Actividad [#1] – [Perdida de Autenticación y Gestión de Sesiones]

[Auditoria Informática]

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

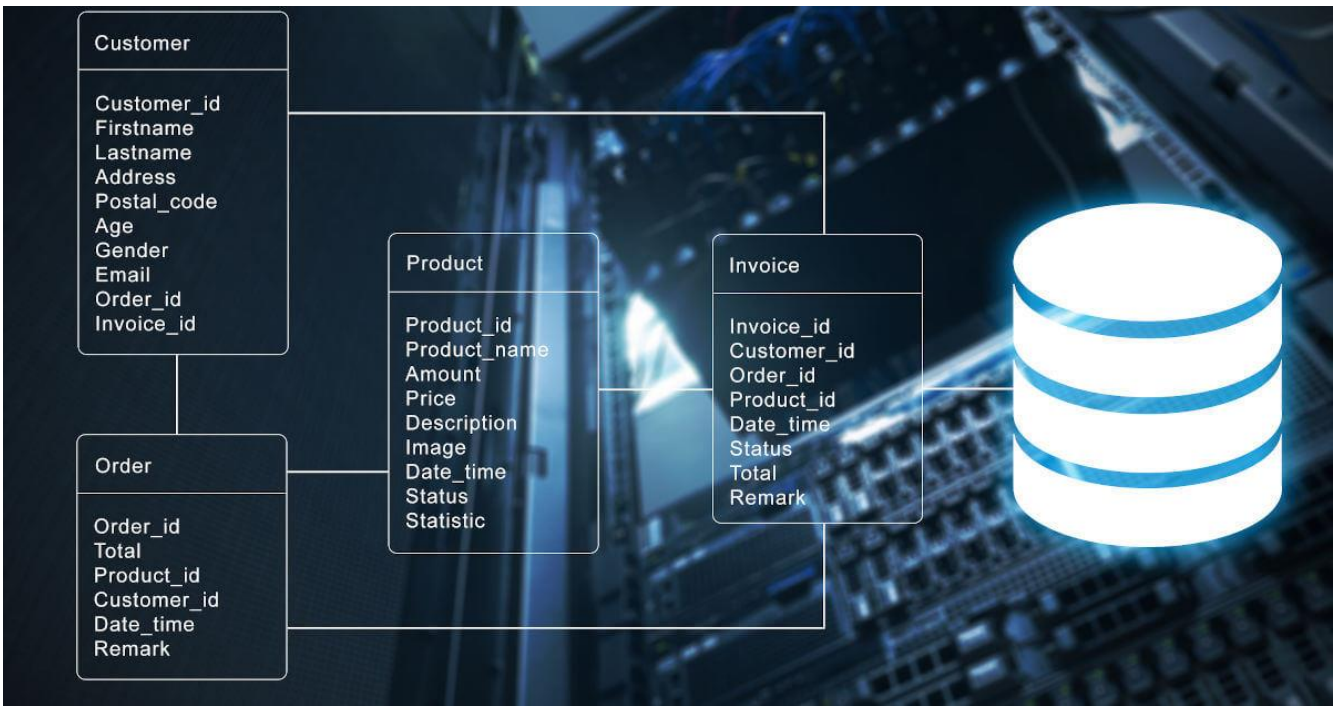
Alumno: Ricardo Rivas Rocha

Fecha: 12-junio-2025

Índice

Introducción

En esta actividad lo que se llevara a cabo es el ataque a una entidad web con ayuda de un software para invadir este mismo se nos indica que realizaremos pruebas de seguridad en esta misma en donde encontraremos sus fallas en sus vulnerabilidades comprobando la seguridad de igual manera para sacar una conclusión de que se debería hacer para tener un sitio web seguro en este caso, ya que en la actualidad aunque aparezcan muchas herramientas de seguridad en la información muchas son vulnerables para este caso vamos a lanzar un ataque directo a una pagina web con protocolos antiguos ya que por medio de estos mismos podemos escuchar a la página web cuando algún usuario ingresa a esta misma obteniendo sus datos a través de algún formulario de registro y almacén de datos o de igual manera muchos hackers muy experimentados pueden obtener todas las credenciales de estos sitios web, secuestran los datos y piden recompensa de manera monetaria para que no se compartan estos mismos es por ello que se necesita un sistema robusto que pueda cumplir con la seguridad de la información tanto para la empresa como para el usuario es por ello que vamos a realizar esta primera actividad en este caso yo elegiré alguna entidad web vulnerable para este primer paso de esta misma comprobando por mi mismo la importancia de tener sistemas seguros y actualizados constantemente.



Descripción

En este primer paso del trabajo lo que realizaremos es un ataque a un sitio web que este vulnerable ya que podemos darnos una idea de como es que trabajan los hackers y para conocer mas del mundo de la ciberseguridad en este tema se nos plantea hacer pruebas de la seguridad de este mismo sitio ya que en estas mismas no cuentan con candados de seguridad a que nos referimos al protocolo http que es con el que algunos sitios web cuentan y que es un peligro a nivel mundial ya que podemos obtener datos del usuario en este caso esta primera actividad se nos pide que este sistema web contenga un inicio de sesión y registro, ya que vamos a dar erróneamente los datos y después vamos a acceder con los datos verdaderos como le vamos a hacer muy fácil con una herramienta llamada Wireshark que nos permitirá escuchar esta misma pagina web cuando el usuario intente meter los datos de inicio de sesión ya que este mismo escuchara a la pagina sin candado de seguridad que en este caso es el protocolo http y aquí veremos la importancia de la seguridad y la actualización de estos mismos ya que en la actualidad los hackers como comente son mas sofisticados y con la ayuda de alguna inteligencia artificial de igual manera poder saber como vulnerar estas mismas es por ello que en el mundo se ocupan de ingenieros en ciberseguridad con muchos conocimientos por que hay muchas formas en las que podemos ser vulnerables aun teniendo una seguridad robusta los hackers buscan el punto más débil dentro de la codificación y atacan.

Justificación

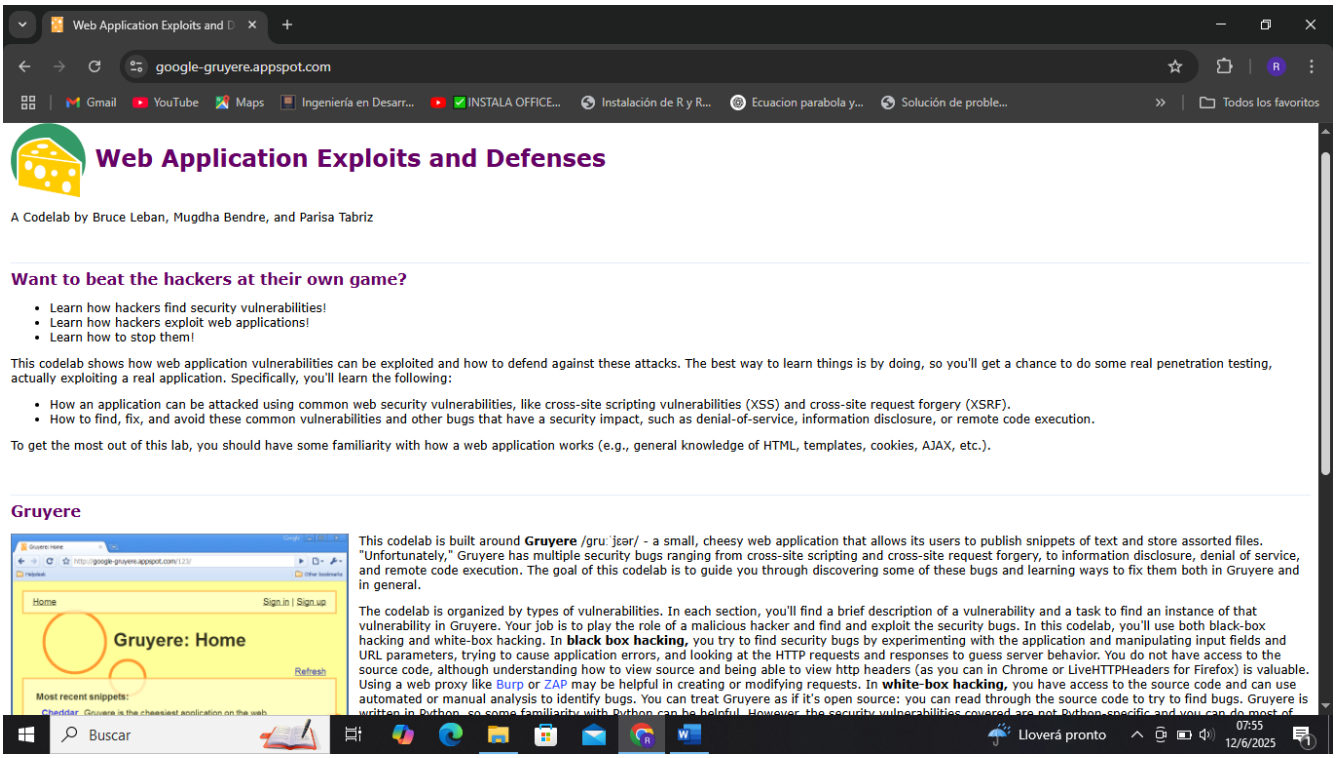
En este pequeño espacio de ciberseguridad nos va a enseñar de forma inicial a como entrar a este mundo ya que en la actualidad ya es más común que las empresas sean vulneradas por hacker ya que estas al no tener mayor seguridad se confían demasiado y algo de lo que observamos y vamos a aprender de esta actividad es a protegernos aun mas de estos ciberdelincuentes que buscan penetrar la seguridad de algún sitio web o aplicación es por ello que muchas empresas realizan ataques internos por los mismos jefes de ciberseguridad para valorar esta misma y dar reportes detallados de que problemas hay dentro del sistema y como protegerlo aun mas ya que en las anteriores materias de igual manera ocupamos de un software que nos ayudara a identificar las vulnerabilidades de nuestro equipo de computo y los pasos que se llevan los riesgos que estos lleven costos y pruebas ya que es muy importante la información en la actualidad porque vale demasiado, si es delicada en este caso el año pasado experimente que en la empresa que en la empresa en donde trabajaba Coppel hackearon el sistema y pues si hubo perdidas para la empresa por meses ya que tenían secuestrados los datos tanto de clientes como de esta misma, el atacante sabia jugar y entrar por la puerta de atrás no me caería de raro que fuera un jefe de ciberseguridad ya que ellos ya saben cuales son los puntos débiles de estos sistemas ya que fue un ransomware que afecto e infecto equipos de computo es por ello saber la importancia del hacking ético en este caso el de esta actividad para enfrentarnos a los problemas de hoy en día relacionados a estos hackeos.

Desarrollo:

- ## Descripción del sitio Web

En este el sitio web que elegí fue Google gruyere ya que intente hacer una pagina para registro e inicio de sesión la aloje en Infinityfree, pero al momento de enviar los datos de registro me marcaba error 500 del protocolo HTTP y pues buscando opte por este sitio web ya que no encontré algún proyecto de inicio de sesión.

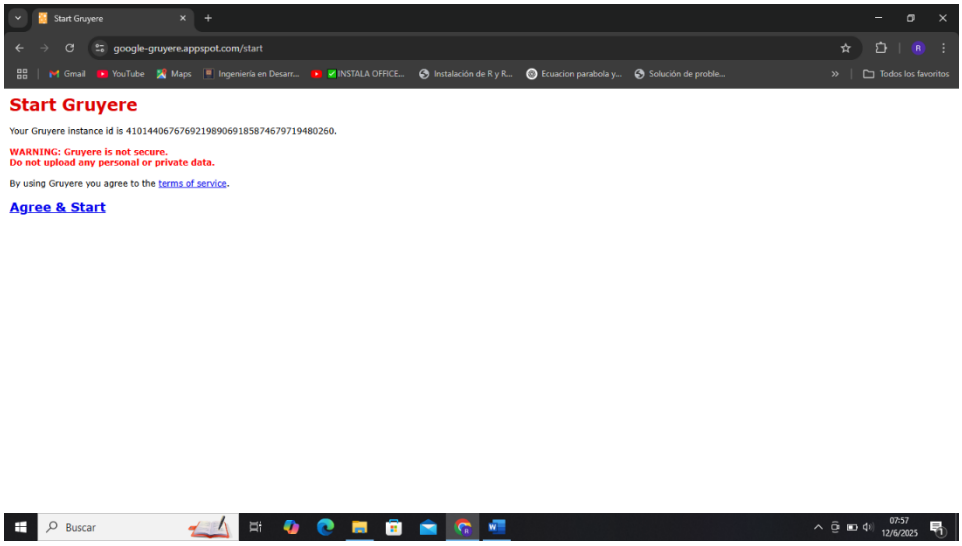
En este caso esta pagina web fue diseñada para el hacking ético en este caso tiene lo que pide la actividad un registro para iniciar sesión o crear una nueva cuenta este mismo sitio web también nos permite subir archivos desde upload para hackear mas este sitio web y practicar en este caso para esta actividad se nos pide que se detecten datos por medio de nuestra tarjeta wifi a través de Wireshark con puertos de escucha que es el HTTP y método get y post para identificar la contraseña a la hora de iniciar el proceso de lectura de paquetes de la página web.



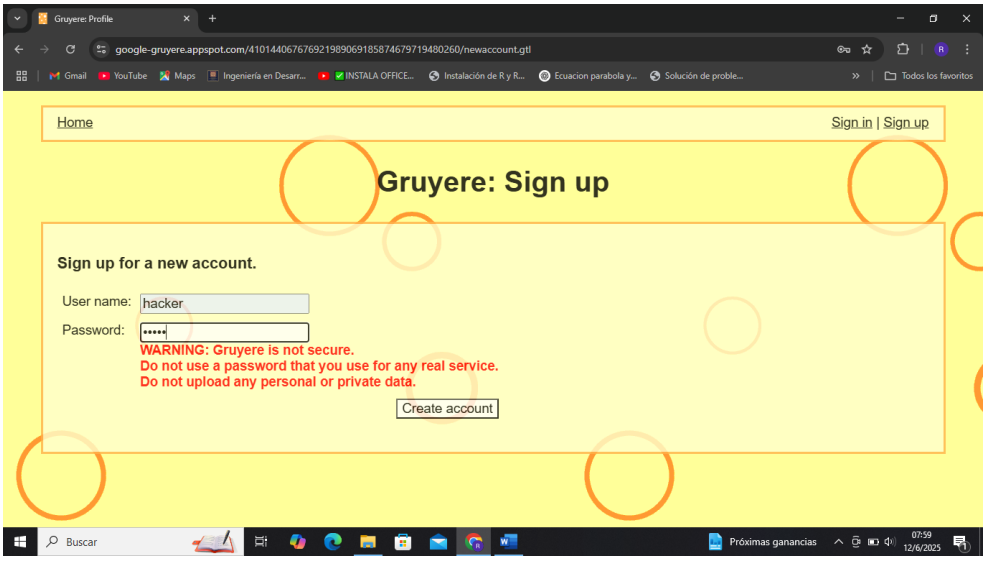
Desarrollo:

- ## Ataque al sitio web

En este caso para el ataque entramos a la pagina web victima que sería la de Google gruyere aceptamos y entramos.



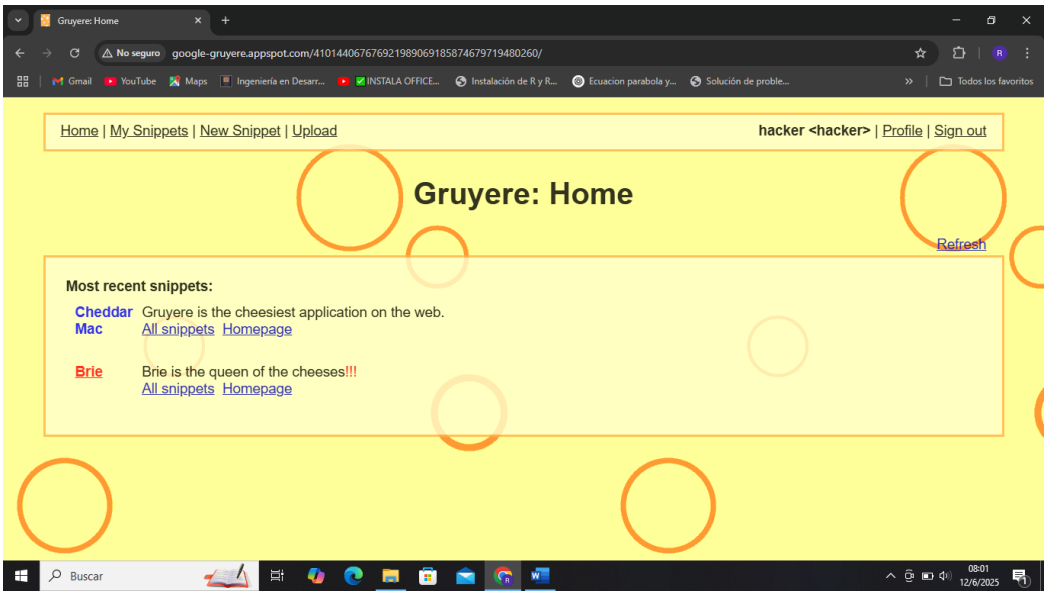
En este caso me voy a registrar para esta practica y quitare la letra S de HTTPS para que la conexión ya no sea segura.



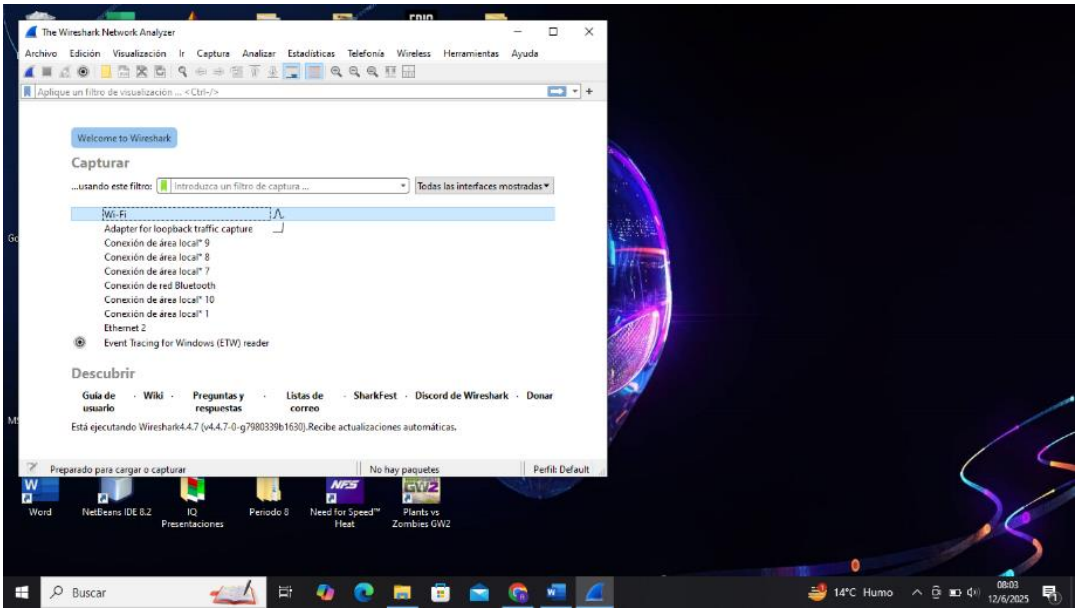
Desarrollo:

- ## Ataque al sitio web

En la imagen anterior observamos que nos registramos regresamos a home y quitamos la “s” del HTTPS y observamos que el sitio web ya no es seguro.



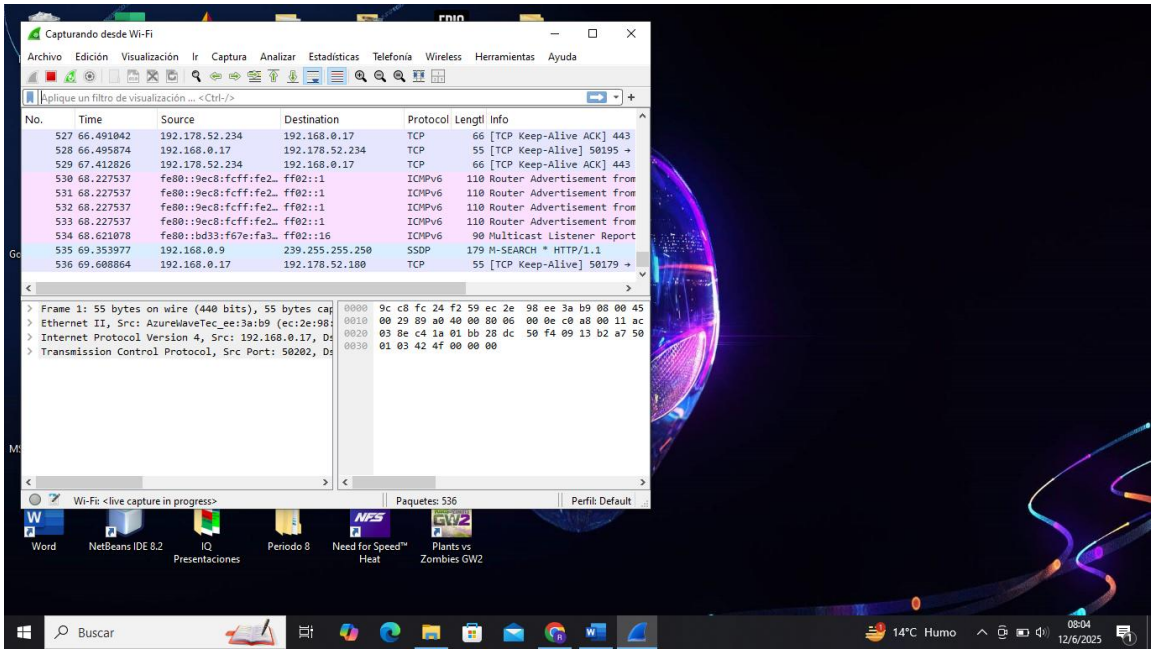
Abrimos la aplicación de Wireshark y nos vamos a wifi.



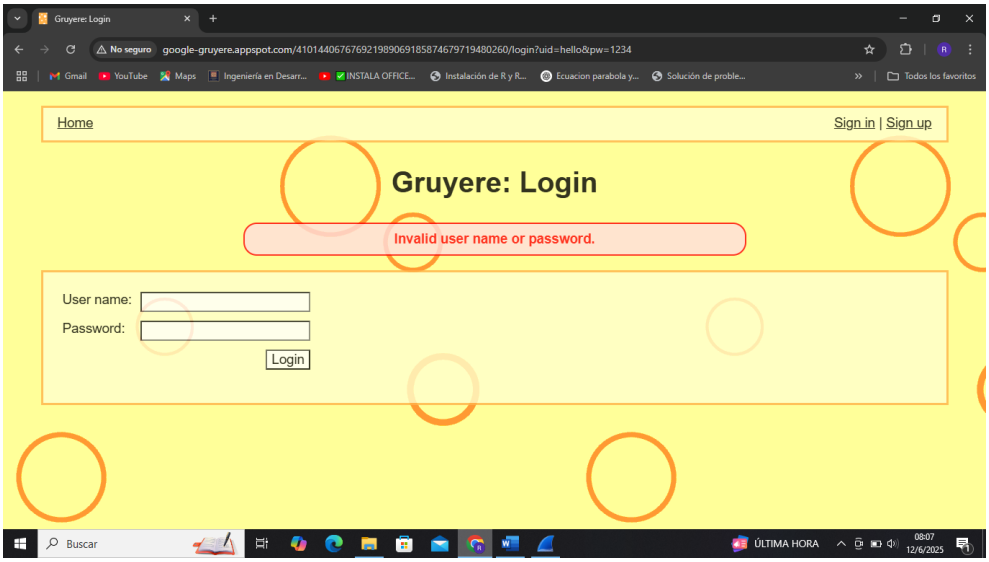
Desarrollo:

- ## Ataque al sitio web

Aquí es donde nuestra aplicación empieza a escuchar todo lo que hay en la página web.



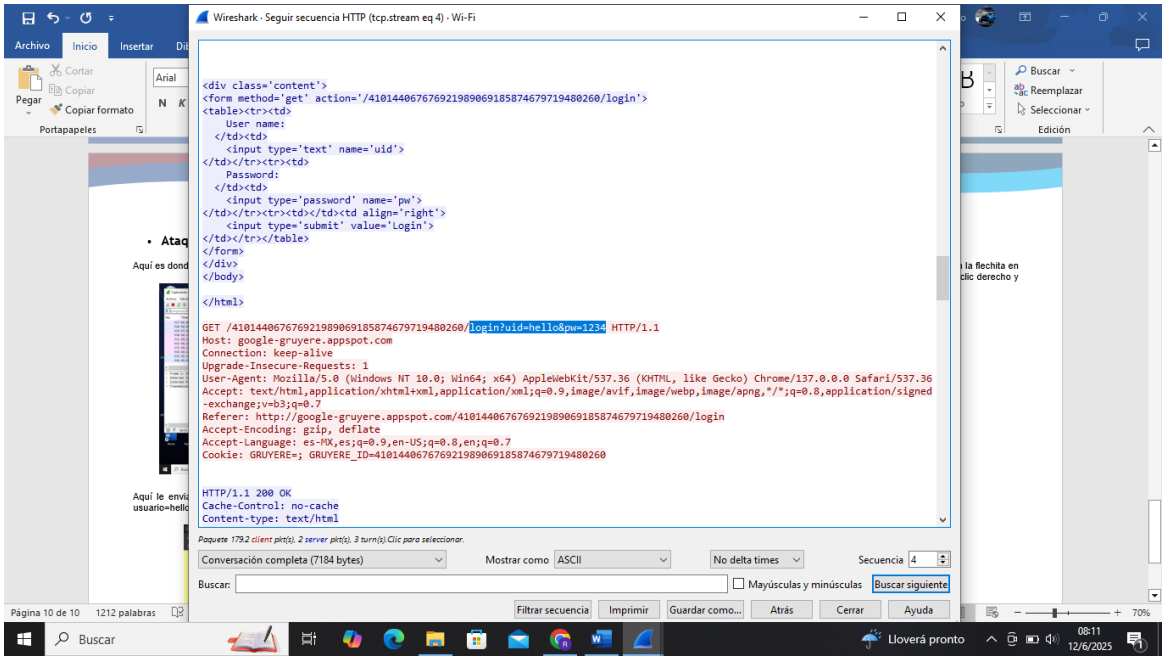
Aquí le enviamos datos erróneos del inicio de sesión desde la página web en este caso usuario=hello Contraseña=12345.



Desarrollo:

- ## Ataque al sitio web

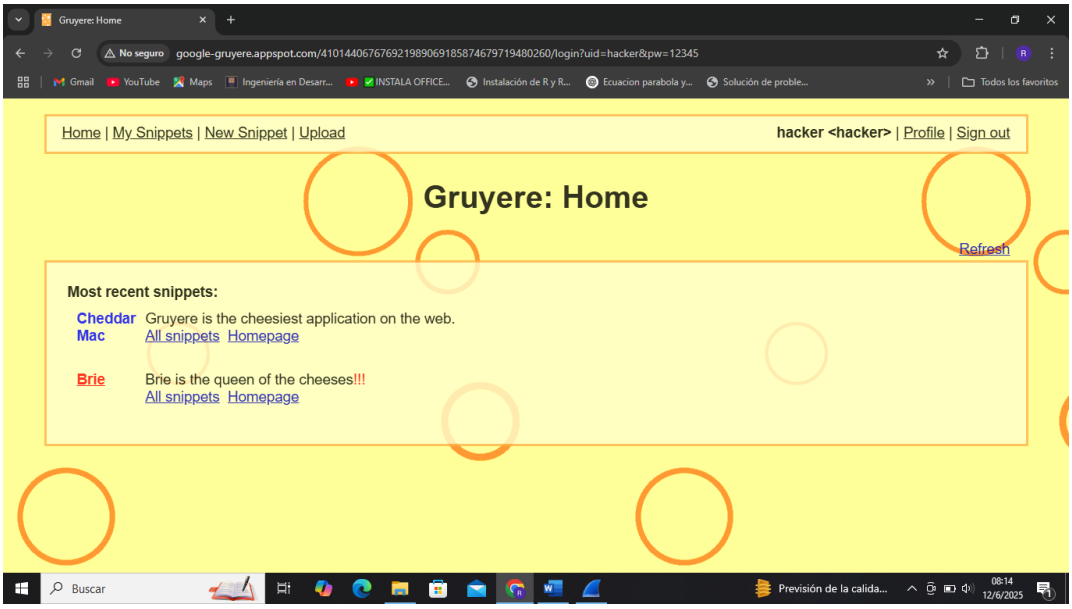
Detenemos el trafico y en la barrita de búsqueda ingresamos http y le damos en la flechita en el método get de primera instancia nos captura el usuario y contraseña dando clic derecho y seguir y http stream se aloja la contraseña errónea.



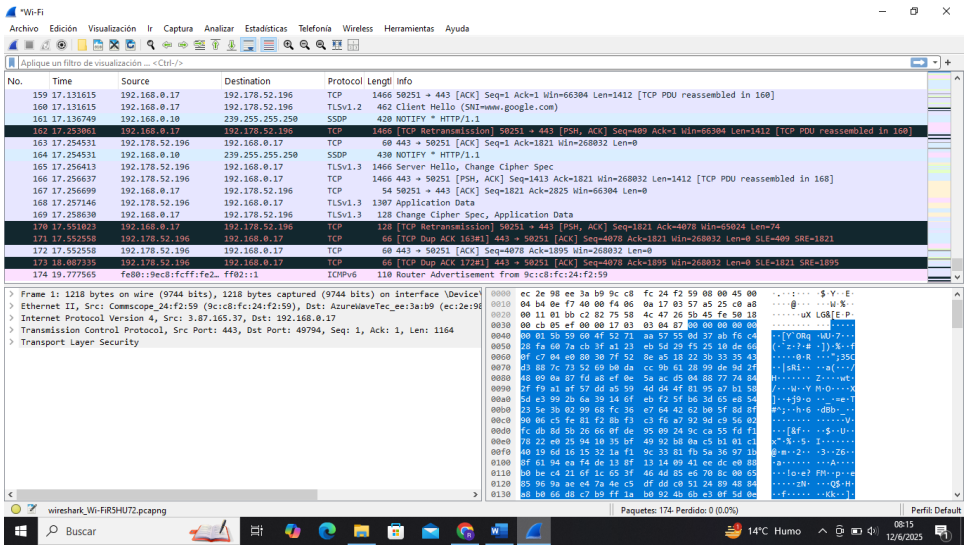
Desarrollo:

- ## Ataque al sitio web

En este otro escenario voy a aplicar la contraseña correcta para que vean que captura trafico de datos el Wireshark que es muy interesante.



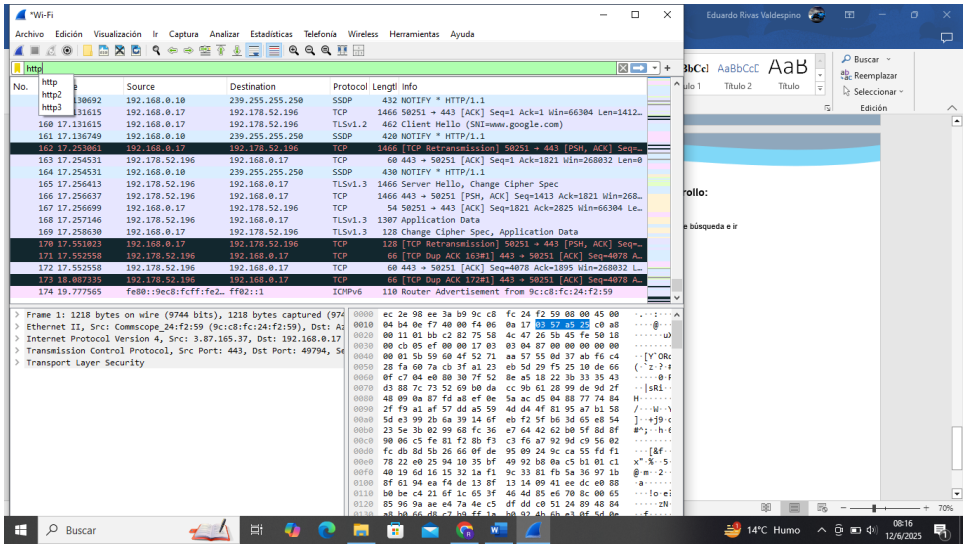
Capturamos el trafico de Datos desde Wireshark a través de wifi y detenemos el tráfico de datos.



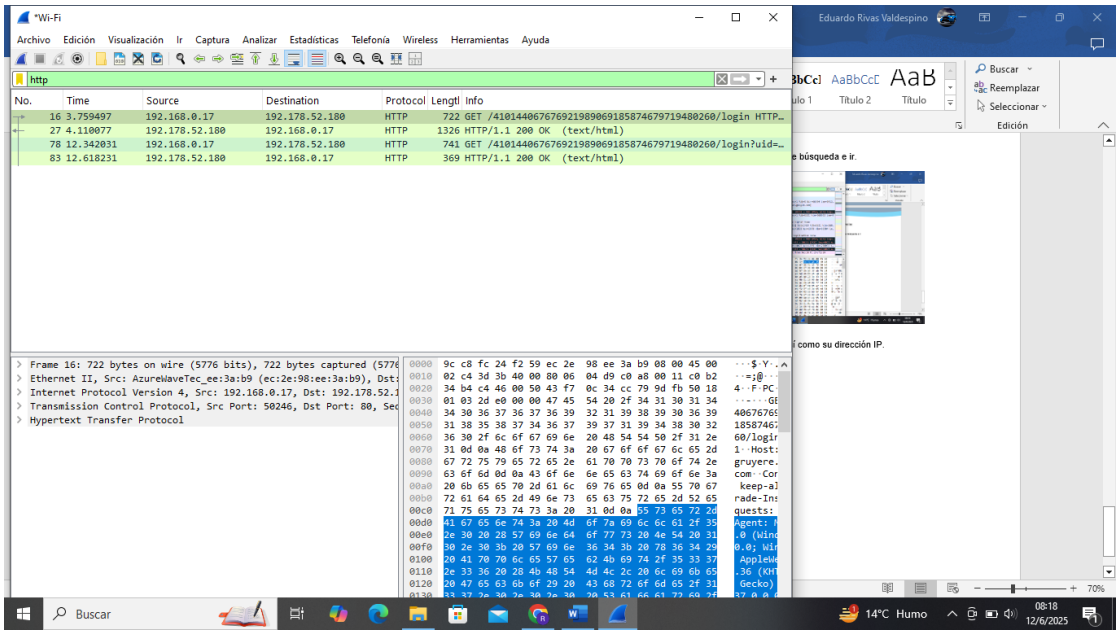
Desarrollo:

- ## Ataque al sitio web

Vamos a buscar el protocolo http en la barrita de búsqueda e ir.



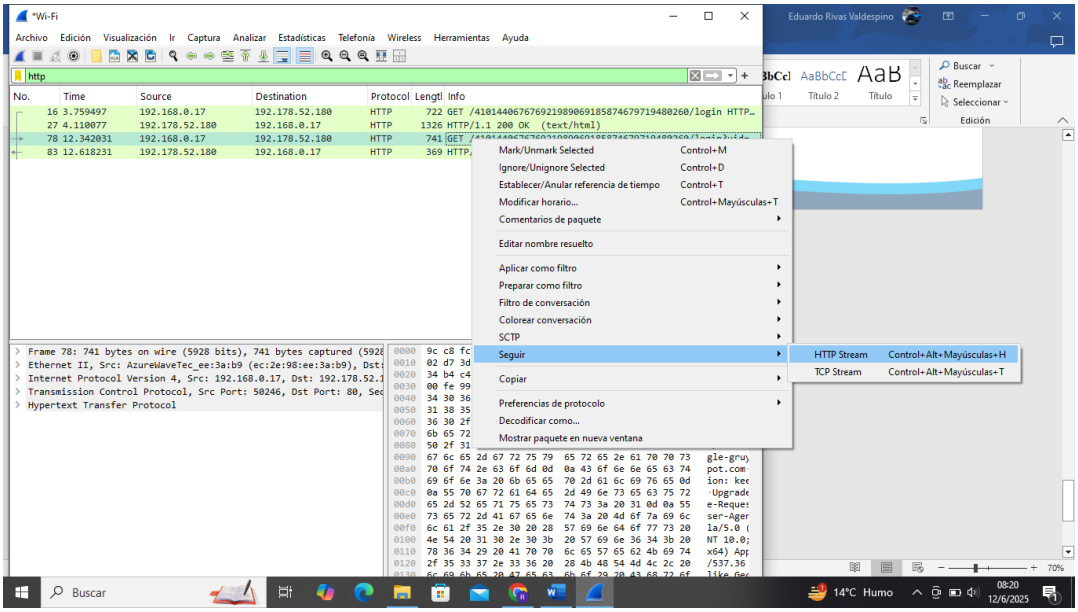
Nos muestra el trafico http de la pagina web, así como su dirección IP.



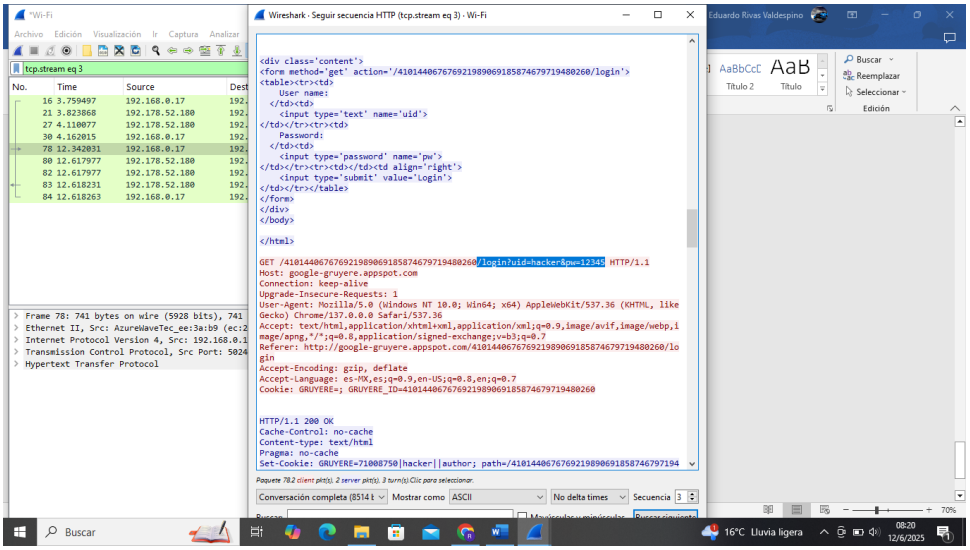
Desarrollo:

- **Ataque al sitio web**

Y nos metemos al método GET damos en seguir http stream.



Y encontramos el Usuario y contraseña ingresados correctamente wau que increíble.



Conclusión

Es increíble como se pueden capturar paquetes de datos por Wireshark ya que observamos es muy cauteloso en este proceso de lectura de estos mismos disimula este proceso, esta actividad aunque sea para empezar a vulnerar nos sirve también para concientizarnos en el mundo del hacking y a ser más empáticos a la hora de vulnerar un sistema aunque si te enfocas a ser hacker de sombrero negro tendrás consecuencias pero sabiendo cambiar o disfrazar tu dirección IP y tener un servidor VPN todo se hace un poco mas seguro para el hacker, sin embargo muchas empresas si es que tienes talento y las vulneras seguido te pueden contratar para ser hacker ético y proteger sus sistemas de información aunque seria arma de doble filo para la empresa al momento que el empleado decida renunciar y arruinar por completo todo el sistema que hoy en la actualidad es lo que pasa y que es difícil de creer a que grado pueden llegar a ser estos jefes de seguridad es por ello que hay que ser consientes y empáticos al momento de manejar o proteger gran cantidad de información ya que se puede tener un sistema de no autorización al momento que el colaborador decida ya no ser parte de la empresa o negocio porque si no pueden vulnerar los sistemas a través de ransomware como vimos en el hackeo en la empresa que trabaje Coppel ya que es importante las normas que dicte la empresa y llevar a cabo los procesos correspondientes de Autenticación. La experiencia en esta primera actividad fue un reto para saber los riesgos que existen en las paginas web así como mitigarlos de igual manera me gusto esta primera actividad.

Referencias

Gruyere: home. (s. f.). https://google-gruyere.appspot.com/4499479021350551859405580146071489171 64/

Wireshark • undefined. (s. f.). Wireshark. https://www.wireshark.org/