



Actividad | 1 |

Pérdida de Autenticación y Gestión de Sesiones

Auditoría Informática

Ingeniería en Desarrollo de Software



academi**ag**lobal

TUTOR: Jessica Hernández Romero

ALUMNO: Yanira Lizbeth Lopez Navarro

FECHA: 23/06/2024

Índice

Introducción 3

Descripción 3

Justificación 5

Descripción del sitio web..... 6

Ataque al sitio 10

Conclusión 15

Referencias 16

Introducción

El ataque de pérdida de autenticación de datos es una amenaza cibernética que afecta gravemente a los usuarios de internet, comprometiendo su seguridad y privacidad. Este tipo de ataque ocurre cuando los sistemas que verifican la identidad de los usuarios fallan, permitiendo que los atacantes accedan a información sensible sin las credenciales adecuadas.

Los usuarios de internet pueden ser víctimas de robo de identidad, donde sus datos personales, como nombres, direcciones y números de tarjetas de crédito, son utilizados fraudulentamente. Además, estos ataques pueden resultar en la pérdida de acceso a cuentas importantes, como correos electrónicos, redes sociales y servicios financieros, causando graves inconvenientes y posibles pérdidas económicas.

La exposición de datos confidenciales puede llevar a problemas de reputación y confianza, tanto para los usuarios afectados como para las empresas involucradas. En el ámbito empresarial, la pérdida de autenticación puede permitir que atacantes internos o externos manipulen datos críticos, afectando la integridad de los sistemas y la continuidad del negocio. Este tipo de ataque subraya la importancia de implementar y mantener sistemas robustos de autenticación y seguridad para proteger a los usuarios de internet.

Descripción

En esta actividad espero aprender de manera práctica cómo identificar y explotar vulnerabilidades relacionadas con la pérdida de autenticación y la gestión de sesiones en páginas web que carecen de candados de seguridad (SSL). Utilizando WireShark, un potente programa de análisis de tráfico de red, espero adquirir habilidades para interceptar y analizar los datos que se transmiten entre un usuario y el servidor web.

El proceso comenzará con la selección de un proyecto web previo que incluya funciones de inicio de sesión y registro de usuarios, así como una conexión a una base de datos. Subir este proyecto a un servidor web y configurarlo adecuadamente será crucial para simular un entorno realista.

Luego, mediante la instalación y uso de WireShark, espero aprender cómo capturar el tráfico de red para identificar y extraer credenciales que se transmiten sin cifrado. Este ejercicio me permitirá entender mejor las implicaciones de la falta de seguridad en las comunicaciones web y la importancia de implementar medidas como SSL para proteger la información sensible de los usuarios. Además, espero desarrollar una mayor capacidad para realizar auditorías de seguridad y aplicar estas habilidades en la mejora de la protección de aplicaciones web.

Justificación

Vivimos en una era digital donde gran parte de nuestra vida y actividades cotidianas dependen de la confianza en la seguridad de las plataformas en línea. Sin embargo, muchas páginas web, especialmente aquellas sin SSL, dejan a los usuarios vulnerables a ataques que pueden exponer sus credenciales y datos personales.

Probar la vulnerabilidad de la pérdida de autenticación utilizando WireShark nos permite identificar fallos críticos en la seguridad de estas plataformas. Esta prueba no solo nos enseña a reconocer los riesgos, sino que también nos equipa con el conocimiento necesario para implementar soluciones efectivas. Al interceptar y analizar el tráfico de red, podemos demostrar de manera tangible cómo los datos pueden ser capturados por actores malintencionados, resaltando la importancia de utilizar protocolos de seguridad robustos.

En última instancia, esta actividad nos prepara para proteger mejor a los usuarios finales, asegurando que sus datos permanezcan seguros y confidenciales. A través de estas pruebas, podemos contribuir a crear un entorno digital más seguro y confiable para todos.

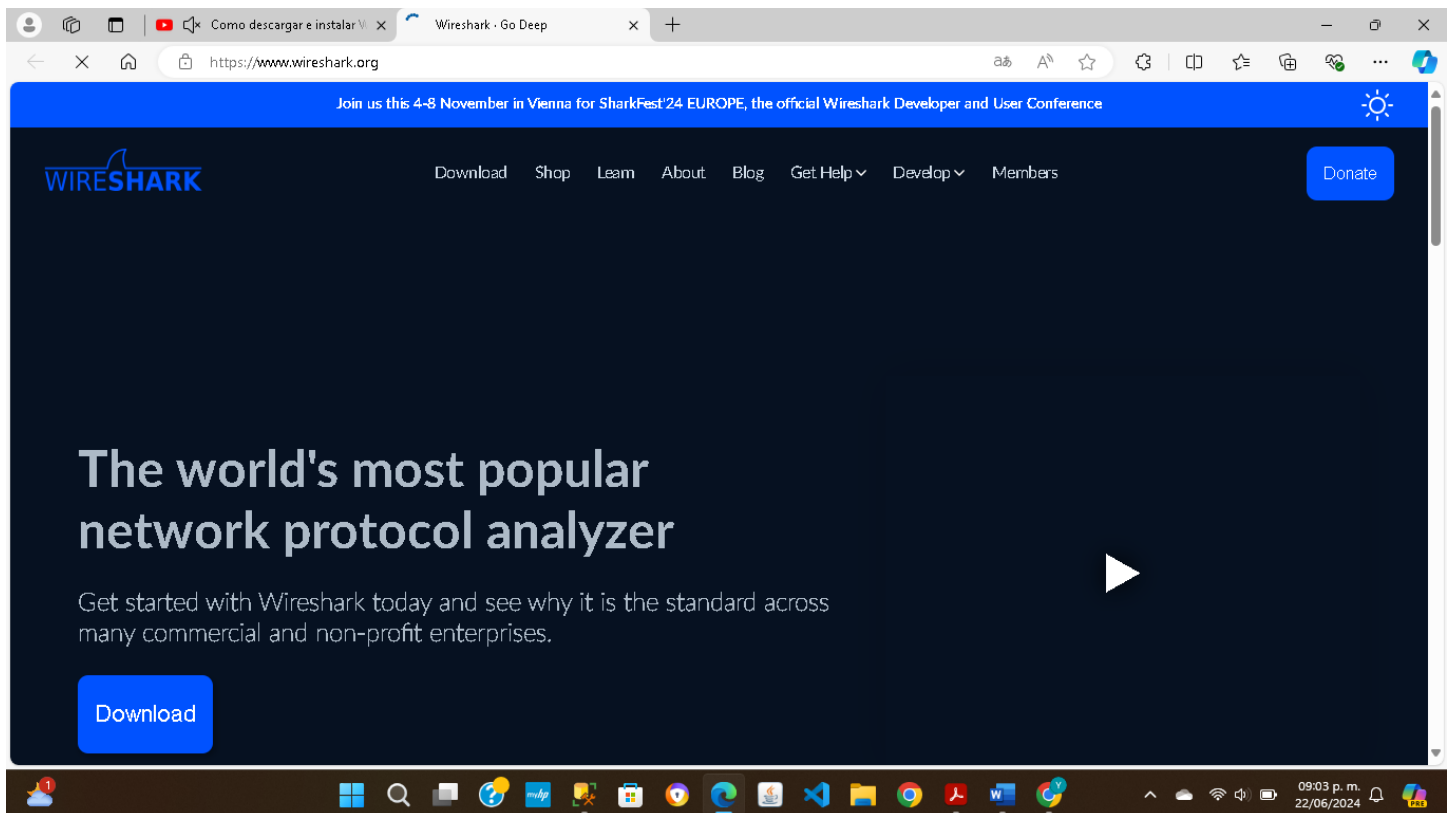
Descripción del sitio web

De acuerdo a lo solicitado en la actividad se llevó a cabo la Selección de un proyecto web realizado anteriormente, aunque no fue de mi autoría cumple con las características solicitadas en la actividad.

- Función de iniciar sesión y de registro de usuarios
- Conexión con una base de datos

<http://www.pruebadeuso.com/index.php?r=site/login>

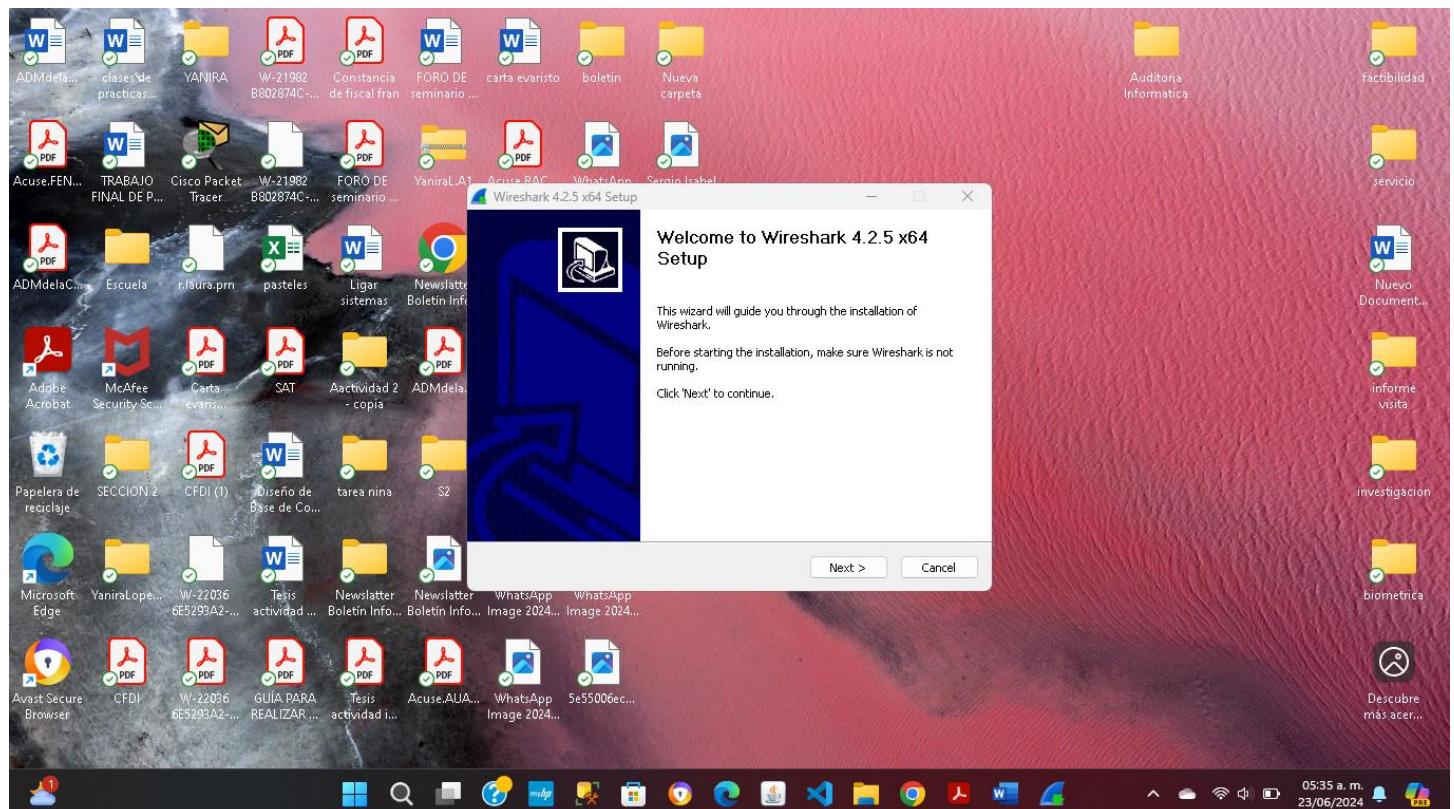
A continuación en la siguiente imagen podemos observar la pagina que nos permite descargar la herramienta recomienda para el desarrollo de la actividad .



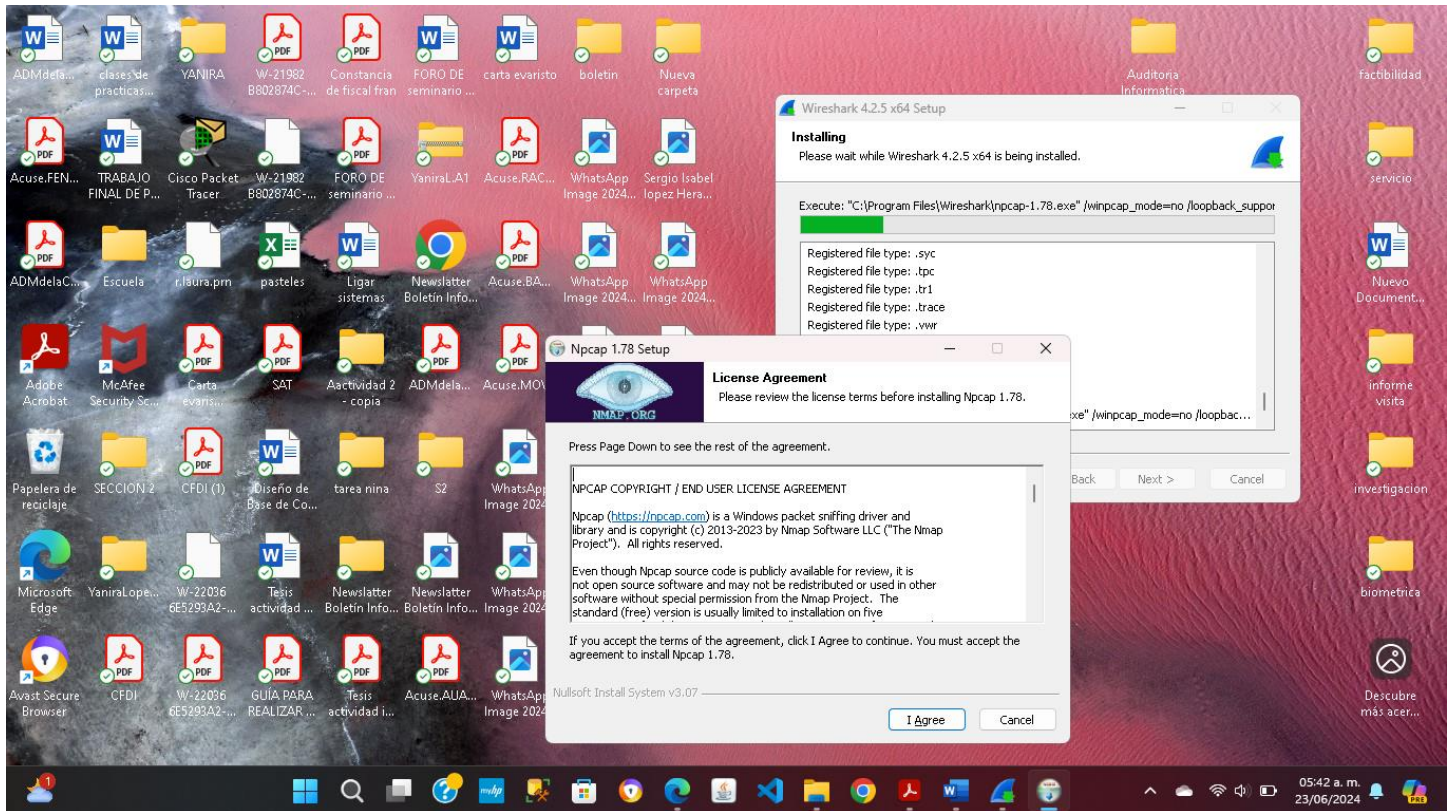
A continuación, seleccionamos el instalador para Windows x64 ya que es compatible con mi equipo



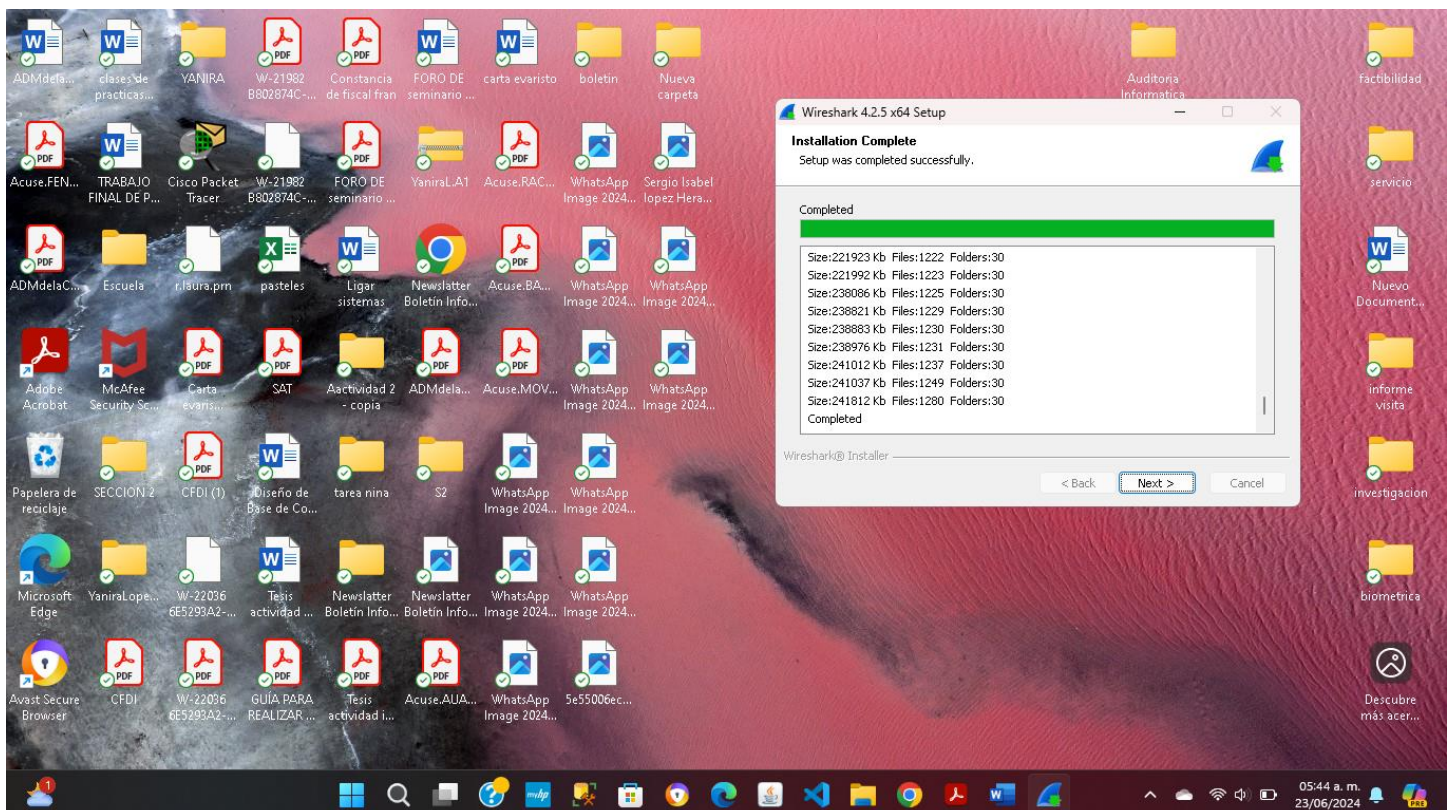
Una vez que WireShark fue descargado procedemos su la instalación.



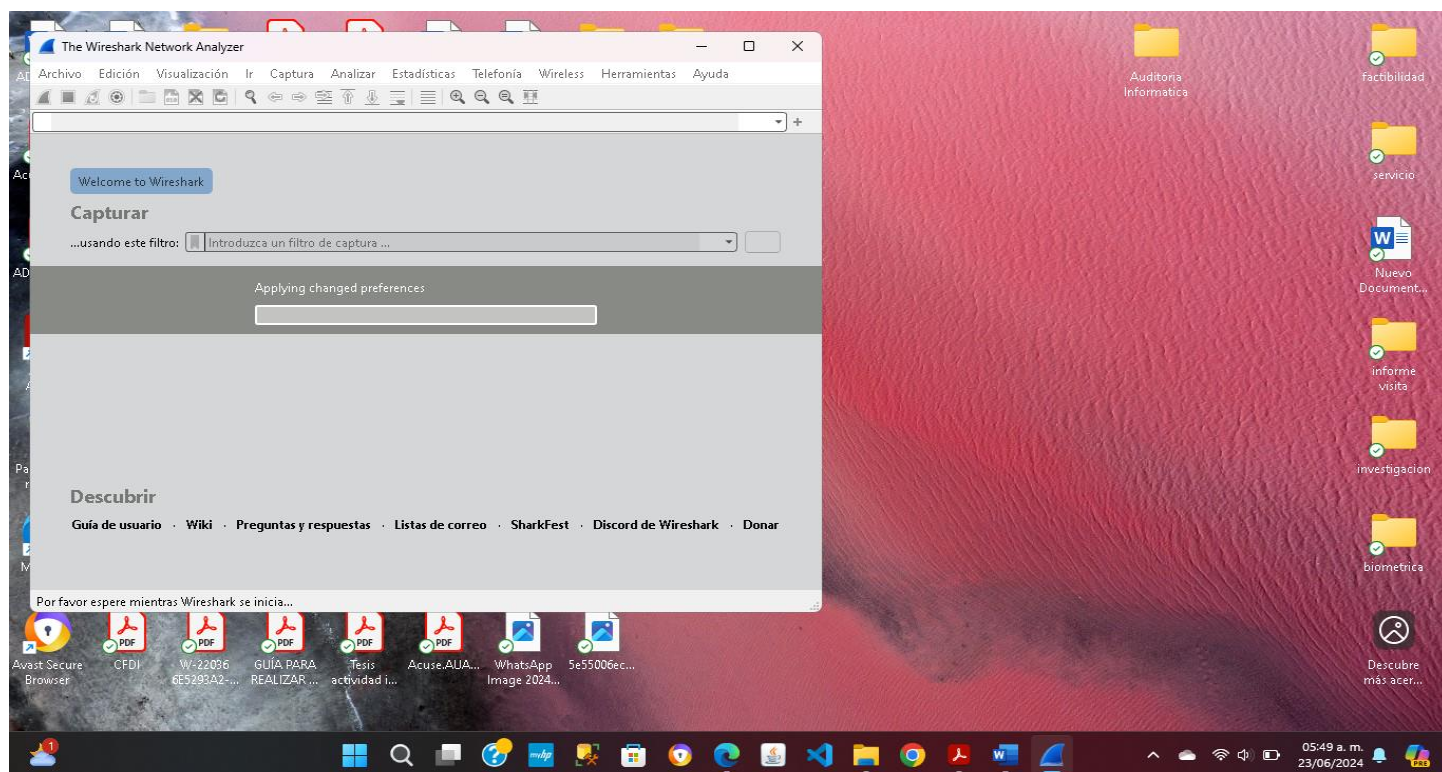
En la siguiente imagen se observa el avance de la instalación de WireShark.



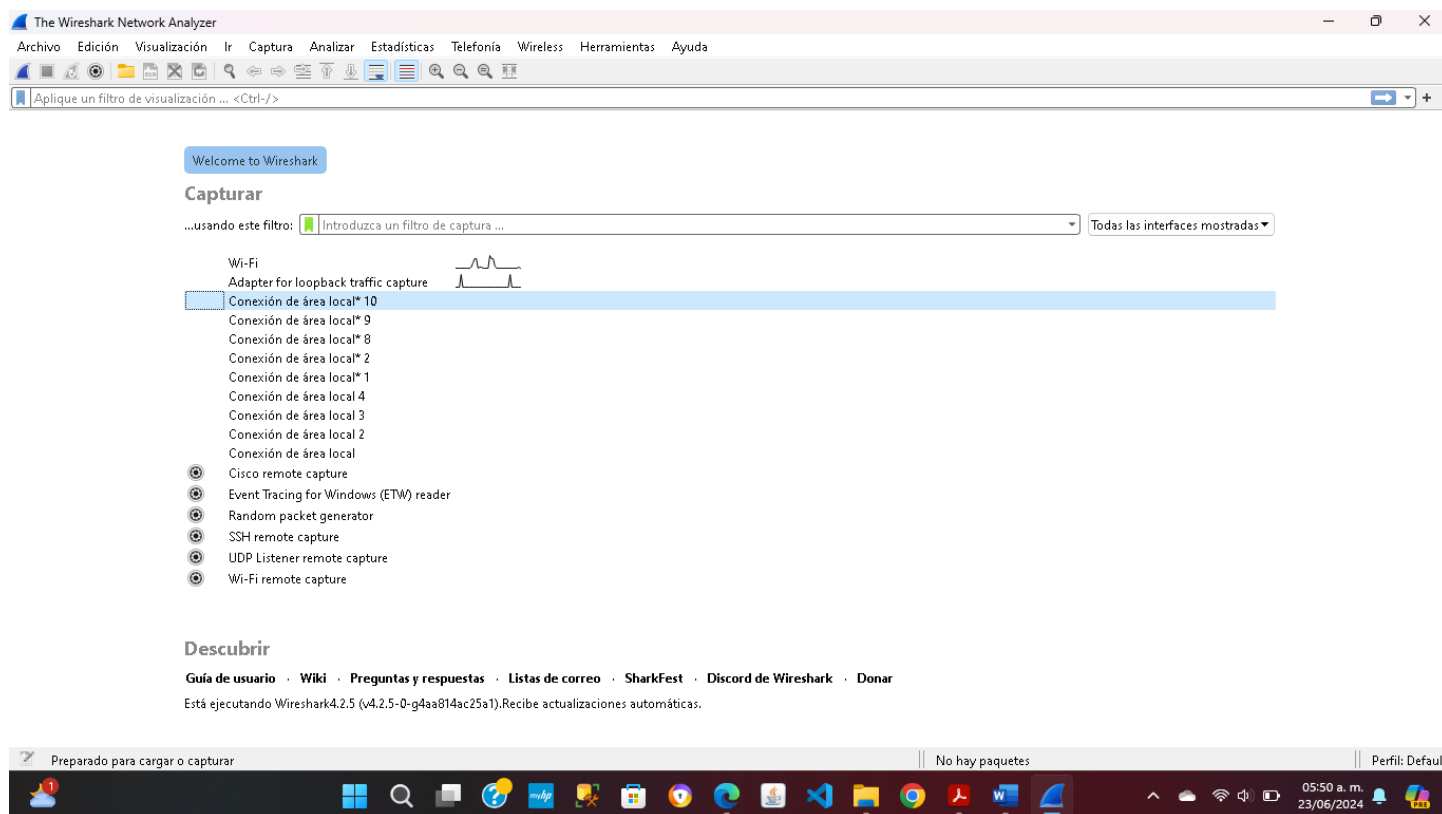
A continuación, podemos observar que esta por finalizar la instalación WireShark.



En la siguiente imagen se me muestra la pantalla de inicio de Wireshark una vez que esta la fue instalada y le damos iniciar como lo indica la actividad.



En la siguiente imagen se podemos observar que se abrió el programa *WireShark*.



Una vez que ya logramos el ingreso a la opción *Wifi* nos permite visualizar la siguiente pantalla.

Capturando desde Wi-Fi

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasTelefoníaWirelessHerramientasAyuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	52.108.248.10	192.168.0.100	TLSh1.2	88	Application Data
2	0.049147	192.168.0.100	52.108.248.10	TCP	54	62492 → 443 [ACK] Seq=1 Ack=34 Win=513 Len=0
3	0.050622	52.108.248.10	192.168.0.100	TCP	88	[TCP Spurious Retransmission] 443 → 62492 [PSH, ACK] Seq=1 Ack=1 Win=2051 Len=33
4	0.050725	192.168.0.100	52.108.248.10	TCP	66	[TCP Dup ACK 2#1] 62492 → 443 [ACK] Seq=1 Ack=34 Win=513 Len=0 SLE=1 SRE=34
5	5.370543	52.108.248.10	192.168.0.100	TLSh1.2	88	Application Data
6	5.416859	192.168.0.100	52.108.248.10	TCP	54	62493 → 443 [ACK] Seq=1 Ack=34 Win=513 Len=0
7	7.372995	52.108.248.10	192.168.0.100	TLSh1.2	88	Application Data
8	7.427395	192.168.0.100	52.108.248.10	TCP	54	62494 → 443 [ACK] Seq=1 Ack=34 Win=516 Len=0
9	11.131985	192.168.0.100	20.7.1.246	TLSh1.2	97	Application Data
10	11.459294	192.168.0.100	20.7.1.246	TCP	97	[TCP Retransmission] 50602 → 443 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=43
11	11.461491	20.7.1.246	192.168.0.100	TLSh1.2	228	Application Data
12	11.506463	192.168.0.100	20.7.1.246	TCP	54	58602 → 443 [ACK] Seq=44 Ack=175 Win=511 Len=0

> Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF...
> Ethernet II, Src: TendaTechnol_f9:ab:d8 (d8:32:14:f9:ab:d8), Dst: AzureWaveTec_3b:1f:11 (50:54:00:3b:1f:11)
> Internet Protocol Version 4, Src: 52.108.248.10, Dst: 192.168.0.100
> Transmission Control Protocol, Src Port: 443, Dst Port: 62492, Seq: 1, Ack: 1, Len: 33
> Transport Layer Security

0000 50 5a 65 3b 1f 11 d8 32 14 f9 ab d8 08 00 45 00 PZe;...2E-
0010 00 49 4f c6 40 00 6f 06 ce 65 34 6c f8 0a c0 a8 IO@o...e1....
0020 00 64 01 bb f4 1c a1 15 79 79 3e 33 e9 3b 50 18 d.....yy>3;P
0030 08 03 4a 8b 00 00 17 03 03 00 1c 00 00 00 00 00 08 03 4a 8b 00 00 17 03 03 00 1c 00 00 00 00 00 00 00 00
0040 00 00 56 e6 cd 81 40 1c 21 6f 9e 75 7b b0 9c 0f ..V...@.to-u{...
0050 b9 3e 58 4f cb 08 e9 dc >XO.....

Wi-Fi: <live capture in progress>

Paquetes: 12 · Mostrado: 12 (100.0%)

Perfil: Default

Ataque al sitio

A continuación, ingresare al sitio web en el navegador de mi preferencia mediante el siguiente link <http://www.pruebadeuso.com/index.php?r=site/login>, en el cual llevare a cabo el ataque al sitio web.

Tiburón de alambre · Profi xDescargar Burp Suite Com xComo descargar e instala x(1) WhatsApp xPrueba de uso - Login Site x

No seguro | www.pruebadeuso.com/index.php?r=site/login

Publi legal

Iniciar sesión

Usuario

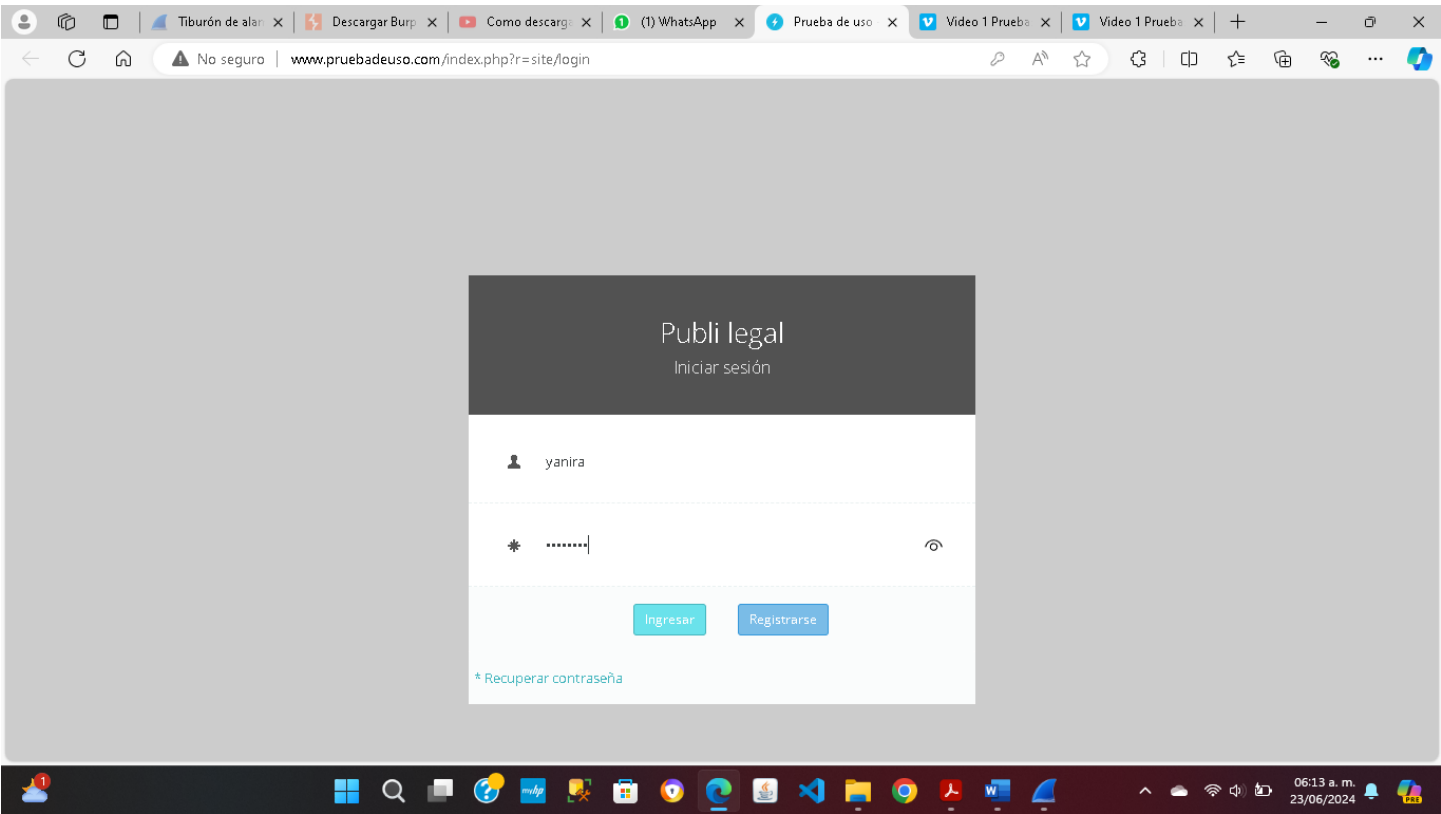
Contraseña

IngresarRegistrarse

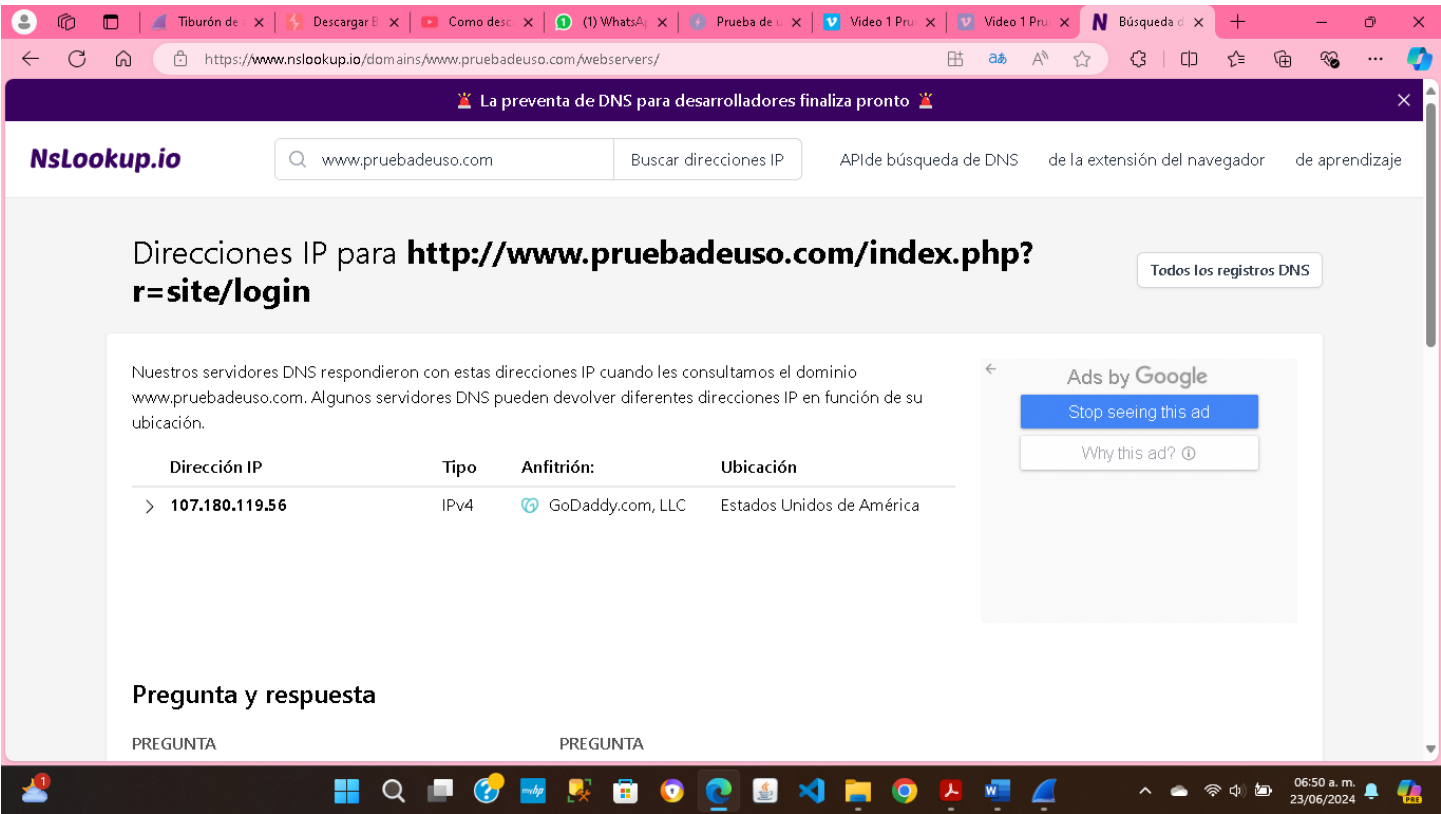
* Recuperar contraseña

06:04 a. m.
23/06/2024

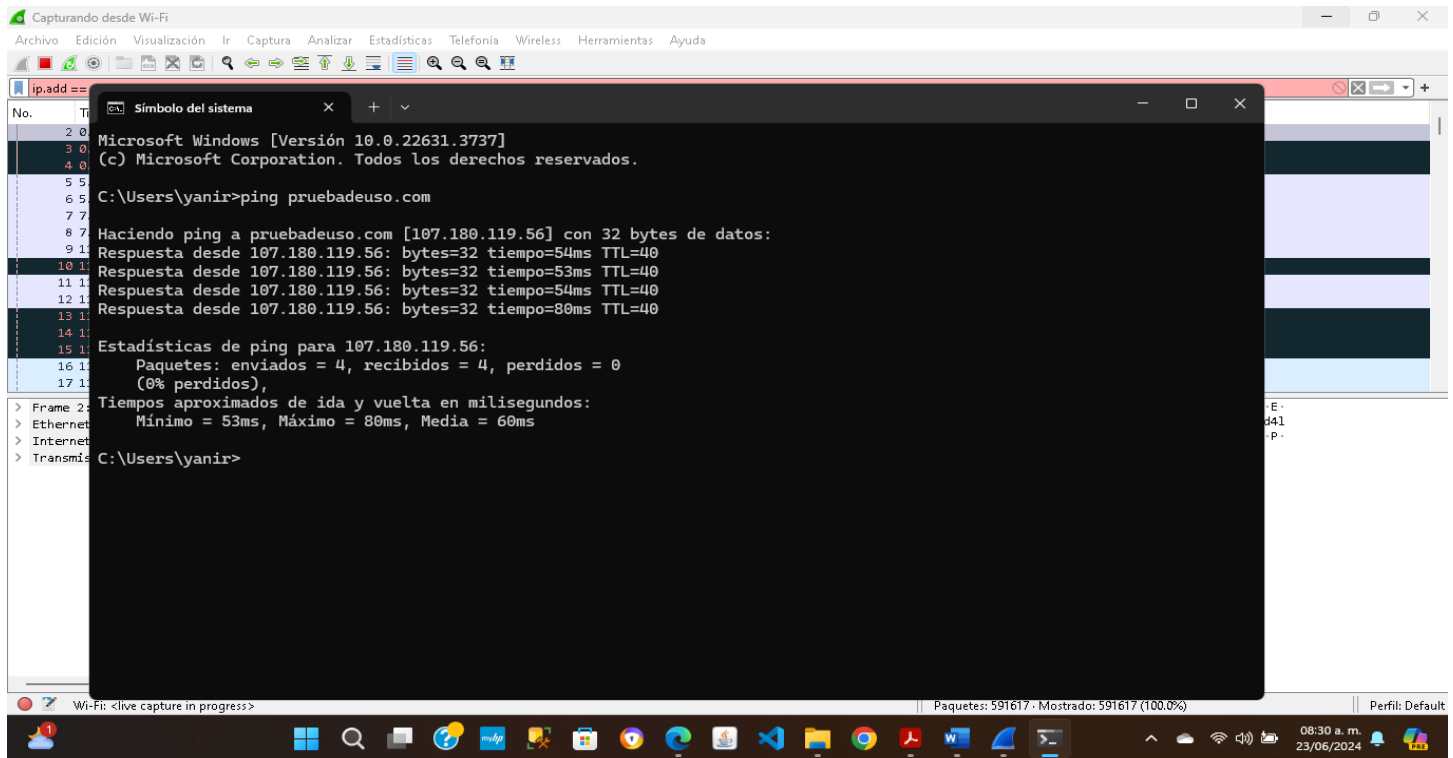
A continuación, intentare iniciar sesión utilizando credenciales incorrectas (esto no permitirá iniciar sesión).



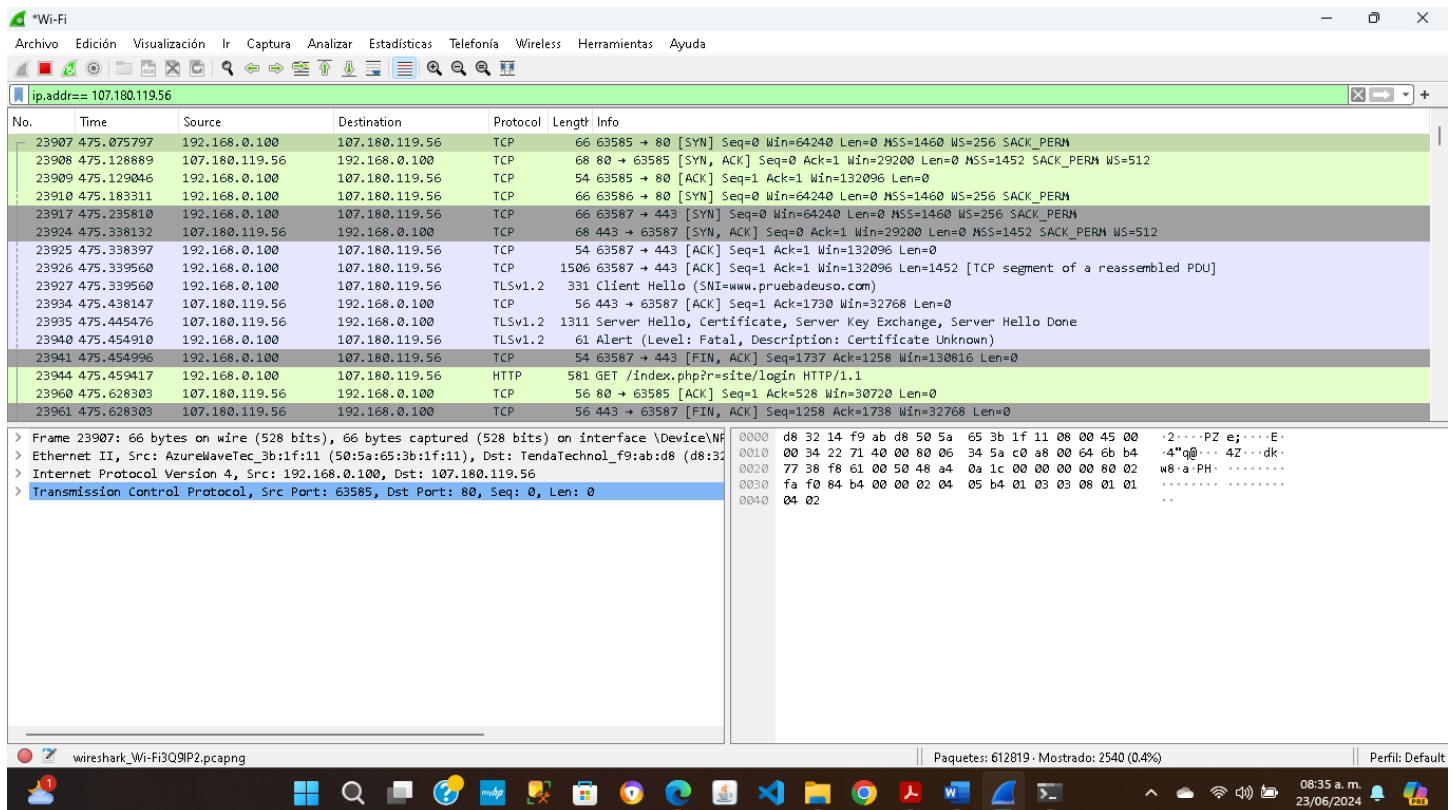
En la siguiente imagen podemos observar que se logró entrar a la configuración del servidor de la sitio web, y buscar su dirección IP.



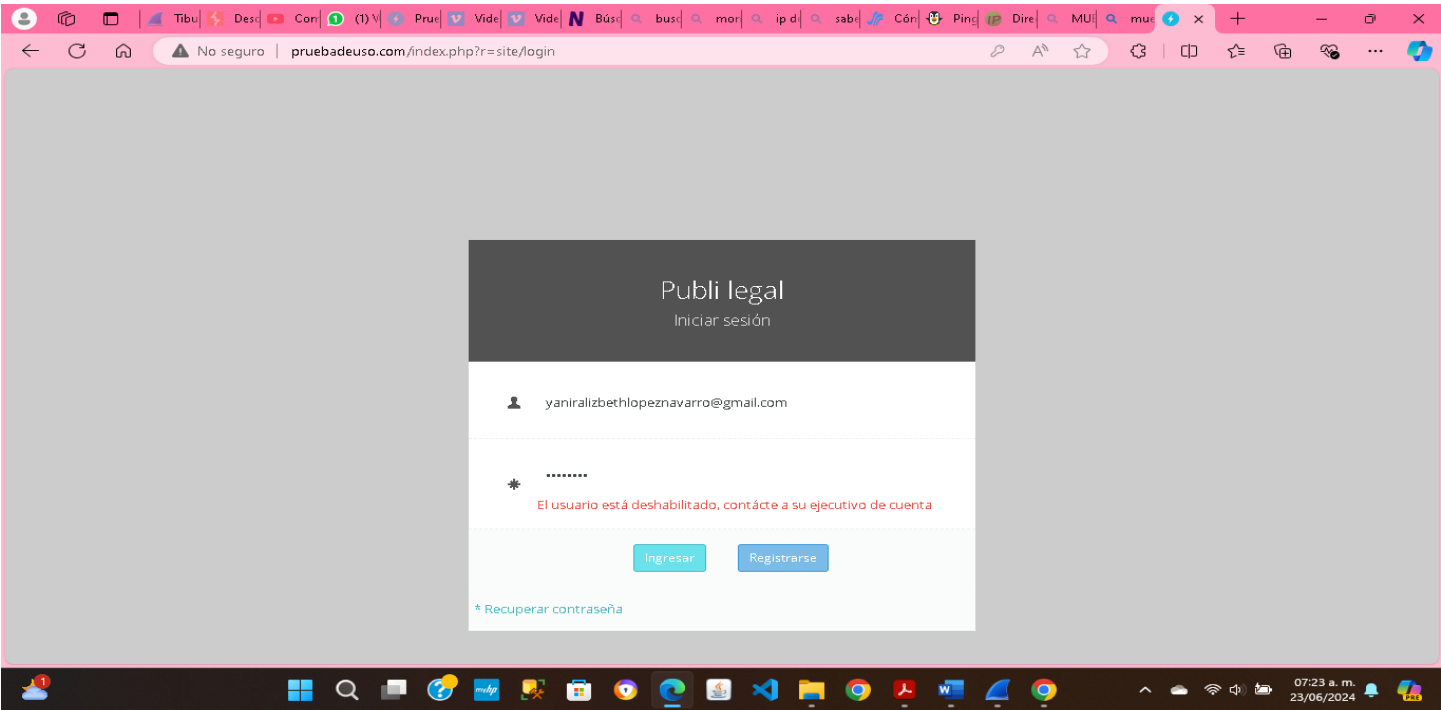
Aun cuando ya conocemos la ip del sitio web que vamos a atacar realice una confirmación de que la ip es correcto mediante el CMD de mi computadora.



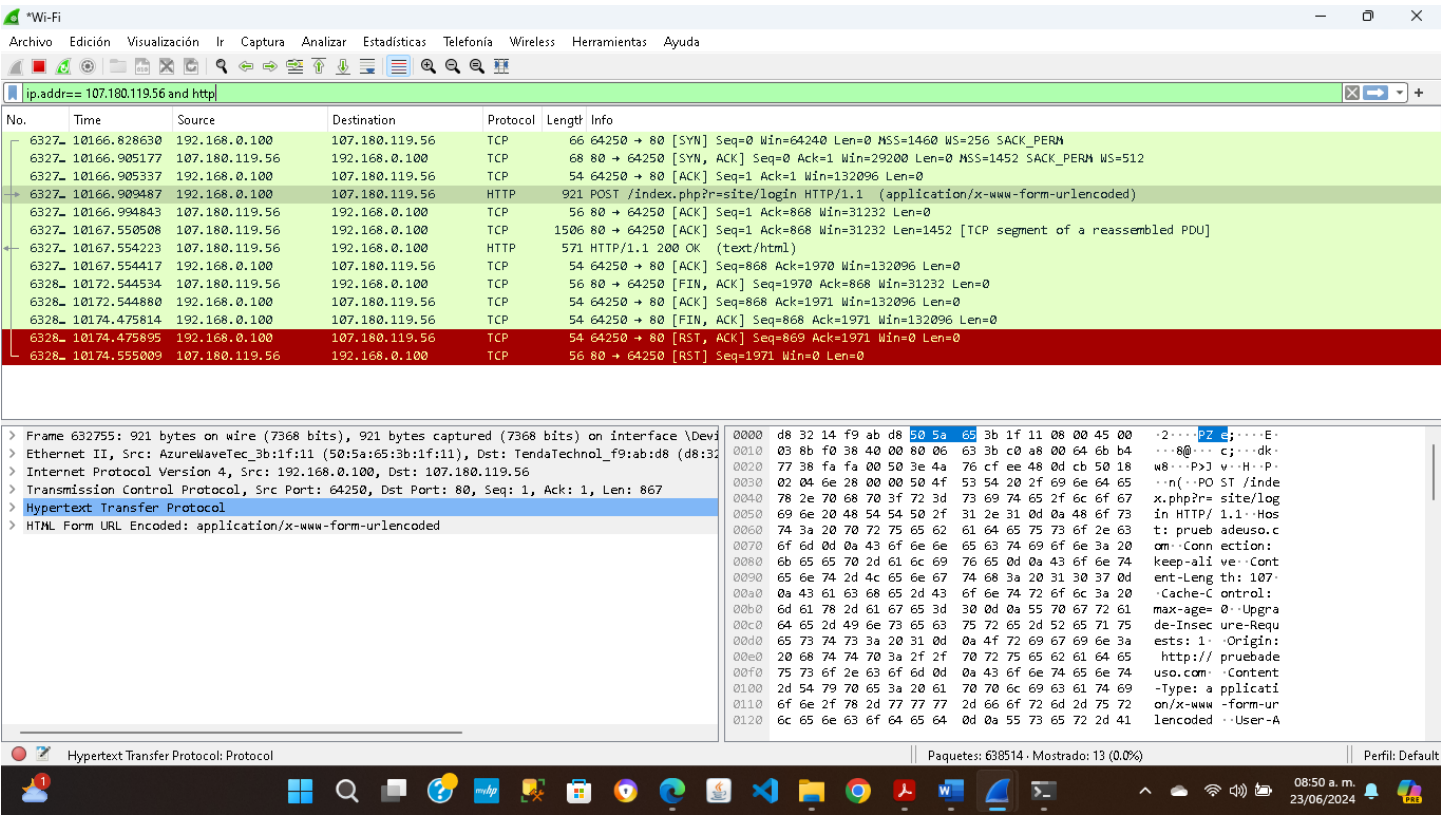
A continuación, se realizó la *búsqueda* de la dirección IP en WireShark mediante el siguiente comando:
ip. Add == dirección IP



Intentamos volver al sitio web e ingresar los datos de manera correcta aun que no nos permite debido a que el sitio web no es de mi propiedad y no cuento con las credenciales correctas.



A continuación, se muestra en Wireshark se puede ver las acciones que ha realizado la dirección IP del sitio web. Buscar mediante una opción que en protocolo tenga HTTP, así como la palabra POST.



A continuación, se muestra el resultado una vez que se dio clic derecho sobre la opción con las características anteriores y seleccionar *Seguir*.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The main window is titled "Wireshark · Seguir secuencia TCP (tcp.stream eq 8613) · Wi-Fi".

The packet list on the left shows a series of packets. Packet 63275 is selected, showing details for the Hypertext Transfer Protocol (HTTP) and HTML Form URL Encoded data. The details pane on the right shows the selected packet's structure, including the POST request to /index.php?r=site/login, the Host (pruebadeuso.com), and the Content-Type (application/x-www-form-urlencoded). The HTML Form URL Encoded data is visible, showing the username and password fields.

The packet details pane shows the following information:

- POST /index.php?r=site/login HTTP/1.1
- Host: pruebadeuso.com
- Connection: keep-alive
- Content-Length: 107
- Cache-Control: max-age=0
- Upgrade-Insecure-Requests: 1
- Origin: http://pruebadeuso.com
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Referer: http://pruebadeuso.com/index.php?r=site/login
- Accept-Encoding: gzip, deflate
- Accept-Language: es-es;q=0.9,en;q=0.8,en-gb;q=0.7,en-us;q=0.6,es-mx;q=0.5,es-us;q=0.4
- Cookie: PHPSESSID=ff4566b1d57d876cc06a433e89de2985

The packet details pane also shows the HTML Form URL Encoded data, which includes the username and password fields. The username is "yaniralizbethlopeznavarro40@gmail.com" and the password is "95659201&yt0=IngresarHTTP/1.1 200 OK".

Con esto nos permite visualizar el usuario/correo y contraseña con el que se intentó el inicio sesión en el sitio web.

Conclusión

La realización de esta actividad ha sido fundamental para comprender de manera profunda las vulnerabilidades que existen en las aplicaciones web sin medidas de seguridad adecuadas. En el ámbito laboral, adquirir esta experiencia nos capacita para identificar y corregir fallos en la seguridad de los sistemas que desarrollamos, asegurando que las aplicaciones que lanzamos al mercado protejan eficazmente la información de los usuarios.

En nuestra vida cotidiana, este conocimiento nos hace más conscientes de los riesgos a los que estamos expuestos al navegar por internet y utilizar diferentes servicios en línea. Entender cómo los datos pueden ser interceptados y utilizados de manera indebida nos motiva a ser más cuidadosos con la información que compartimos y a preferir sitios web que implementen medidas de seguridad robustas como el SSL.

Además, esta actividad nos ha demostrado la importancia de estar siempre actualizados y preparados para enfrentar los desafíos de la ciberseguridad. En un mundo cada vez más interconectado, proteger la información personal y corporativa es una responsabilidad compartida. A través de ejercicios prácticos como este, fortalecemos nuestras habilidades y contribuimos a un entorno digital más seguro y confiable para todos.

Referencias

Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 10 de junio de 2024, umi.edu.mx/coppel/IDS/mod/scorm/player.php

Video conferencing, web conferencing, webinars, screen sharing. (s. f.). Zoom. https://academiaglobal-mx.zoom.us/rec/play/1MpPOitg1mPH7hMrQbeKHuOfNATsJi8d-11SrXSJAu47yV86hS2ucF5HuPqQNqN-5pZJMIbN4JUyp-k.dq6TBS1J-S98frpn?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FMpClRdjf8kiSF7ceZKjOQ_bXHsOk1vjK9p0eC9-NBgN1d51EH3XfjvPqcYahxers.doPPNRS_HIQiVvgg

Global, A. (2024, 23 junio). *Video 1 Pruebas de Vulnerabilidades Pérdida de Autenticación y Gestión de Sesiones.mp4* [Vídeo]. Vimeo. <https://vimeo.com/711845557/a5ae411ce9>