

Actividad [#1]

[Pérdida de Autentificacion y Gestión de Sesiones]

[“Auditoría Informática”]

Ingeniería en Desarrollo de Software

**Tutor: Jessica Hernández Romero**

**Alumno: Manuel Enrique Ramirez Lopez**

**Fecha: 05/02/2023**

***Indice***

***[Introduccion](#_Toc21735)* [1](#_Toc21735)**

***[Descripción](#_Toc20896)* [2](#_Toc20896)**

***[Justificación](#_Toc14955)* [3](#_Toc14955)**

***[Investigación](#_Toc18515)* [4](#_Toc18515)**

***[Descripción del sitio web](#_Toc22065)* [6](#_Toc22065)**

***[Ataque al sitio](#_Toc5258)* [7](#_Toc5258)**

***[Conclucion](#_Toc13716)* [9](#_Toc13716)**

# 

# *Introduccion*

Día a día se se generan multitud de sistemas/ sitios web donde la se enfocan en un área en especifica ya sea la medicina, escuela o redes sociales pero todas y cada una comparten una cosa en común bueno varias, su sistema de seguridad o prueba de errores donde personas que se dedican a fracturar dichos sistemas para un fin en concreto que va desde la sustracción de datos, robo de identidad u otros actos ilícitos pero para la empresa encargada de cada una de las ramas antes mencionadas su proposito es salvaguardar la informacion de la empresa y de sus clientes/usuarios donde estos últimos tengan la confianza de saber que su informacion esta a salvo de todo problema... Para un mejor entendimiento de como podrían vulnerar algo tan sencillo como lo son los datos de acceso a continuación observaremos como es que con un programa “WireShark” lograremos vulnerar el acceso y lograremos acceder a la informacion contenida por el usuario.

# *Descripción*

Con esta actividad busco el obtener el conocimiento o las bases para poder saber

Como realizar estos ataques (sin fines de daños)

Como proteger el y los sistemas que desarrolle

Para esto debemos saber como funcionan dichas herramientas que tenemos a disposición con este programa “WireShark” saber sus ventajas y desventajas de las mismas.

Y mas que nada la practica de como hacerlo en ambos sentidos.

# *Justificación*

Las pruebas de ataque de pérdida de autentificacion y gestión de sesiones son importantes para garantizar la seguridad de un sistema. Estos tipos de pruebas ayudan a identificar vulnerabilidades en la gestión de autentificacion y sesiones, que pueden ser explotadas por atacantes para acceder a información confidencial o realizar acciones no autorizadas. Al realizar estas pruebas, se pueden encontrar y corregir los errores de seguridad antes de que un atacante los descubra y los aproveche. Por lo tanto, es esencial realizar pruebas de ataque de pérdida de autentificacion y gestión de sesiones para garantizar la confidencialidad, integridad y disponibilidad de los datos y la información en un sistema.

# *Investigación*

Ataque de pérdida de autentificacion y gestión de sesiones

***¿Cómo funciona este ataque?***

Un ataque de pérdida de autentificacion y gestión de sesiones se basa en explotar vulnerabilidades en la implementación de la gestión de sesiones y autentificacion en una aplicación o sistema web. Por ejemplo, si un sitio web no implementa correctamente la expiación de sesiones, un atacante puede robar una sesión activa y acceder a información o realizar acciones con el permiso de la víctima. Otra técnica común es interceptar y manipular los tokens de sesión, lo que permite a un atacante tomar el control de una sesión existente. Para protegerse contra estos tipos de ataques, es importante implementar adecuadamente la gestión de sesiones y la autentificacion y asegurarse de seguir las mejores prácticas de seguridad recomendadas.

***¿Cómo afecta este tipo de ataques a los sitios y usuarios?***

Un ataque de pérdida de autentificacion y gestión de sesiones puede tener graves consecuencias para los sitios web y sus usuarios. Algunos de los efectos incluyen:

Robo de información confidencial: Los atacantes pueden acceder a información confidencial, como nombres de usuario y contraseñas, datos bancarios, información personal, etc.

Uso no autorizado de la cuenta de la víctima: Los atacantes pueden utilizar la cuenta de la víctima para realizar acciones fraudulentas, como compras en línea, transferir fondos, publicar contenido no deseado, etc.

Daño a la reputación: Un ataque exitoso puede dañar la reputación de un sitio web y disuadir a los usuarios de confiar en él en el futuro.

Costos de la respuesta a incidentes: Los sitios web pueden enfrentar costos significativos para investigar y corregir los efectos de un ataque de pérdida de autentificacion y gestión de sesiones.

Por lo tanto, es importante que los sitios web implementen medidas de seguridad adecuadas y sigan las mejores prácticas recomendadas para protegerse contra este tipo de ataques.

***¿Cómo se puede prevenir?***

Para prevenir un ataque de pérdida de autentificacion y gestión de sesiones, es importante seguir las siguientes mejores prácticas de seguridad:

Implementar autentificacion de dos factores (2FA): La autentificacion de dos factores proporciona una capa adicional de seguridad al requerir dos formas de identificación, como una contraseña y un código de seguridad enviado por mensaje de texto o autentificacion por aplicación.

Implementar tokens de sesión seguros: Los tokens de sesión deben ser únicos y seguros y deben expirar después de un período de tiempo corto.

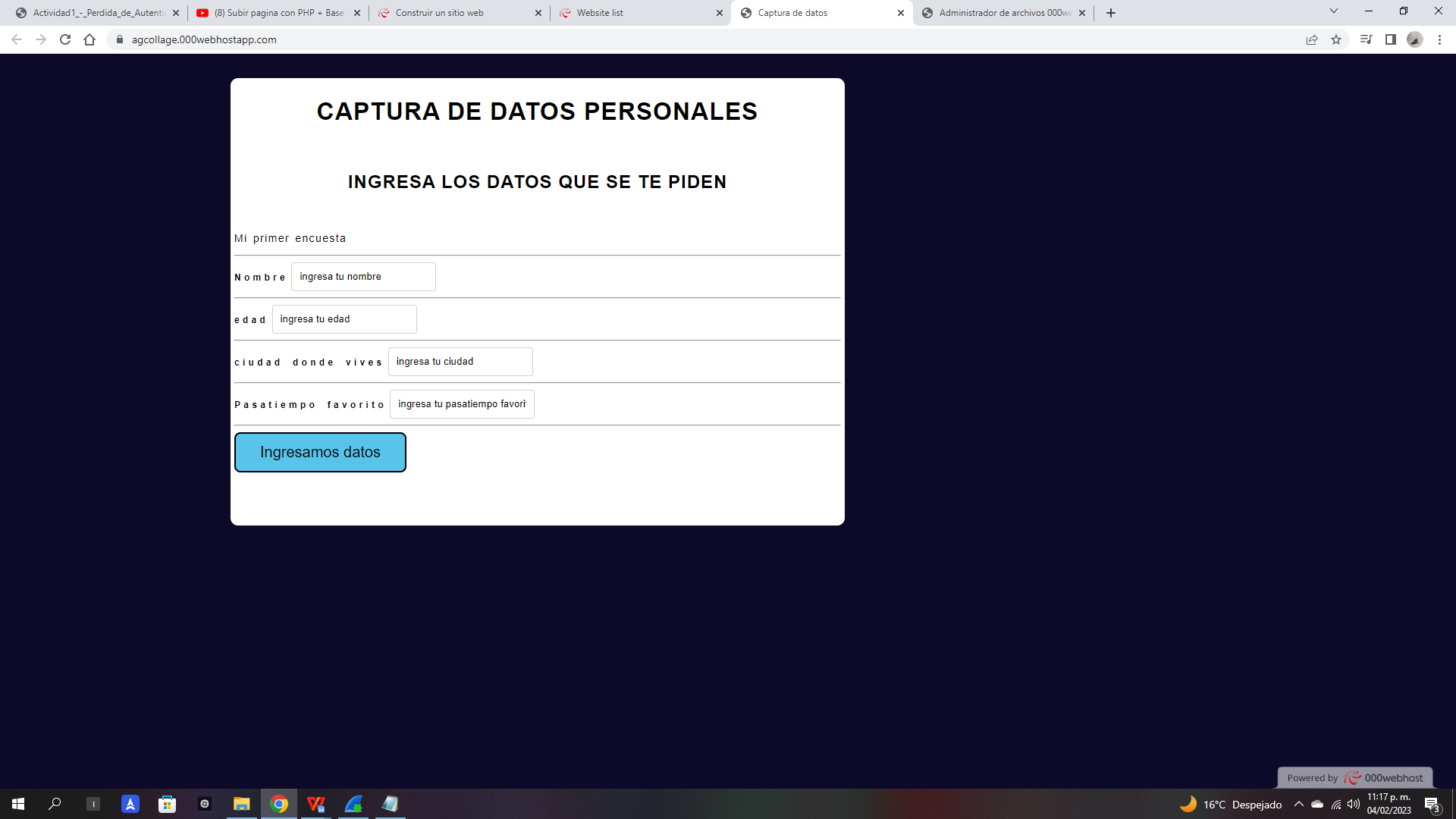
Almacenar contraseñas de manera segura: Las contraseñas deben ser almacenadas de manera segura, utilizando un algoritmo de hash seguro y una sal adicional.

Proteger la transmisión de datos: La transmisión de datos, incluidos los tokens de sesión, debe protegerse mediante cifrado SSL/TLS.

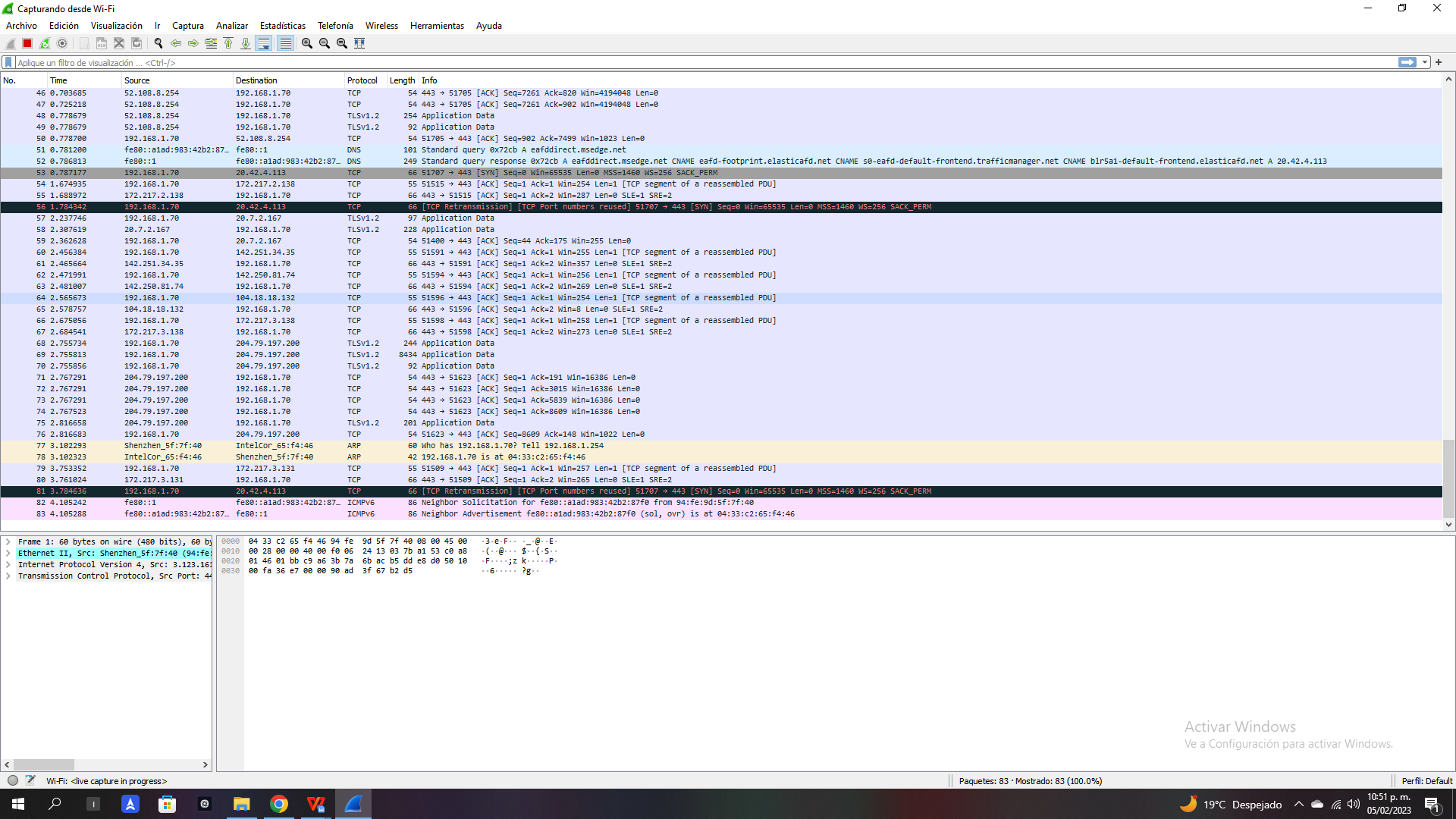
Realizar pruebas de penetración periódica: Es importante realizar pruebas de penetración periódica para identificar y corregir vulnerabilidades en la gestión de sesiones y autenticación.

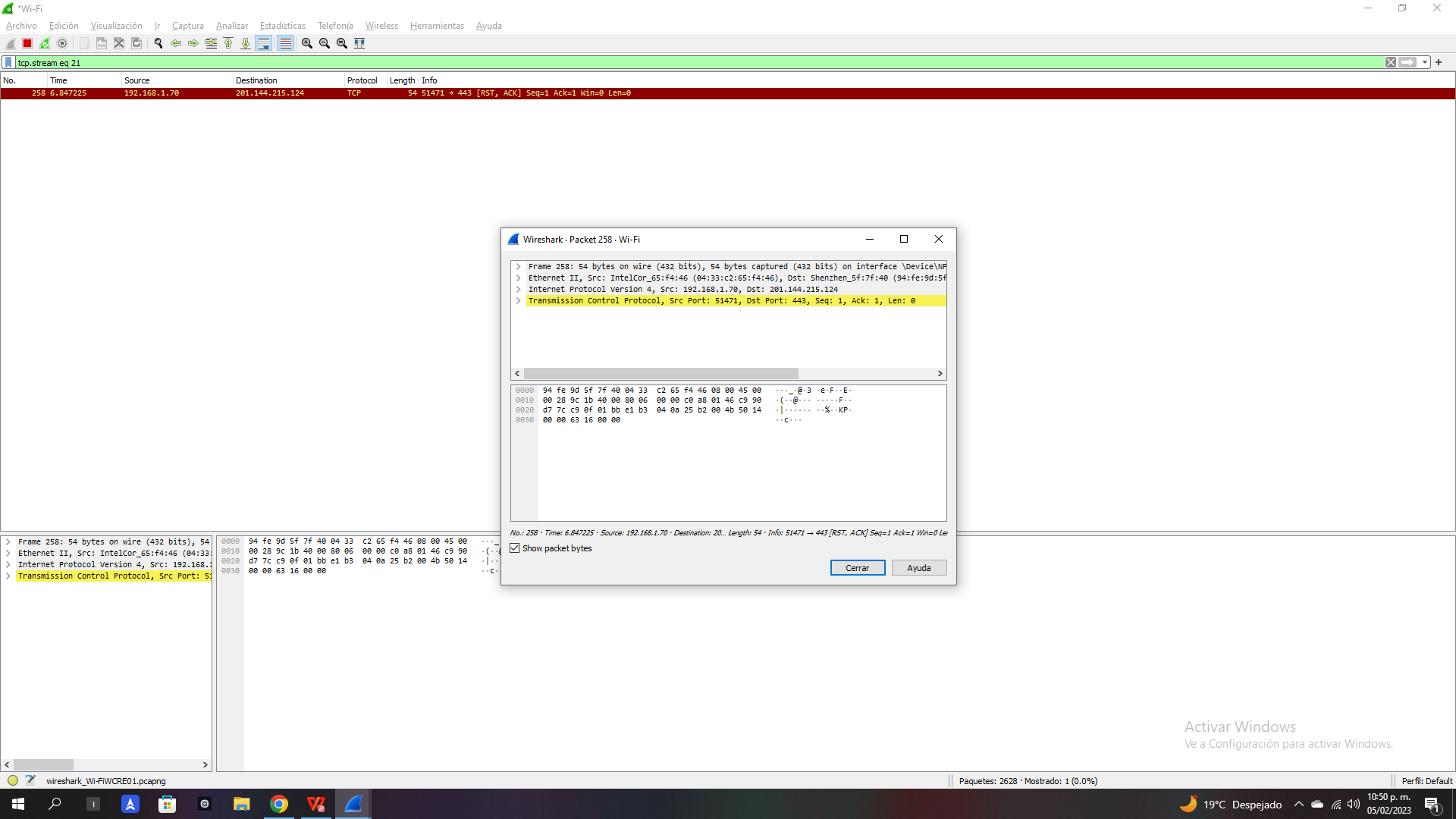
Además de estas medidas, es importante mantener actualizado sobre las últimas amenazas y vulnerabilidades y aplicar parches y actualizaciones de seguridad de manera oportuna.

# *Descripción del sitio web*

**Datos para el posterior registro donde arrojara mensaje personalizado.**

# *Ataque al sitio*

Paquetes enviados/ escaneados desde la opción Wifi



Seguimiento ante la apertura de inicio de sesión

# *Conclucion*

En conclusión, la pérdida de autentificacion y la gestión de sesiones son una amenaza importante para la seguridad en línea. Si no se implementan medidas de seguridad adecuadas, los atacantes pueden aprovecharse de las vulnerabilidades en el sistema de autentificacion y gestión de sesiones para acceder a información confidencial y realizar acciones fraudulentas. Para protegerse contra este tipo de ataques, es importante seguir las mejores prácticas de seguridad, incluida la implementación de autentificacion de dos factores, la utilización de tokens de sesión seguros, el almacenamiento seguro de contraseñas y la protección de la transmisión de datos. Además, es crucial realizar pruebas de penetración regulares y estabilizar actualizadas sobre las últimas amenazas y vulnerabilidades.