientras que Parrot OS tiene una configuración más simple que facilitan la implementación y el uso en el entorno de aprendizaje de la Unidad Educativa Babahoyo. Los usuarios pueden aprender Parrot OS más rápido y de manera más eficiente, lo que es importante en entornos con recursos limitados.

En resumen, ambos sistemas operativos ofrecen importantes capacidades de ciberseguridad, Parrot OS se adapta mejor a las necesidades y los recursos del entorno educativo. La facilidad de uso, los bajos costos de instalación y el sólido rendimiento hacen de esta solución una opción más práctica para proteger su infraestructura de TI educativa. Kali Linux, si bien es potente y altamente especializado, puede ser más adecuado para usuarios experimentados que tienen el soporte técnico para administrar la complejidad y aprovechar al máximo sus capacidades. En general, Parrot OS ofrece una solución más accesible y sostenible para mejorar la ciberseguridad de la Institución Educativa, impulsando una adopción más amplia y efectiva entre el personal y los estudiantes y permitiendo una protección eficaz de la infraestructura de TI utilizando los recursos existentes.

RECOMENDACIONES

Dado que Parrot Os es más accesible y fácil de usar, se recomienda su implementación en la Unidad Educativa Babahoyo. Su configuración más simple y su proceso de aprendizaje más sencillo facilitarán su utilización por parte de las personas encargadas del departamento de TICs.

Es importante realizar programas de capacitaciones en ciberseguridad tanto para el personal administrativo como para los docentes y estudiantes que aborde temas de concia sobre amenazas cibernéticas y prácticas de seguridad ya que no solo protegerá a la institución contra amenazas informáticas, sino que también prepara a los estudiantes para un futuro en el que la ciberseguridad será una competencia cada vez más valiosa.

REFERENCIAS

Albo Castro, M. M. (2020). *Importancia de la calidad de la distribución GNU/Linux Nova para la informatización del sistema de salud de Cuba*. https://www.medigraphic.com/pdfs/acimed/aci-2020/aci204h.pdf

Bastidas García, J. M., Vargas Moreno, L. F., & Osuna Cerecer, E. R. (2023). ANÁLISIS DE RENDIMIENTO ENTRE LINUX Y WINDOWS EN LA EJECUCIÓN DE VIDEOJUEGOS UTILIZANDO DIFERENTES NIVELES DE HARDWARE. *Revista Digital de Tecnologías Informáticas y Sistemas*, *7*(1), 9–14. https://doi.org/10.61530/redtis.vol7.n1.2023.168.9-14

Bolívar Díaz, C., & Ayala, D. (2020). Red de alta velocidad que permite la cobertura de acceso a internet en parroquias rurales de América Latina. *Journal of Business and Entrepreneurial Studies*, *4*(1). https://dialnet.unirioja.es/descarga/articulo/7472734.pdf

Cabañas Pérez, J. (2022). *Análisis de vulnerabilidades en drones mediante el uso de aplicaciones Open-Source*. https://oa.upm.es/72249/1/TFG_JORGE_CABANAS_PEREZ.pdf

Fernández Iglesias, M. J. (2023). Conceptos básicos de sistemas operativos. *Universidad de Vigo*. https://doi.org/10.17605/OSF.IO/38MKS

Marín Valencia, J. J., Pariño Valencia, A., & Acevedo Bedoya, J. C. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. *Revista Universidad Católica de Oriente*. https://revistas.uco.edu.co/index.php/uco/article/view/284/370

Mendivil Caldentey, J. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Revista de Medios y Educación*. https://idus.us.es/bitstream/handle/11441/145488/Formaci%c3%b3n%20y%20concienciaci%c3%b3n%20en%20ciberseguridad%20basada%20en%20competencias.pdf?sequence=1&isAllowed=y

Monterrubio-Hernández, E. (2023). Redes locales. *Con-Ciencia Serrana Boletín Científico de La Escuela Preparatoria Ixtlahuaco*, *5*(10), 14–15. https://repository.uaeh.edu.mx/revistas/index.php/ixtlahuaco/article/view/11007/10469

Mora Bandera, E. F., & Villero Contreras, S. L. (2019). IMPORTANCIA DE LA IMPLEMENTACIÓN DE FIREWALL EN REDES EMPRESARIALES COMO MECANISMO PARA LA PROTECCIÓN DE INFORMACIÓN. *Revista Interdisciplinar de Estudios En Ciencias Básicas e Ingenierías*. https://dialnet.unirioja.es/servlet/articulo?codigo=8742508

Mora Zambrano, E. R. (2024). Análisis de vulnerabilidades en redes inalámbricas: métodos y soluciones. *Revista INSTA Magazine*, *7*(1). http://186.69.149.245/index.php/instamagazine/article/view/66/85

Orozco Bonilla, C. A. (2021). *ESTRATEGIAS ALGORÍTMICAS ORIENTADAS A LA CIBERSEGURIDAD: UN MAPEO SISTEMÁTICO*. https://dspace.ups.edu.ec/bitstream/123456789/20933/1/UPS-GT003374.pdf

Pita Tomalá, R. A. (2023). *IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE RED MEDIANTE REDES LAN Y WLAN, EMPLEANDO EQUIPOS DE REDES, PARA LA OPTIMIZACIÓN DE LA RED DE LA INSTITUCIÓN EDUCATIVA ANCÓN*. https://repositorio.upse.edu.ec/bitstream/46000/9256/1/UPSE-TTI-2023-0021.pdf

Solórzano Álava, W. L., Rodríguez Ixtlahuaca, A., Anzules Ávila, X. L., & Cornelio, O. M. (2022). Redes inalámbricas, su incidencia en la privacidad de la información. *Journal TechInnovation*, *1*(2), 104–109. https://doi.org/10.47230/journal.techinnovation.v1.n2.2022.104-109

Vargas, G., Guarda, T., Muyón, C., & Ninahualpa Quiña, G. (2020). *Obtención de claves en redes WLAN/WPS usando Wifislax y Denegación de Servicios con Kali Linux*. https://www.proquest.com/openview/f4b193b46ccb16a2fa7f1e3c633e8dd1/1?pq-origsite=gscholar&cbl=1006393

Vinueza Gualotuña, A. D. (2021). *ELABORACIÓN DE GUÍAS DE PRÁCTICAS DE LABORATORIO PARA LA ASIGNATURA SEGURIDAD DE REDES EMPLEANDO KALI LINUX*. https://bibdigital.epn.edu.ec/bitstream/15000/21434/1/CD%2010926.pdf

ANEXOS

Anexo 1. Encuestas

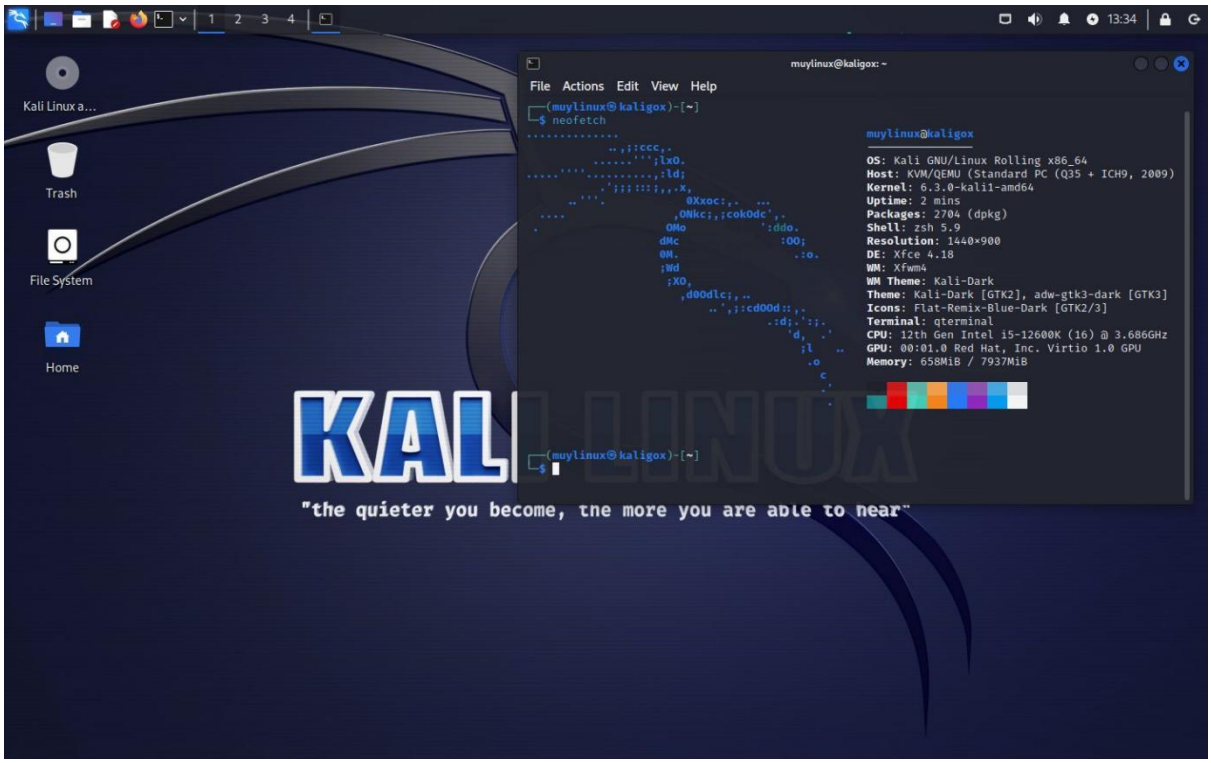
ENCUESTA REALIZADA A UN DOCENTE	
1. ¿Conoce usted acerca de la ciberseguridad?	Sí, estoy bastante familiarizado con el tema de ciberseguridad
2. ¿Está de acuerdo en hacer capacitaciones sobre temas de seguridad informática?	Sí, estoy de acuerdo en hacer capacitaciones ya que es esencial para proteger la infraestructura tecnológica y la formación de nuestro estudiantes y personal
3. ¿Cuáles han sido las principales vulnerabilidades que ha identificado en sus sistemas?	Se ha identificado vulnerabilidades relacionadas con software desactualizados
4. ¿Qué tipo de ataques ha enfrentado la Institución Educativa en el pasado?	En el pasado ha habido ataques de phishing hacia los docentes
5. ¿Qué medidas de seguridad tiene implementadas para prevenir ataques informáticos?	Se ha implementado una combinación de medidas preventivas como firewalls

6. ¿Conoce las principales amenazas y vulnerabilidades que afectan a su infraestructura de red actualmente?	Sí, se está al tanto de amenazas como los ataques de ransomware
7. ¿Cuántos sistemas operativos diferentes se utiliza en la Institución Educativa?	En la Institución Educativa solo se utiliza Windows
8. ¿Está familiarizado con Kali Linux y Parrot Os?	Sí, estoy familiarizado con ambos sistemas operativos
9. ¿Estaría dispuesto en hacer capacitaciones sobre el uso de Kali Linux y Parrot Os?	Sí, estoy dispuesto en realizar capacitaciones sobre ambos sistemas ya que podría ser beneficioso
10. ¿Es posible que implemente uno de estos sistemas operativos en la Institución Educativa?	Sí, estoy dispuesto en realizar capacitaciones sobre ambos sistemas ya que podría ser beneficioso

ENCUESTA REALIZADA AL VICERRECTOR	
1. ¿Conoce usted acerca de la ciberseguridad?	Sí, tengo un profundo conocimiento acerca de la ciberseguridad y su importancia en el entorno educativo
2. ¿Está de acuerdo en hacer capacitaciones sobre temas de seguridad informática?	Sí, es bueno adquirir más conocimientos con respecto al tema
3. ¿Cuáles han sido las principales vulnerabilidades que ha identificado en sus sistemas?	Una de las vulnerabilidades identificada es la falta de segmentación adecuada en la red interna
4. ¿Qué tipo de ataques ha enfrentado la Institución Educativa en el pasado?	Uno de los ataques que ocurrieron fueron los intentos de acceso no autorizado a través de vulnerabilidades en software no actualizados
5. ¿Qué medidas de seguridad tiene implementadas para prevenir ataques informáticos?	Se ha realizado capacitaciones para los docentes y estudiantes sobre las prácticas de seguridad como el manejo seguro de correos

6. ¿Conoce las principales amenazas y vulnerabilidades que afectan a su infraestructura de red actualmente?	Si, una de las tantas que es el phishing que sigue siendo una preocupación importante
7. ¿Cuántos sistemas operativos diferentes se utiliza en la Institución Educativa?	Por el momento solo contamos con el Windows 10
8. ¿Está familiarizado con Kali Linux y Parrot Os?	Sí, tengo más conocimiento de Kali Linux que de Parrot Os
9. ¿Estaría dispuesto en hacer capacitaciones sobre el uso de Kali Linux y Parrot Os?	Definitivamente, estoy abierto a capacitaciones sobre estos sistemas operativos porque fortalece las habilidades en seguridad informática
10. ¿Es posible que implemente uno de estos sistemas operativos en la Institución Educativa?	La implementación de uno de estos sistemas operativos es factible y podría ser evaluada más a fondo

Anexo 2. Sistema Operativo Kali Linux



Anexo 3. Sistema Operativo Parrot Os