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:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANALISIS DE VULNERABILIDADES DE REDES INALAMBRICAS CON EL EMPLEO DEL SISTEMA OPERATIVO KALI LINUX USANDO LA HERRAMMIENTA WIRESHARK EN LA DISTRIBUIDORA DE PRODUCTOS DE PAPELERIA ESTELAR S.A.

ESTUDIANTE:

CADENA PINELA JOHN ALEXANDER

TUTOR:

ING. ANDY BAYAS HUILCAPI

AÑO 2024

Contenido

Planteamiento del problema ……. 3

Justificación…… 7

Objetivos del estudio …… 9

Líneas de investigación…… 10

Marco conceptual……. 11

Marco metodológico…… 21

Resultados…… …… 23

Discusión de Resultados…… 24

Conclusiones……. 28

Recomendaciones……. 29

Referencias…… 30

Anexos ……. 33

Planteamiento del problema

A nivel mundial en la década de los noventa se rompió el paradigma de usar cables como medio de comunicación, en los últimos años las redes de área local Inalámbrica (WLAN, Wireless) se está haciendo popular, Ecuador ha tenido un gran desarrollo tecnológico en los medios de comunicación, es así que muchas empresas ofertan el servicio de internet aprovechando los distintos medios posibles, esto ha llevado que las principales ciudades cuenten con todas las opciones de servicio de comunicación que existen en la actualidad.

En Ecuador a consecuencia a la pandemia que se vive desde el año 2020, internet creció debido al teletrabajo y las clases virtuales la mayoría de los usuarios optaron en adquirir un servicio de internet. A nivel nacional viviendo un incremento en los usuarios de internet de un 7.7% en el porcentaje de hogares con acceso a internet.

El tráfico de redes es un problema que ha surgido desde la creación de redes inalámbricas donde los principales afectados son los usuarios de dichas redes porque a medida que aumenta el tráfico de red también disminuye el interés de los usuarios de poder contar con una red de Internet. Según “Actualmente la seguridad se ha convertido en uno de los principales problemas de los sistemas de acceso inalámbrico”, lo que afecta a los usuarios que tienen que recurrir a las medidas de seguridad más costosas para tener un mejor servicio de red Wi-Fi, hoy en el mundo existen diferentes aplicaciones y herramientas para descubrir la clave de una red en donde una persona puede pasar por alto debido a la falta de conocimiento sobre las redes.

Ecuador es uno de los países con mayor vulnerabilidad con el tráfico de red debido al hecho de que hay muy poco interés en trabajar en la seguridad de los usuarios, pero a medida que pasa el tiempo, se observa una mayor responsabilidad por parte de las empresas privadas que comparten el recurso de Internet para que de esta manera las personas que adquieren el servicio no se vean afectadas por el tráfico de la red.

La ciberseguridad es sin duda un campo crucial debido a la creciente demanda y las vulnerabilidades asociadas, especialmente en redes inalámbricas. Estas redes son ampliamente reconocidas como menos seguras en comparación con las redes cableadas, dado que los datos transmitidos a través de ellas pueden ser interceptados si no se implementan las medidas de seguridad adecuadas.

Debido a la gran demanda de este tipo de red las probabilidades de sufrir algún ataque o cualquier tipo de robo de datos es muy elevada, por lo tanto, cualquier usuario está expuesto a sufrir este tipo de ataque y que le roben información privada para cualquier medio ilícito.

La captura de datos cifrados en estas redes representa un riesgo significativo, ya que la información sensible o confidencial, tanto de organizaciones como de redes domésticas, puede estar en riesgo. Esto podría incluir desde datos financieros y personales hasta información estratégica de negocios.

Por lo tanto, es crucial que tanto las empresas como los usuarios domésticos implementen medidas de seguridad efectivas, como el cifrado fuerte de datos, configuraciones de red seguras, actualizaciones regulares de software y conciencia constante sobre las amenazas cibernéticas.

Aunque las redes inalámbricas ofrecen una gran conveniencia, presentan un reto significativo en términos de seguridad. Proteger adecuadamente estas redes es fundamental para evitar la exposición no autorizada de datos sensibles y mitigar los riesgos asociados con la ciberseguridad en el mundo digital actual.

De la misma manera el tráfico de cada red inalámbrica es muy alto en especial las redes abiertas ya que hay muchas personas se conectan a la red para poder navegar o usar las redes sociales sin embargo las personas se conectan sin el conocimiento de cómo esto puede perjudicarlos con el simple hecho de conectarse a la red sin necesidad de hacer un registro con el correo personas o también haciendo el registro.

La incidencia del tráfico de red es un problema que está presente en nuestra vida cotidiana, por eso se hace un llamado a los seres humanos para que sean más cautelosos con las claves de sus redes Wi-Fi y les den doble seguridad para que no puedan tiene problemas con los piratas de las redes inalámbricas.

Las redes inalámbricas han provocado un impacto en los ámbitos sociales y económicos, tanto la comunicación como la transferencia de datos, han pasado de ser herramientas ancladas a un lugar y conectadas con cables o componentes que pueden ser trasladados y ser utilizados mientras nos movemos, en cualquier momento o en cualquier sitio. Por tanto, se han convertido en dispositivos con tecnologías que permiten realizar actividades que antes sólo podíamos desarrollar mientras estábamos sentados en una oficina de una empresa, en el hogar o en un centro de investigación

En el presente trabajo se buscó analizar las vulnerabilidades de redes inalámbricas con el empleo del sistema operativo kali linux usando la herramienta wireshark en la distribuidora de productos de papelería ESTELAR S.A**.**

Justificación

Actualmente en el país lo que más se está llevando a cabo son las redes inalámbricas abiertas en los espacios abiertos como lo puede ser parques, terminales, centros comerciales en los cuales la mayoría te pide hacer un registro para poder acceder a dicha red y tener la posibilidad de navegar.

Normalmente para poder ingresar a estas redes pide que se ingrese con el correo electrónico propio del usuario y así quedar registrado ya que si se quiere volver a ingresar en muchas ocasiones no se requiere ingresar nuevamente el correo electrónico del usuario para volver a conectarse.

En otras redes inalámbricas no se necesita ingresar con el correo electrónico simplemente se selecciona la red y ya el usuario está conectado y puede navegar libremente, muchas veces el tráfico de esta red es demasiada alta ya que hay cientos de personas que se conectan, la velocidad de navegación disminuye y por ende el usuario tiende a tener molestias al momento de navegar.

Sin embargo, los usuarios que se conectan a estas redes ingresando o no el correo electrónico, no conoce los peligro que incluye esta ya que con el simple hecho de conectarse a una red de la que no se tenga información o sea desconocido es un peligro, en ciertas ocasiones simplemente al conectarse a estas redes ya nos pueden estar robando la información de los usuarios que se vayan a conectar a estas redes

Al ser una red debe garantizar la confidencialidad, integridad y disponibilidad de la información que se transmite disponiendo de seguridad ya que es un punto vulnerable en este tipo de redes, las amenazas de accesos no autorizados, ataques cibernéticos y vulnerabilidades ocurren en cualquier momento.

En Ecuador la ciberseguridad es un tema innovador en los últimos años, cierto porcentaje de empresas públicas y privadas han sido víctimas de ataques cibernéticos a sus sistemas informáticos, poniendo en riesgos datos importantes de instituciones publica como privadas, esto debido a que hay varias empresas no tienen un sistema de seguridad que controlen los sistemas de los equipos tecnológicos por lo que los hace más vulnerables a los ataques cibernéticos que existen en la actualidad.

En los actuales momentos a nivel mundial el uso de nuevas infraestructuras tecnologías son una base fundamental para el uso de las instituciones en sus diversas actividades, el manejo de la información y de los datos proporcionados por cada una de ellas, por lo tanto si no se tiene un buen sistema que permita mantener a salvo la información estas estarán expuestas a sufrir ataques cibernéticos o que hacker intenten irrumpir en sus sistemas mediante la vulnerabilidad que existe a través de redes inalámbricas e intenten apropiarse de la información para hacer buen o mal uso de los datos, esto es una parte fundamental para mantener la integridad, confiabilidad y autenticidad de la información

Objetivos

General

Evaluar la red inalámbrica para determinar el nivel de seguridad de la empresa ESTELAR S.A. mediante el sistema operativo kali linux usando la herramienta wireshark

Específicos

- Establecer los controles de seguridad que serán evaluados para determinar el nivel de seguridad.

- Evaluar la red inalámbrica mediante el escenario de pruebas y controles establecidos para determinar el nivel de seguridad.

- Analizar las vulnerabilidades encontradas de acuerdo a los riesgos detectados en la red.

LINEA DE INVESTIGACION

Sistemas de información y comunicación, emprendimiento e innovación.

SUBLINEA DE INVESTIGACION

Redes y tecnologías inteligentes de software y hardware

Marco conceptual

Según (Rusdianti, 2024) una red inalámbrica es un sistema de comunicación de datos que posee un área de cobertura para brindar una conexión inalámbrica entre equipos, la transmisión y recepción de datos se los realiza mediante ondas electromagnéticas teniendo como medio de transmisión el aire. Existen diferentes tecnologías de transmisión de espectro ensanchado y los rangos de frecuencia que se utiliza en 802.11

De acuerdo con (Solórzano Álava et al., 2022) las redes inalámbricas "Son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas", lo que hace que las personas sean vulnerables para el hurto de la información a través de una red inalámbrica y optan por cambiarse a una red cableada.

También los usuarios ven afectado el rendimiento de la red porque muchas veces de esa red que tienen en sus casas están conectados sus teléfonos, las redes inalámbricas no solo se emplean para realizar conexiones de datos, también se utilizan para emitir señal de televisión, telefonía, para seguridad webcam.

En el mundo actual se ve la necesidad de realizar un análisis en la que permita acceder a la seguridad en las redes inalámbricas, estas son utilizadas por distintas organizaciones por la fácil instalación, por la conexión y por el bajo precio, el fin de esta investigación de dar conocimiento sobre los peligros que puede llevar conectarse a una red inalámbrica desconocida.

La información de estas redes viajan por medio de las ondas de radio quedando así la información vulnerable a varios ataques con propósito malicioso, en la que así se pueden aprovechar de los protocolos existentes que no son seguros, cada cierto tiempo una revisión da seguridad en las redes, así se pueden evitar ataques, existen herramientas que se pueden utilizar para observas el nivel de seguridad en la que se verifican los ataques permitiendo asi mejorar la seguridad en las redes inalámbricas.

De acuerdo con (Stalin et al., 2023) el uso de las tecnologías de la información y redes WiFi es cada vez más extenso en el mundo, por tal razón, la seguridad informática hoy en día es un tema de preocupación e importancia para cualquier empresa u organización, lo que significa que las entidades deben reconsiderar por completo la forma de tener protegidas las redes y los dispositivos, las vulnerabilidades van en aumento cada que pasa ya que las redes inalámbricas están propensas a que pase en cada momento un ataque, la que lleva a la divulgación de activos críticos y relevación de información.

Redes WAN

De acuerdo con (Rodriguez Toala et al., 2022) las WAN públicas son operadas por proveedores de servicios de Internet para permitir a sus clientes el acceso a este. Las redes que son privadas de un área amplia, son utilizadas principalmente por las empresas para permitir los servicios en la nube y para que se puedan conectar las redes en las diferentes sedes de la empresa.

La historia de esta red WAN da inicio en el año 1993, cuando las personas Lawrence Roberts y Thomas Merrill les surge la idea de conectar dos ordenadores, uno es un DX-2 en laciudad de Massachusetts junto con un Q-33 en la ciudad de california, a través de una línea telefónica de baja velocidad, creando la primera red de área amplia

Este tipo de red es necesaria por el crecimiento de los negocios de redes, e donde las redes LAN ya no serían suficientes, porque se requiere una forma para poder pasar la información de la empresa a otra de una manera más rápida y más eficiente, la red WAN se puede conectar a redes de un área amplia en la que va a permitir una comunicación de larga distancia.

Redes LAN

De acuerdo con (Capinera, 2021) una red de área local (LAN) es una red informática que conecta las computadoras en un área subjetivamente pequeña y predeterminad. Sobre todo, tienen la posibilidad de conectar entre ellas por medio de líneas telefónicas y ondas de radio, permitiendo compartir bases de datos, programas y periféricos como podría ser un módem, una impresora, un escáner, entre otros; poniendo a nuestra disposición otros medios de comunicación como tienen la posibilidad de ser la correspondencia electrónica y el chat.

Cabe destacar que una red de área local ofrece ahorros fundamentales, tanto en términos de dinero, ya que no es necesario comprar muchos dispositivos y consume menos papel, y en un acceso al internet se puede usar una exclusiva conexión telefónica compartida por diversas computadoras conectados en red; como de tiempo, debido a que se consigue administración de la información y del trabajo.

Seguridad Física

De acuerdo con (Pacheco, 2022) esta componente se relaciona con el acceso físico a la infraestructura, desde el punto de vista de las redes de comunicaciones es un tema crítico para tomar en cuenta, ya que en la red la capa de acceso, interactúa directamente con los usuarios. Además, en el punto de vista la conexión a los proveedores de servicios, los medios usados para el transporte de datos en la planta externa pueden estar expuestos a intervenciones humanas o ambientales.

Gestión de red

La gestión de acuerdo con (Jesús et al., 2022), “es vital para funcionar de forma eficiente y generar estrategias para participar de la compartición de información y conocimiento”. En gestión de red se trata de la planificación, la organización, supervisión y el control de los elementos de comunicaciones, con el fin de garantizar un adecuado nivel de servicio, y de acuerdo con un determinado costo. Los objetivos principales de esta gestión consisten en mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad

Ciberseguridad

Según (Ospina & Sanabria, 2020) la ciberseguridad (o seguridad informática) se origina para tomar medidas para la protección de infraestructura, software y hardware, contrarrestando las posibles amenazas mediante internet, y para desarrollar estrategias de contraataque. Esta perspectiva implicó la creación de sinnúmero de normas y sanciones para 203 Desafíos nacionales frente a la ciberseguridad en el escenario global

La ciberseguridad garantiza que se mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos correspondientes en el ciber entorno. La aplicación implica los aspectos estructurales que son los elementos computacionales que van a generar capacidades, fuerzas y dominio en el ciberespacio, pues estos son los que han venido a hacer presencia en las confrontaciones de ingeniería social, por lo tanto, propuso realizar ciertos estudios en concreto sobre el concepto que permitan.

Ciberataques

Según (Feito et al., 2023) El auge de la digitalización de las empresas y el teletrabajo debido a la pandemia ocasionada por la Covid-19 se ha visto acompañado de un aumento en el número de ciberataques. Según un artículo publicado en El Mundo, se han dado de media 40.000 ciberataques cada día durante 2021, solo en España

Otro acontecimiento que generó un incremento de ciberataques a nivel mundial fue el comienzo del conflicto entre Ucrania y Rusia tras el inicio de la invasión rusa el 24 de febrero de 2022. Entre los objetivos de los ataques derivados de esta situación política se encuentran administraciones públicas, servicios esenciales e infraestructuras críticas de diversos países, entre los que destacan los miembros de la OTAN.

Desde que se inició la invasión de Ucrania, en España han sufrido este tipo de ataques compañías de infraestructuras críticas como Iberdrola, entidades públicas como la Policía Nacional o la Agencia tecnológicas como Microsoft y Apple, como en la gran mayoría de bancos españoles (BBVA, Santander, Caixabank, Sabadell Liberbank), entre otros.

Los ciberdelincuentes (Hackers)

Según (Arroyo, 2020) la perspectiva de manera criminológica, es el estudio del sujeto que va a comete el delito, de una manera especial de importancia para una adecuada política preventiva, debido a los estudios de categoría criminológico estos deben tener en cuenta las circunstancias que son concretas del fenómeno criminal y de las personas, la identificación de los “perfiles” puede ser una técnica muy eficaz para poder introducir las políticas de seguridad y posteriormente la identificación de los delincuentes.

El estudio de los determinados tipos de comportamiento, vinculados a los perfiles socioeconómicos que son concretos, han arrojado algunas conclusiones que son importantes en el campo de la prevención delictiva. Así, por ejemplo, estudios realizados como el realizado por SHAW (2006), que arrojan sugerentes postulados sobre el papel general de los patrones de comportamiento, pues en muchos de estos casos formaron la base de la investigación para así poder determinar y poder evaluar las conductas de los delincuentes cibernéticos.

¿Qué es Wireshark?

Dice (Fernández Paucar & Robayo Tipán, 2022) que es una herramienta que se define como analizador útil porque aplica los conceptos de un código abierto, muy eficiente para el área académica por su ofrecimiento de ser gratuito. Su función en el campo es específicamente para trabajar con los paquetes de datos de la red, esta herramienta característica ayuda sobre todo en algún problema que presente la red. Ofrece función multiplataforma con constantes actualizaciones en nuevas versiones, implementar interfaces más amigables en el entorno de comunicación con los usuarios que trabajan con esta aplicación.

El objetivo es simple encuentra una red captura los paquetes de datos verifica, trabaja y finalmente envía un reporte de que tan seguro esta la red de trabajo. Su gran valor viene por trabajar a la par con varios sistemas operativos muy usados en el mundo de la tecnología algunos privados y otros libres, su manejo es ilimitado al ofrecernos una conexión con aplicaciones distintas que solo ayudan a buscar mejor servicio en la red.

¿Para qué sirve Wireshark

Según (ROBERTO LUIS MOREIRA SANCHEZ & CRISTHIAN DARIO VASQUEZ ARRIAGA, 2022) quienes lo manejan y controlan también llamados administradores del sistema especifican que su uso principal es el buscar dispositivos defectuosos que siempre intentan comunicarse por medio de la red enviando archivos o datos maliciosos la mayoría siempre ocasionan un tráfico en la red de cualquier modo, finalmente los peligrosos que buscan extraer información sin permiso.

La herramienta Wireshark considerada la más poderosa e importante el motivo es que una de sus reglas es pedir a los usuarios un básico conocimiento en los concetos de su uso y funciones, las empresas modernas manejan protocolos HTTP analizando cada nodo de dato muchos fáciles y otros bastante complejos por eso esta herramienta es viable en trabajar y entregar respuestas seguras.

Dice (HARO & GUERRERO, 2022) que es un programa el cual sirve como analizador de tráfico para redes informáticas, su función es capturar paquetes de la red, registrar cada uno de los datos en línea y así analizar los mismos para presentar toda la información que se pudo generar con sus respectivos detalles, es por ello que tiene compatibilidad con variedad de protocolos. Un analizador de paquetes de red es como un dispositivo de medición utilizado para examinar lo que está pasando en el interior de un cable de red, permitiendo así dar una respuesta rápida a intrusiones no deseadas.

Wireshark: Ventajas y Desventajas

Según (Turap et al., n.d. 2021) Wireshark es un software de análisis de red y paquetes que proporciona una amplia gama de funcionalidades para el monitoreo y la resolución de problemas en redes de comunicación. Ahora observaremos las ventajas y desventajas de utilizar Wireshark

Ventajas de Wireshark

- Observación en vivo de la red
- Análisis detallado de paquetes
- Interfaz intuitiva y fácil de usar
- Soporte para múltiples protocolos
- Captura de datos en tiempo real
- Análisis de tráfico cifrado
- Comunidad activa y soporte
- Personalizable y extensible
- Disponible de forma gratuita
- Multiplataforma

Desventajas de Wireshark

- Requiere conocimientos técnicos
- Consumo de recursos
- Dificultad para poder leer y poder analizar lo grandes volúmenes de datos
- Puede generar información sensible
- Dificultad para depurar problemas complejos
- Interferencia con otras aplicaciones de seguridad
- Limitaciones en entornos virtualizados
- La falta de los análisis en tiempo real en ciertos protocolos
- Configuración y filtrado complejo
- Riesgo de interpretación incorrecta de los resultados

MARCO METODOLOGICO

Metodología

Diseño de la Investigación.

El diseño de la investigación es no experimental por lo que solo se observa el fenómeno tal y como se presenta para luego ser analizado y transversal porque se va medir una o varias características.

Tipo de Investigación.

El nivel de investigación es causal por el análisis que se realizó en la Distribuidora de papelería ESTELAR S.A. se describió con el uso de la máquina virtual kali linux empleando la herramienta wireshark

Población y Muestra

Población:

La población está conformada por los trabajadores de la empresa y por clientes, a quienes se les aplicó una encuesta de 6 preguntas validando un total de 29 respuestas.

Lugar y Periodo de Ejecución.

El estudio se lo llevó a cabo en la distribuidora de papelería ESTELAR S.A, en el periodo académico 2024.

Técnicas e Instrumentos de Recolección de Datos

Se aplicó la encuesta a 29 personas para obtener información sobre la vulnerabilidad en la red inalámbrica del establecimiento para generar un aprendizaje significativo a los clientes y trabajadores

Interpretación:

De acuerdo con los datos obtenidos, sobre si ¿suele conectarse a una red inalámbrica abierta cuando se encuentra en establecimientos públicos?, al respecto un 75.9 por ciento, manifiestan que a veces se conectan, un 20.7 por ciento comentan que siempre se conectan y un 3.4 por ciento, manifiestan que nunca, asimismo un 69 por ciento, no se sienten seguros al conectarse a estas redes, mientras que un 31 por ciento, si se sienten seguros, mientras tanto 48.3 por ciento, comenta que no es consiente de los peligros de conectarse a una red inalámbrica abierta, un 51.7 por ciento, comenta que si es consiente de los peligros, y finalmente el 100 por ciento respondió a que si esta de acuerdo a que el gobierno debería de invertir mas en ciberseguridad

RESULTADOS

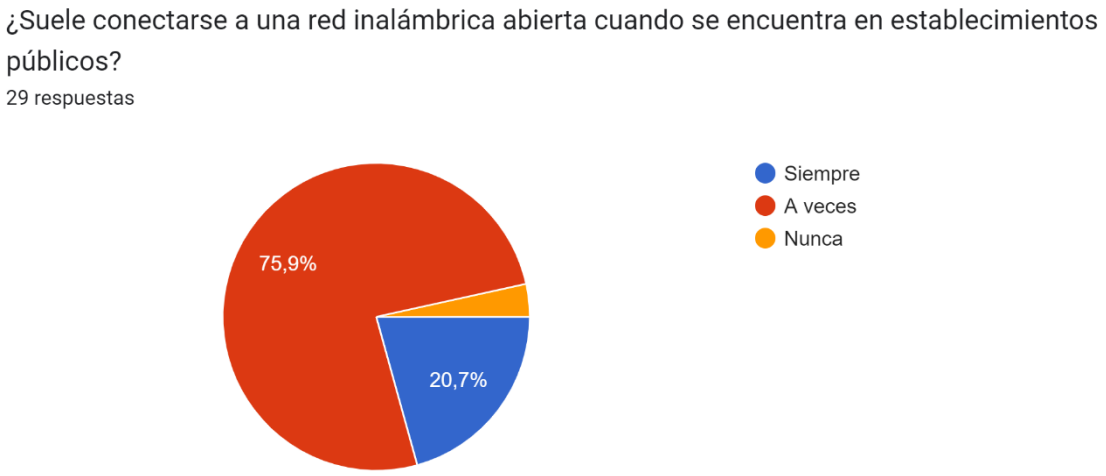
Como podemos observar que un 74,1% de las personas encuestadas se suele conectar a las redes inalámbricas abiertas en espacios públicos y la mitad de ellos no es consiente de los peligros que lleva conectarse a esas redes halando con ellos se le pudieron inculcar sobre los conocimientos que aporto de los peligros y los vulnerables que son al conectarse a estas redes en cualquier sitio

Siendo consiente de los conocimientos de los usuarios a los vulnerables que son en este tipo de casos con las redes inalámbricas pude notar la sorpresa de ellos al enterarse de lo que puede pasar con el simple hecho de conectarse a una red desconocida estando en un establecimiento público.

Dado que estos conocimientos que adquirieron los usuarios el 100% de ellos están de acuerdo de que el gobierno debería invertir más económicamente en la ciberseguridad de estos sitios, aunque no todas las redes abiertas son con el fin de hurtar información de las personas que lleguen a conectarse a ellas, hay redes que están abiertas al público con el fin de recabar información personal de los usuarios que se lleguen a conectar a estas

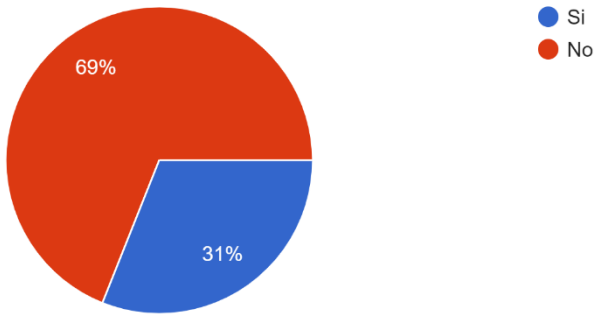
DISCUSIÓN DE RESULTADOS

Se realizó una encuesta con las preguntas pertinentes, las que permitieron conocer la importancia de expandir este conocimiento acerca de las redes inalámbricas y su seguridad, así como realizar un respectivo análisis cada cierto tiempo en las redes con el uso de herramientas tecnológicas, algunas de las preguntas más relevantes fueron:



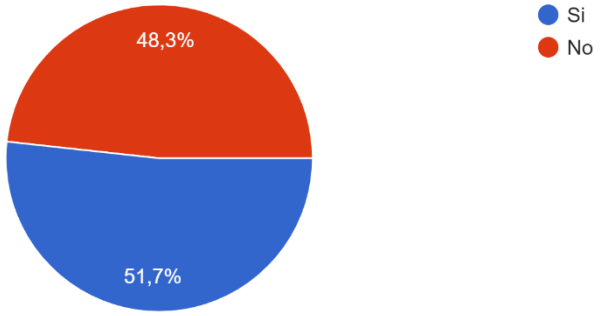
- Como podemos observar en el grafico encuestado a 29 personas en la cual el 75,9 por ciento, suele conectarse a veces a una red inalámbrica abierta en establecimientos públicos, mientras que el 20,7 por ciento suele conectarse siempre a una red inalámbrica abierta y con el 4,4 por ciento nunca se conectan a una

¿Se siente seguro al conectarse a una red inalámbrica abierta?
29 respuestas



- En la gráfica poder observar que el 69 por ciento no se siente seguro al conectarse a una red inalámbrica abierta y el 31 `por ciento si se siente seguro al conectarse a una red inalámbrica abierta

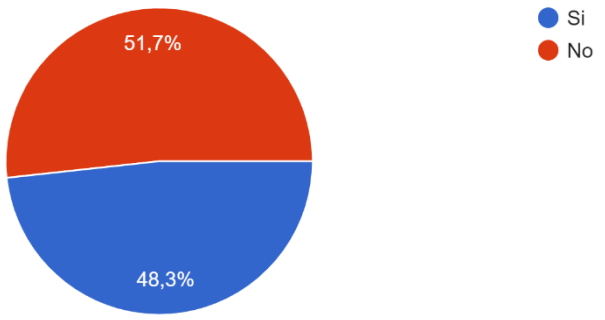
¿Estas usted consciente sobre los peligros que tiene conectarse a una red inalámbrica abierta desconocida?
29 respuestas



- Observamos en la gráfica que el 48,3 por cierto no está consiente sobre los peligros de conectarse a una red inalámbrica y un 51,7 si saben de los peligros de conectarse a una red inalámbrica desconocida

¿Sabia usted que al conectarse a una red abierta pueden obtener sus datos como usuarios y contraseñas?

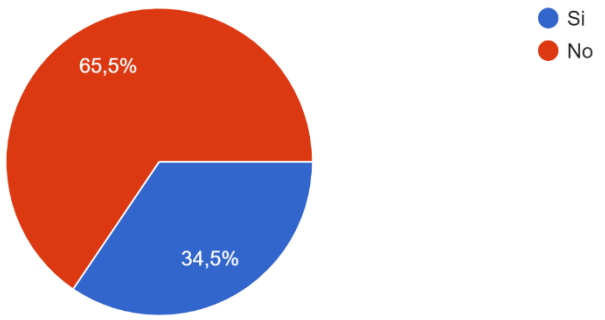
29 respuestas



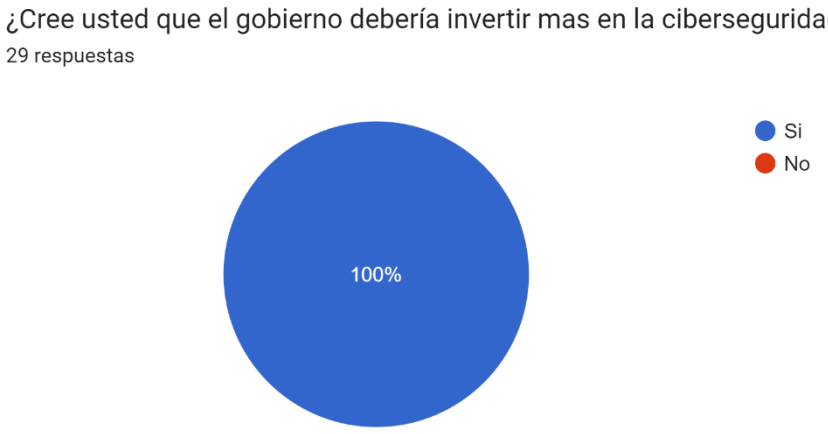
- En esta pregunta observamos en la gráfica el 51,7 por ciento no está consciente de que puede obtener ciertos datos y el 48.3 por ciento si esta consiente

¿Sabe usted porque al conectarse a una red publica su conexión es inestable?

29 respuestas



- En la gráfica podemos observar que el 65,5 por ciento de los encuestados no sabe porque al conectarse a una red inalámbrica abierta su conexión es inestable y el 34,5 por ciento si esta consiente de él porque su conexión es inestable



- En la siguiente grafica tenemos presente de que el 100 por ciento de los encuestados están en total acuerdo de que el gobierno debería invertir más económicamente en ciberseguridad

CONCLUSIONES

Un análisis de vulnerabilidades en las redes inalámbricas surge como una tarea de manera crucial en esta era digital, en donde la seguridad de la información de los usuarios se convierte en una presencia critica en cualquier organización. En esta investigación se resalta la importancia que puede llegar a tener una practica de los enfoques para así poder fortalecer la seguridad.

El análisis de las vulnerabilidades termina siendo una herramienta muy esencial para así proteger la integridad de los datos y así poder prevenir los ataques con fin malicioso ya que estos pueden comprometer información vital, se descarta la importancia de tener que adoptar las medidas que eliminen estos riegos identificados mediante un análisis de vulnerabilidades.

Una actualización de manera regular de firmware y software personaliza la configuración personalizada de dispositivos y la política de seguridad, con la seguridad cibernética el compromiso se posesiona como un proceso de manera dinámica y en evolución constante

Es crucial que las organizaciones mantengan un compromiso continuo con la seguridad, estando al tanto de las últimas tendencias y amenazas en el panorama cibernético, esto implica no solo implementar medidas de seguridad, sino también realizar evaluaciones periódicas de riesgos y ajustar las estrategias de seguridad según sea necesario, además de las soluciones técnicas, la concienciación y la capacitación del personal emergen como aspectos

RECOMENDACIONES

- Tanto al personal docente, administrativo y de TI de la institución educativa, deben concientizar acerca del uso de software y herramientas informáticas para proteger contra ataques a los dispositivos.
- Los computadores deben utilizar protección antivirus o antimalware de preferencia una versión de paga ya que poseen características mejoradas a la versión gratuita evitando ataques.
- El personal de TI debe mantenerse al tanto de cualquier vulnerabilidad o indicio de riesgo encontrado en la red.
- Proteger la red LAN mediante el uso de IPS e IDS, mejorando así la seguridad.
- Capacitar constantemente al personal de TI en torno a la seguridad informática.
- Adquirir un firewall físico para filtrar accesos indebidos y mantener una buena configuración protegiendo de cualquier amenaza a toda la red y a los dispositivos que se conectan a ella.
- Evitar abrir cualquier enlace que llegue al personal, sea por correo electrónico, por mensajes, o, de cualquier forma, en un navegador sin saber si proviene de una fuente confiable.
- Implementar certificado de seguridad SSL y autentificación en dos pasos en el sitio web.
- Realizar cada cierto tiempo los procesos de hacking ético, para así poder detectar vulnerabilidades y también poder detectar si se han podido eliminar las encontradas.

REFERENCIAS

Arroyo, S. C. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, *60*, 470–512. www.derechoycambiosocial.com

Capinera, john L. (2021). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *Block Caving – A Viable Alternative?*, *21*(1), 1–9. https://doi.org/10.1016/j.solener.2019.02.027%0Ahttps://www.golder.com/insights/block-caving-a-viable-alternative/%0A???

Feito, D., Manuel Vázquez, J., Rubén, N., & Jove, P. (2023). *Análisis, diseño e implementación de una aplicación web de concienciación sobre ciberseguridad*. 1–102. https://ruc.udc.es/dspace/bitstream/handle/2183/33011/FeitoPin_Daniel_TFG_2023.pdf?sequence=3&isAllowed=y

Fernández Paucar, L. J., & Robayo Tipán, A. S. (2022). *Ensamble De Un Adaptador Inalámbrico Para El Desarrollo Del Software Sniffer En Una Red Lorawan Y Análisis Con Wireshark*. 1–80. https://dspace.ups.edu.ec/bitstream/123456789/23442/1/UPS - TTS1028.pdf

HARO, A. S. G., & GUERRERO, G. A. S. (2022). Análisis De Datos Y Hackeo Ético Para La Detección De Vulnerabilidades En La Red Wi-Fi Con Usuarios Del Laboratorio Iot De La Universidad Politécnica Salesiana. *Tesis*, 80.

Jesús, O. M. M., Alcides, A. O. C., Enoc, V. R. W., & Enrique, P. M. L. (2022). Network traffic management in the quality of service “QoS” WAN in Tambopata-Peru 2021. *Revista de Ciencias Sociales*, *28*(2), 300–318. https://doi.org/10.31876/rcs.v28i2.37940

Ospina, M., & Sanabria, P. E. (2020). National Challenges for Cybersecurity on a Global Level: an Analysis for Colombia Desafios nacionais da cibersegurança no cenário global: uma análise para a Colômbia. *Revista Criminalidad, 62(2)*, *62*, 199–217.

https://www.policia.gov.co/revista/revista-criminalidad-volumen-62-no-2

Pacheco, D. S. (2022). Seguridad en redes de comunicaciones: Perspectivas y desafíos. *Ingeniare*, *30*(2), 215–217. https://doi.org/10.4067/S0718-33052022000200215

ROBERTO LUIS MOREIRA SANCHEZ, & CRISTHIAN DARIO VASQUEZ ARRIAGA. (2022). *Universidad Politécnica Salesiana Sede Guayaquil Carrera De Ingenieria Electrónica*. *1*, 131. https://dspace.ups.edu.ec/bitstream/123456789/6505/1/UPS-GT000596.pdf%0Ahttps://dspace.ups.edu.ec/bitstream/123456789/22653/1/UPS-GT003752.pdf

Rodriguez Toala, B. A., Pincay Segovia, E. J., & Maldonado Zúñiga, K. (2022). Las Redes Wan Y Su Importancia Para Los Ordenadores. *UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN 2602-8166*, *6*(1), 1–14. https://doi.org/10.47230/unesum-ciencias.v5.n4.2021.510

Rusdianti. (2024). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*.

Solórzano Álava, W. L., Rodríguez Rodríguez, 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

Stalin, O., Pinargote, B., Efraín, J., Cruzatty, Á., Alberto, J., Ferrin, C., Nicole, G., & Robles, P. (2023). *Seguridad informática en redes inalámbricas Computer security in wireless networks*. *16*(4), 67–76.

Turap, T., Merupakan, T. B., Lebih, T. B., & Turap, T. D. (n.d.) (2021). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*. 1–17.

(Iqbal, 2022). (2022). No Title2005–2003, *8.5.2017*, הארץ .הכי קשה לראות את מה שבאמת לנגד העינים
www.aging-us.com

ANEXOS

FIGURA 1

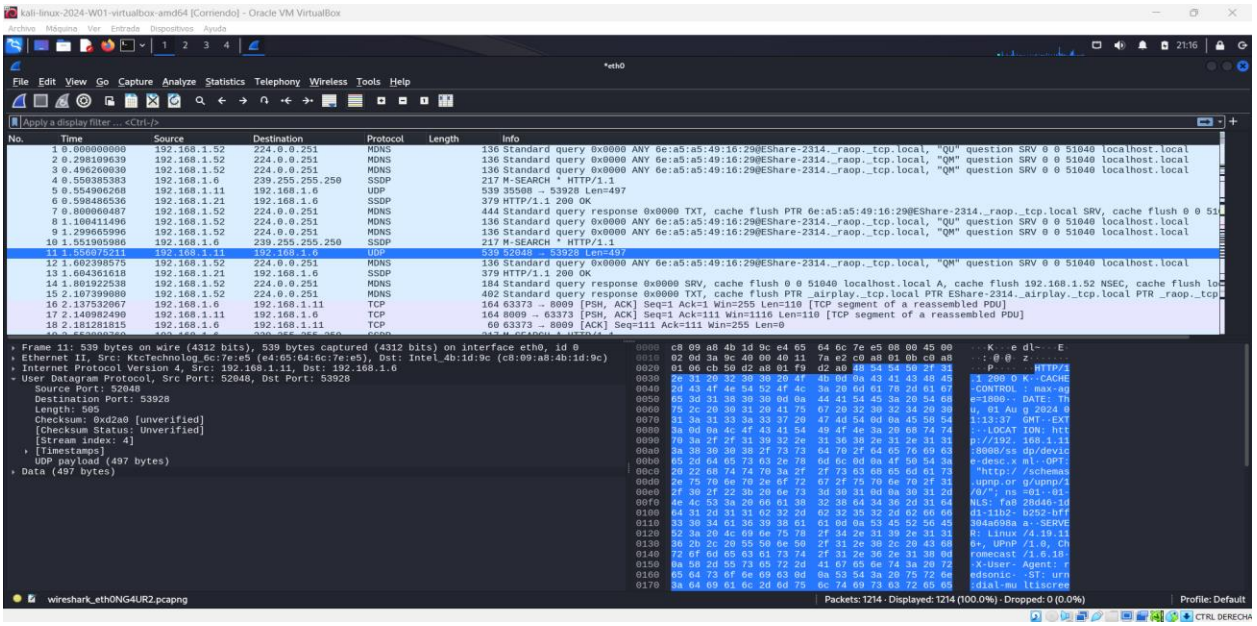


FIGURA 2

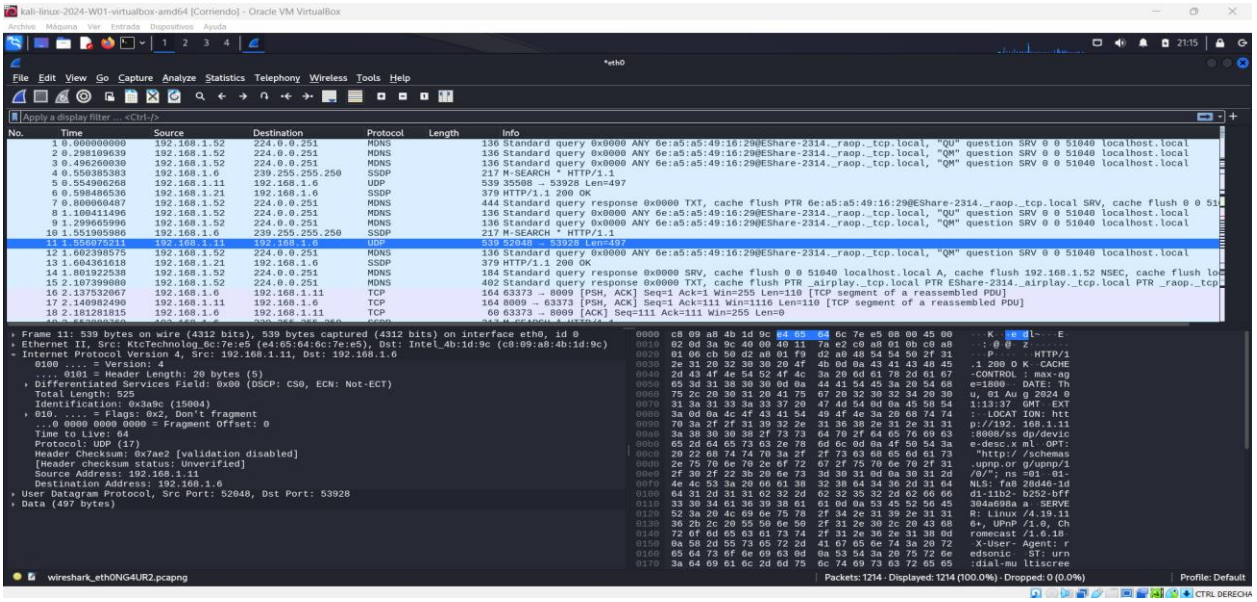


FIGURA 3

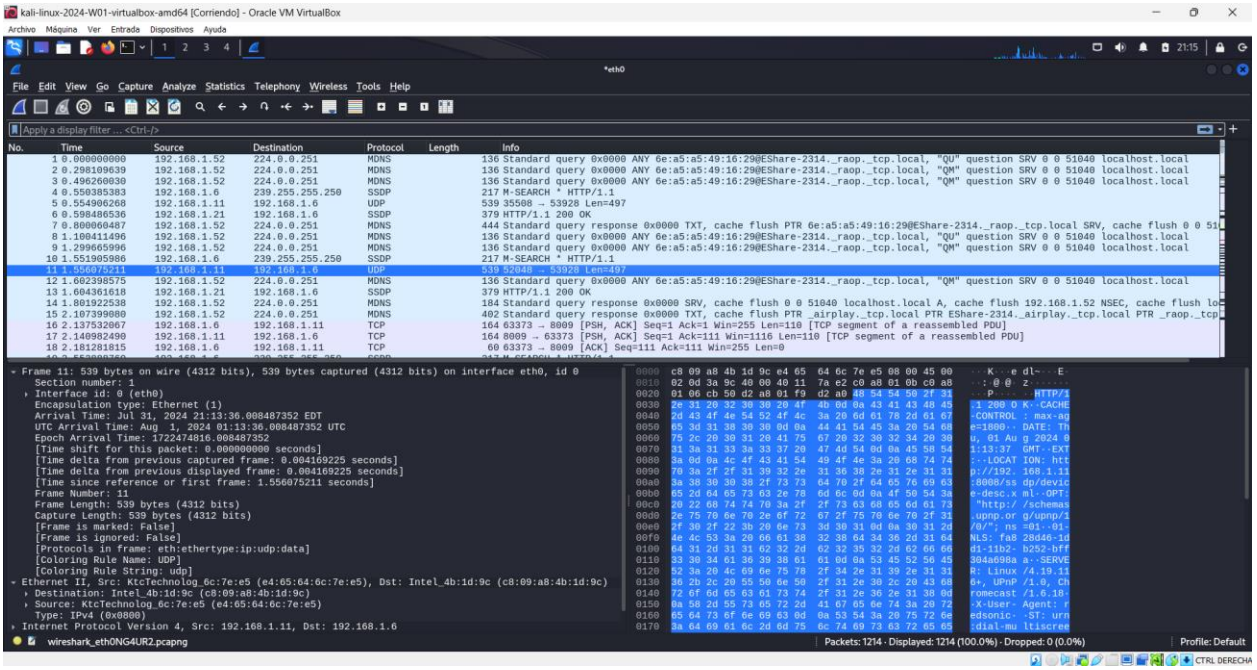


FIGURA 4

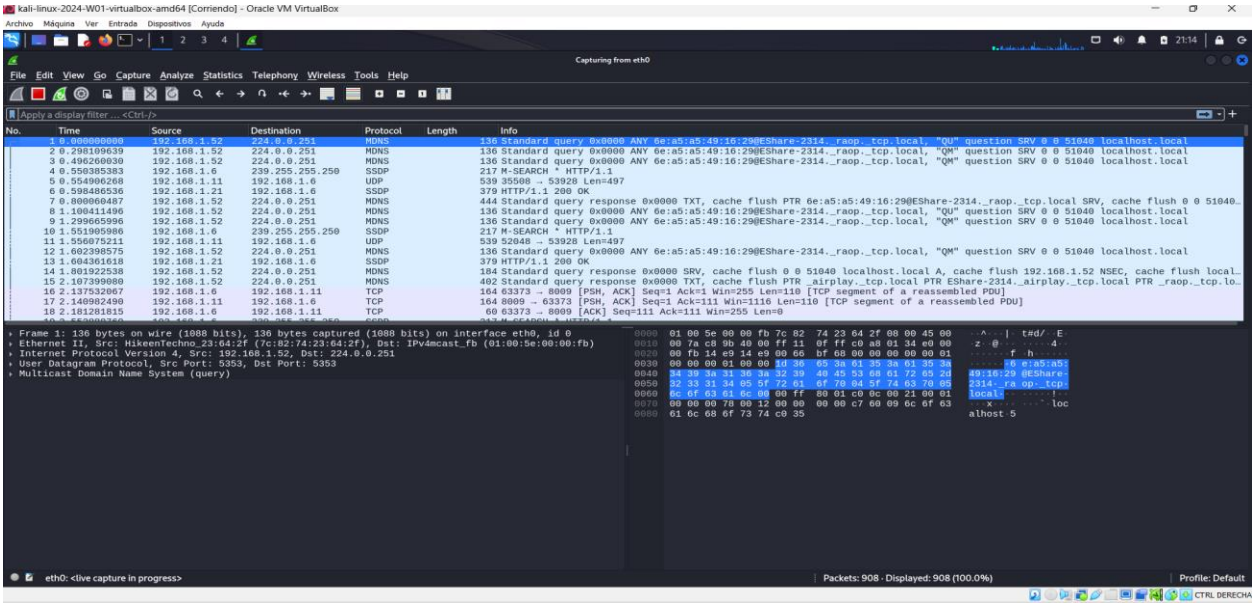


FIGURA 5

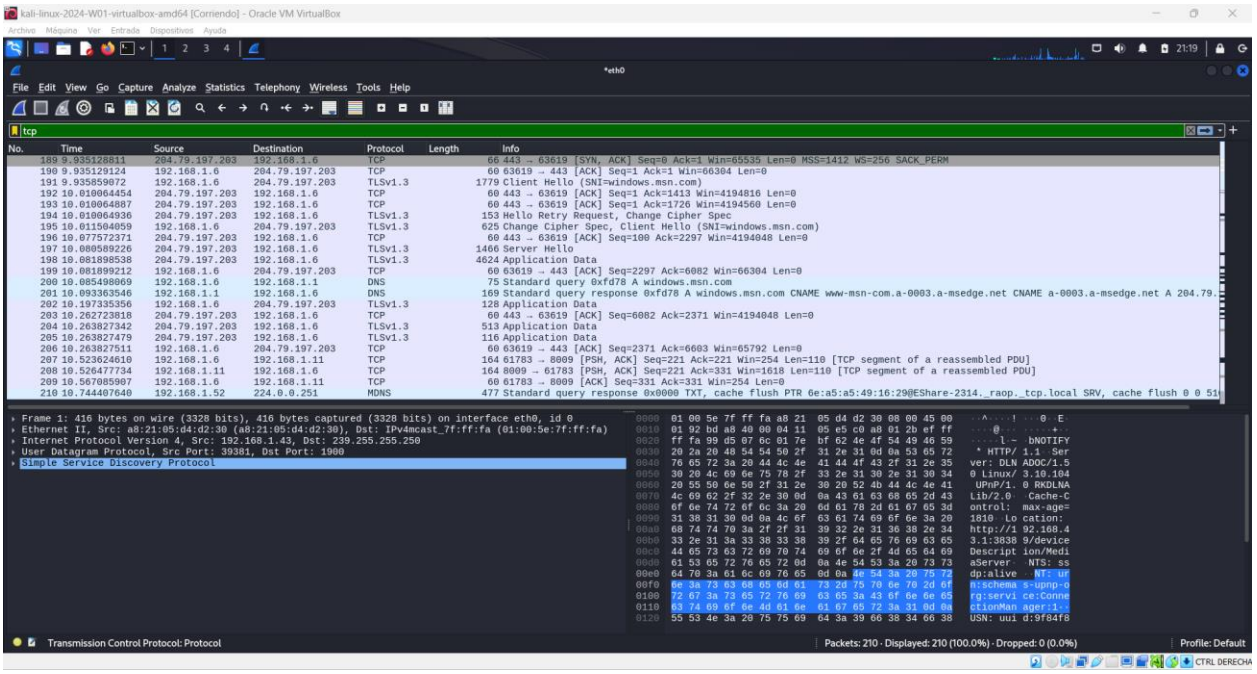


FIGURA 6