UD1 - ACTIVIDAD 2:

Análisis de tramas de un acceso HTTP - Wireshark

Unidad 1: Principios de Seguridad

Seguridad y Alta Disponibilidad

2º ASIR

Mei Núñez Sanz

16 de septiembre de 2024

DESCRIPCIÓN DE LA ACTIVIDAD PRÁCTICA

1. Introducción

En el área de la seguridad informática, es necesario comprender cómo se transmiten los datos a través de las redes y los riesgos asociados con el uso de protocolos no seguros, como HTTP. Una de las herramientas más utilizadas para analizar el tráfico de red y detectar posibles vulnerabilidades es **Wireshark**.

Wireshark es una herramienta de análisis de redes que permite capturar y examinar el tráfico que circula a través de una red en tiempo real. Funciona como un **sniffer** o rastreador de paquetes, lo que significa que puede interceptar, registrar y analizar los datos transmitidos entre dispositivos en la red.

Un **sniffer**, también conocido como analizador de paquetes, es un software diseñado para monitorear y analizar el tráfico de red. Estas herramientas permiten a los administradores de sistemas y expertos en seguridad capturar paquetes de datos, examinar su contenido y estructura, y diagnosticar posibles problemas o vulnerabilidades en la red.

El objetivo de esta práctica es realizar un **análisis de tráfico HTTP** utilizando **Wireshark**, enfocándonos en la captura de tramas que implican un proceso de autenticación (login) en un sitio web que no utiliza cifrado, es decir, mediante **HTTP**.

El análisis se centrará en capturar y examinar los datos intercambiados entre el cliente y el servidor, durante el inicio de sesión en la URL: http://celfi.gob.ar.

2. Instalación y configuración de WIRESHARK

2.1. Descargar Wireshark

Accede al sitio oficial de Wireshark a través de:

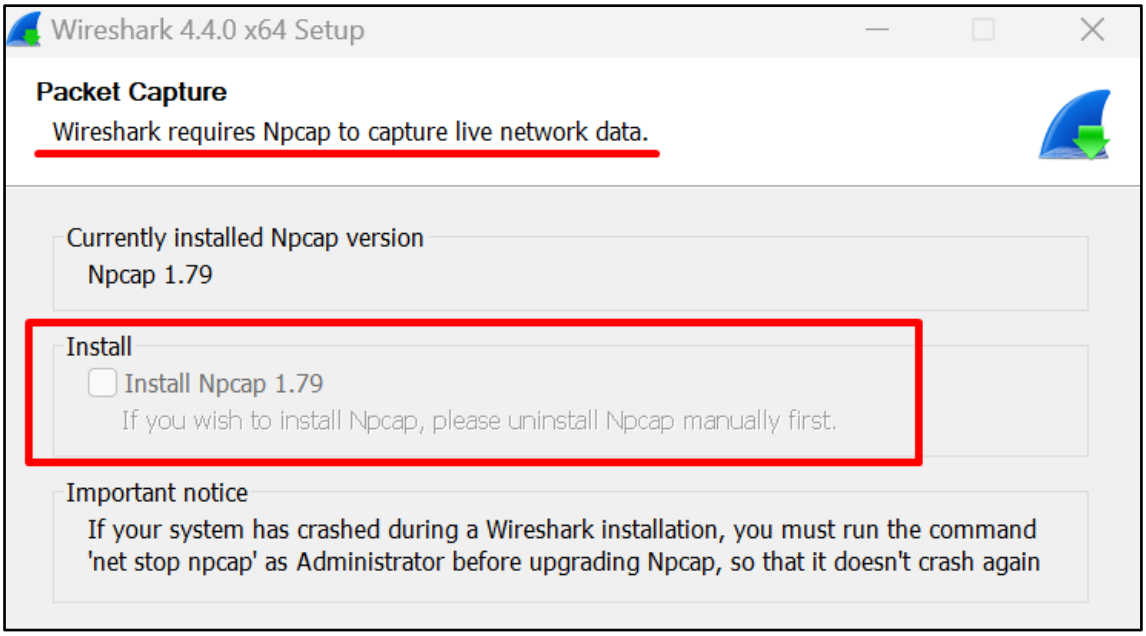
- https://www.wireshark.org/download.html.

Una vez descargado el instalador correspondiente a tu sistema operativo y ejecútalo para iniciar la instalación.

2.2. Instalación de Npcap

Durante la instalación de Wireshark, se indicará que esta herramienta necesita Npcap para capturar el tráfico de red en vivo.

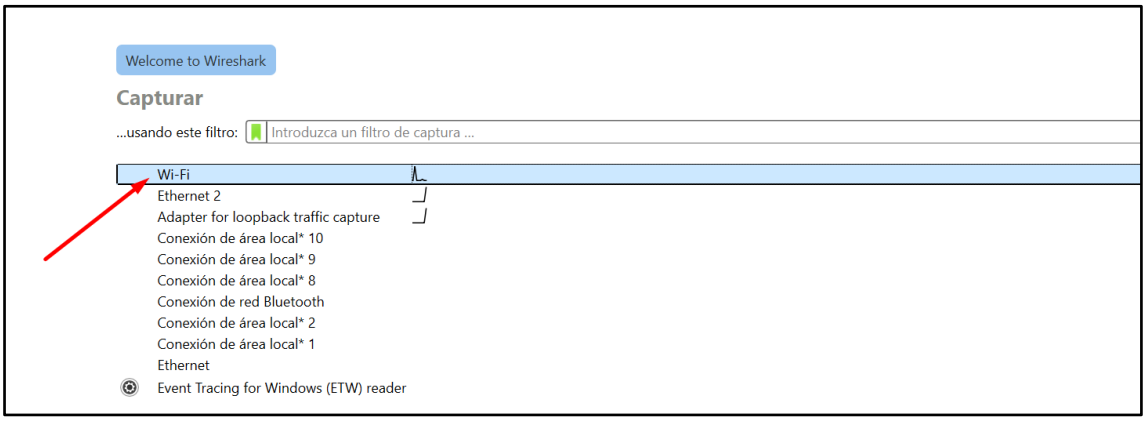
- Si Npcap ya está instalado y actualizado, la casilla de instalación estará desmarcada.
- Si su versión instalada de Npcap es anterior a la versión que viene con Wireshark, se recomienda que se instale la versión más reciente haciendo clic en la casilla de verificación **Install Npcap**



2.3. Finalizar la instalación

Una vez completada la instalación, haz clic en **Finish** para cerrar el asistente y ejecútalo.

Si todo está instalado correctamente, Wireshark debería detectar tus interfaces de red y permitir la captura de tráfico en tiempo real.

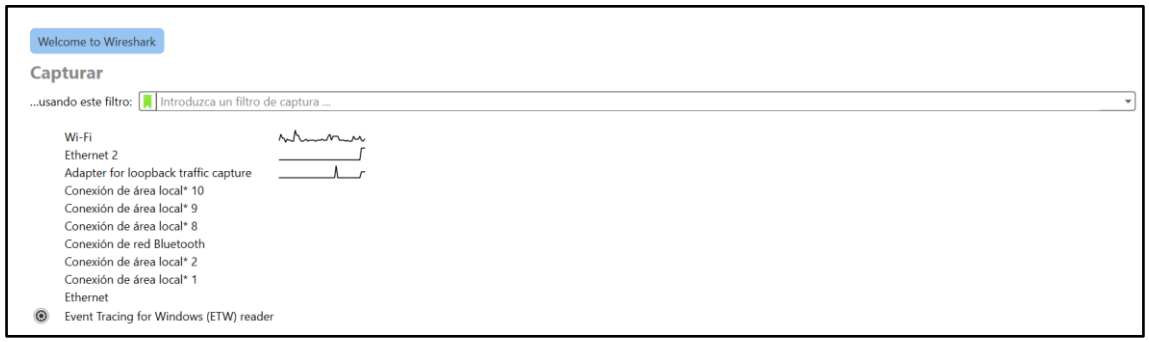


3. Iniciar Wireshark

Para capturar el tráfico HTTP con Wireshark, seguiremos unos sencillos pasos que nos permitirán monitorear y analizar el tráfico en tiempo real mientras navegamos por una página web no segura.

3.1. Ejecutar Wireshark:

Inicia Wireshark para capturar y analizar los paquetes de datos que circulan a través de la red. Esta herramienta permite obtener detalles sobre las solicitudes y respuestas HTTP, facilitando el análisis del tráfico web no cifrado.



3.2. Seleccionar la interfaz de red

En la pantalla principal de Wireshark, se mostrará una lista de interfaces de red disponibles, como **Wi-Fi**, **Ethernet** y **Conexión de Área Local**.

Las diferentes opciones de red representan distintos métodos de conexión a internet o a una red local. Por lo tanto, es necesario seleccionar la interfaz más adecuada para poder capturar correctamente el tráfico de red que se va a analizar.

¿Cómo saber qué interfaz seleccionar para capturar tráfico en Wireshark?

- **Wi-Fi**: Es la interfaz que tendrá que elegir si se está conectado a internet de forma inalámbrica. Esta interfaz captura todo el tráfico que pasa a través del adaptador Wi-Fi.

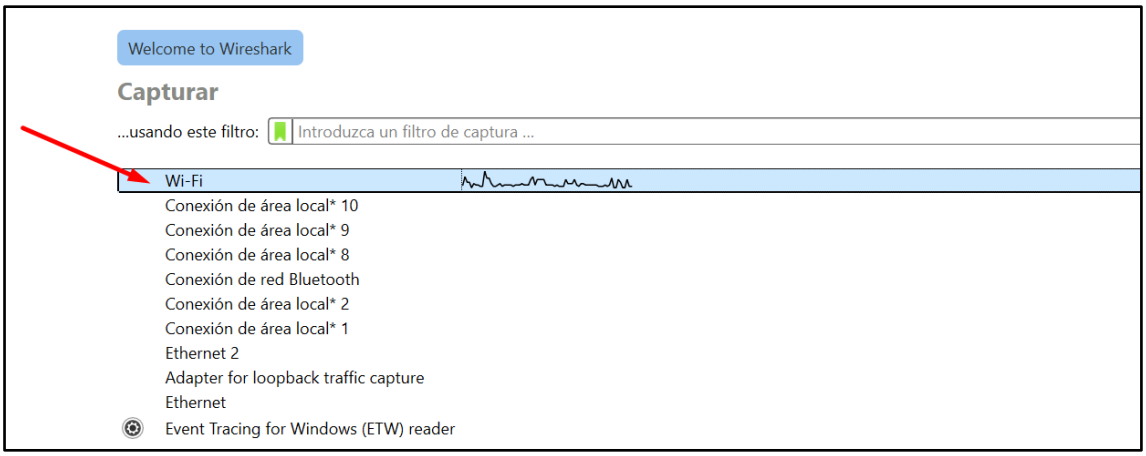
- **Ethernet**: Se refiere a las conexiones por cable. Si estás conectado directamente al router mediante un cable de red, esta es la interfaz que se deberá seleccionar.

- **Conexión de Área Local**: Hace referencia a conexiones físicas o virtuales (VPN, redes internas). Se optará esta opción si se está utilizando algún tipo de conexión interna a través de una LAN o VPN.

¿Por qué seleccionamos el adaptador Wi-Fi para el análisis?

Para esta práctica, el ordenador estará conectado a internet de manera inalámbrica a través de Wi-Fi. Por lo tanto, es necesario seleccionar la interfaz **Wi-Fi** en Wireshark para capturar el tráfico de red adecuado.

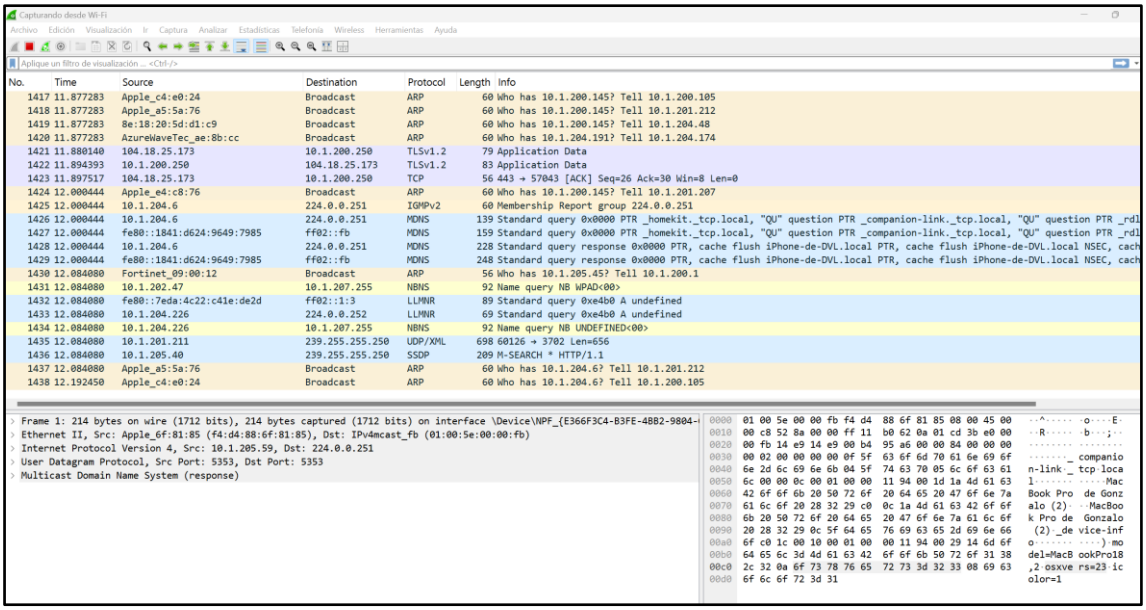
Al elegir esta interfaz, nos aseguramos que Wireshark registre el tráfico que circula a través de la conexión inalámbrica utilizada por el equipo.



3.3. Iniciar y detener la captura:

1. Iniciar captura:

Una vez seleccionada la interfaz adecuada, en este caso el adaptador Wi-Fi, Wireshark comenzará automáticamente a capturar el tráfico de la red en tiempo real. La herramienta empezará a registrar todos los paquetes de datos que pasan a través de la interfaz seleccionada.



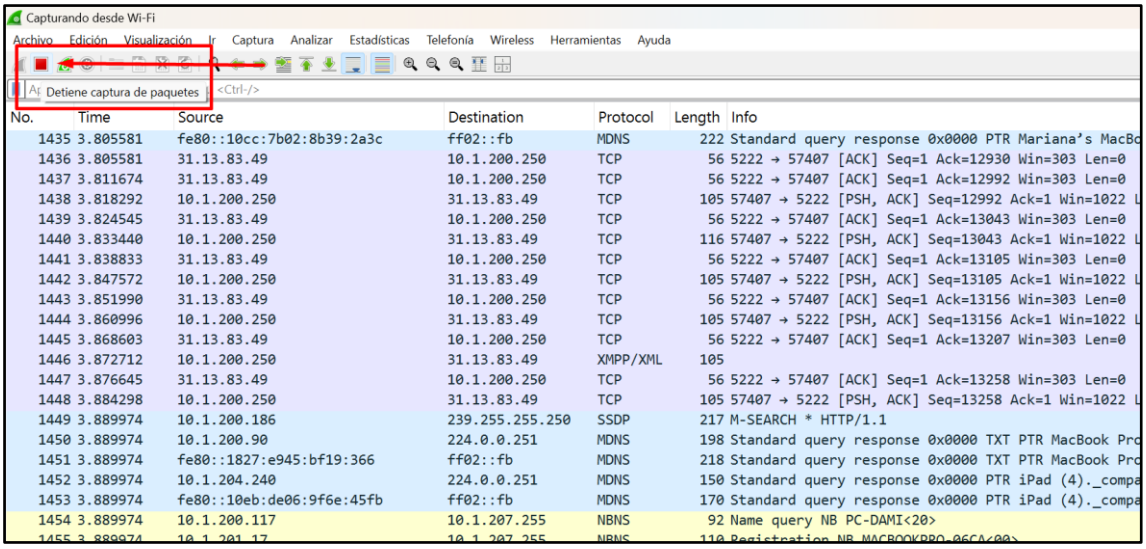
Como se puede ver en la imagen, en Wireshark, cada trama capturada muestra información detallada en varias columnas. Los principales campos de cada paquete son:

- **Número (No.):** Un identificador único asignado a cada paquete para facilitar su referencia y análisis.
- **Tiempo (Time):** La marca temporal que indica cuándo se capturó el paquete. Muestra el tiempo transcurrido desde el inicio de la captura.
- **Origen (Source):** La dirección IP o la dirección MAC del dispositivo desde el que se envió el paquete. Indica el origen del tráfico.
- **Destino (Destination):** La dirección IP o la dirección MAC del dispositivo al que se dirige el paquete. Indica el destinatario del tráfico.
- **Protocolo (Protocol):** El protocolo de red utilizado en el paquete (por ejemplo, HTTP, TCP, UDP). Muestra el tipo de comunicación que está ocurriendo.
- **Longitud (Length):** El tamaño del paquete en bytes, que indica la cantidad de datos transportados.

Estos campos permiten analizar y entender el tráfico de red, identificando detalles importantes sobre cada paquete capturado.

2. **Detener la captura**:

Para detener la captura, vuelve a Wireshark y haz clic en el botón rojo de **"Detener captura"** (botón rojo). Esto finalizará el registro de datos y permitirá que examines los paquetes capturados durante el análisis.



4. Capturar el tráfico de un acceso HTTP con Wireshark

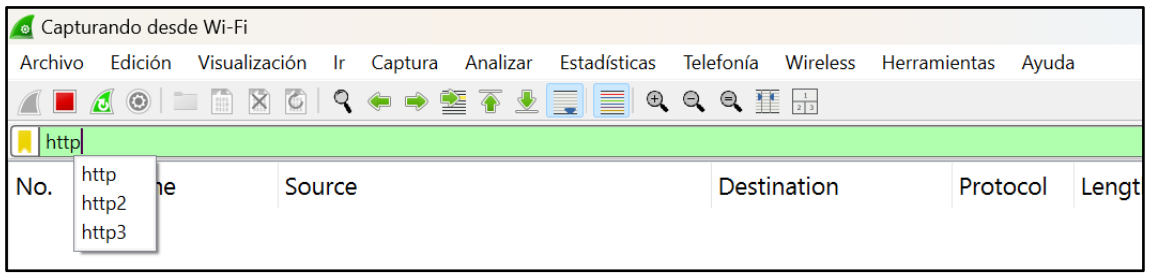
En este apartado, comenzaremos a capturar el tráfico de red generado durante un acceso a un sitio web HTTP no seguro.

El objetivo es analizar el proceso de autenticación (login) para identificar posibles vulnerabilidades, como el envío de credenciales en texto plano.

4.1. Filtrar por protocolo HTTP:

Para enfocar la práctica únicamente en el tráfico HTTP, deberemos escribir "**http**" en la barra de filtros en la parte superior de Wireshark.

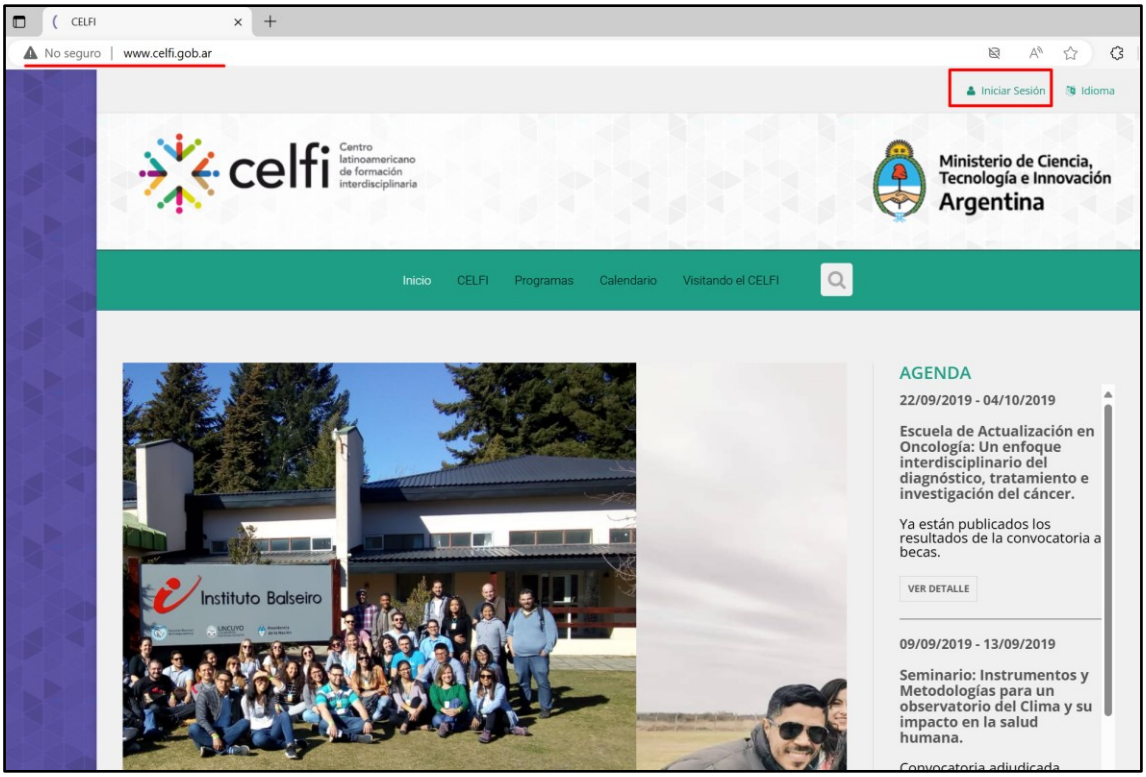
Esto nos permitirá filtrar el tráfico de red para mostrar solo las tramas relacionadas con el protocolo HTTP.



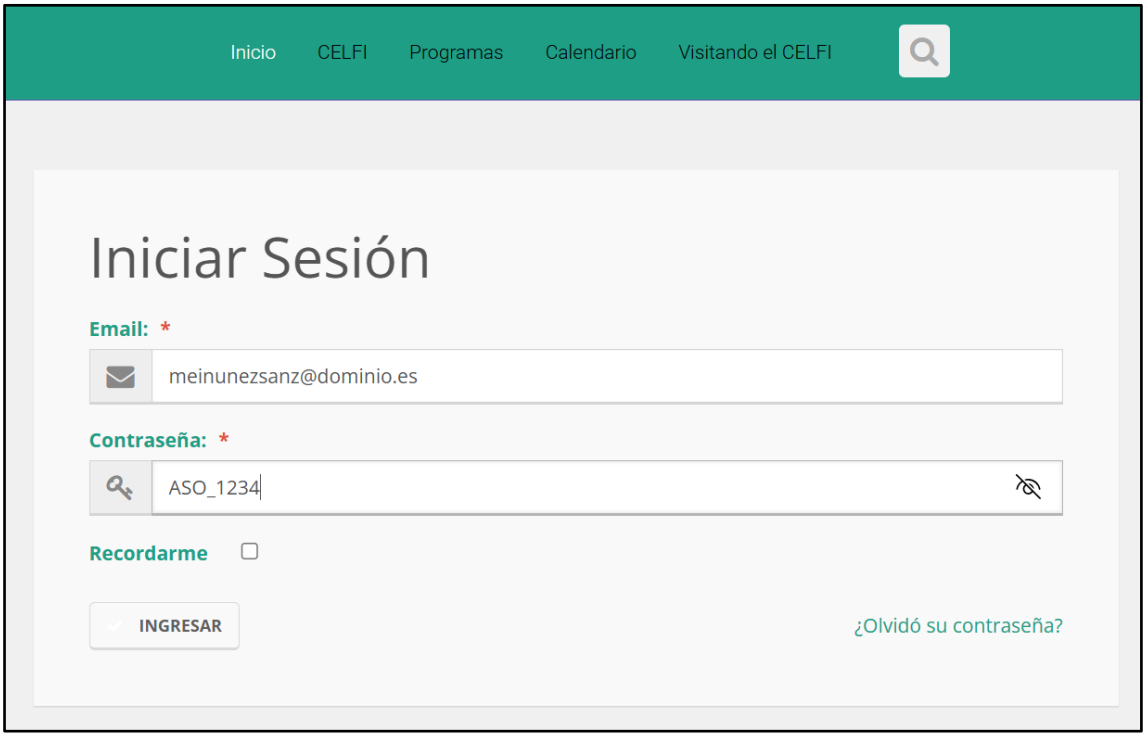
4.2. Acceder al sitio web HTTP:

Abriremos el navegador y accederemos a la página web: http://celfi.gob.ar, un sitio web no seguro, ya que comienza con "**http://**".

A continuación, realizaremos un procedimiento de autenticación (login), simulando que estamos iniciando sesión en el sitio.



Para ello, utilizaremos un **correo electrónico y una contraseña ficticia**, con el fin de observar cómo se transmiten estos datos en texto plano, lo que permitirá identificar posibles vulnerabilidades en la comunicación y riesgos en la seguridad de los datos en un sitio web no cifrado.



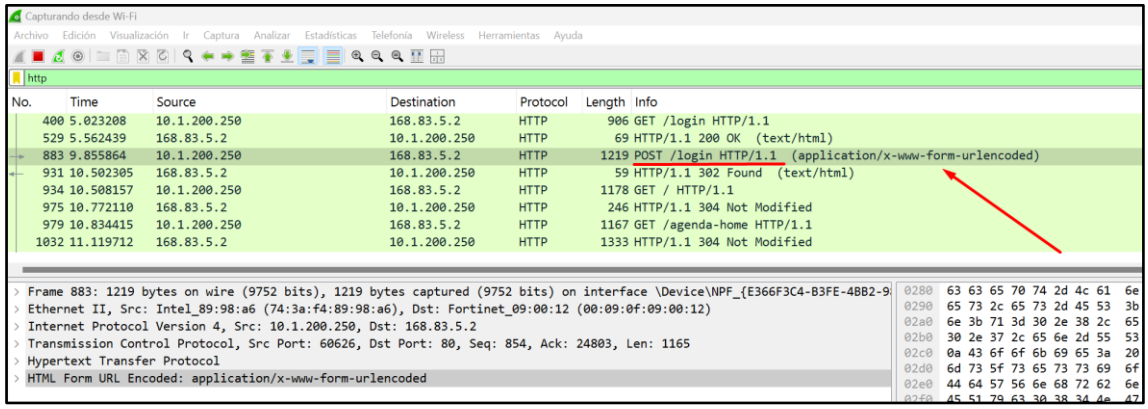
5. Análisis de la captura

Una vez que hayamos iniciado sesión, ya podremos observar el tráfico de paquetes capturados utilizando el protocolo HTTP en Wireshark.

Estos paquetes mostrarán cómo se transmiten los datos de autenticación, como el correo electrónico y la contraseña, en texto plano, lo que nos permitirá identificar las vulnerabilidades que existen en una conexión no segura.

5.1. Buscar el tráfico del login en Wireshark:

Entre las tramas HTTP que se han capturado, tendremos que identificar el paquete de login. Normalmente, los datos de inicio de sesión, como usuario y contraseña, se envían a través del método POST. Este método se utiliza para entregar los datos del formulario de autenticación.



5.2. Análisis de la trama HTTP login:

Una vez localizada la trama correspondiente al proceso de login, podremos analizar en detalle las diferentes capas del **modelo TCP/IP** y observar cómo se estructura la comunicación en cada una de ellas:

1. *Capa de Acceso a la Red (Capa 2 en OSI)*

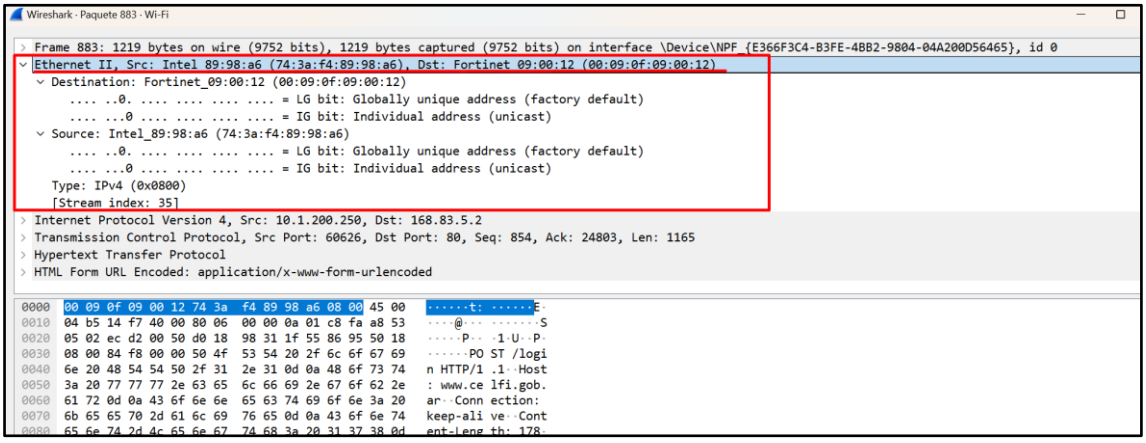
Dentro de la jerarquía del protocolo TCP/IP la capa de acceso a red se encuentra en el nivel más bajo.

Protocolo: Ethernet

En esta capa, se define cómo los datagramas IP se encapsulan en tramas que pueden ser transmitidas por la red local (LAN), como Ethernet. Aquí se manejan las direcciones **MAC** del origen y destino, que identifican los dispositivos físicos conectados a la red.

¿Cuál es la función de la capa en la trama capturada?

Transporta la trama a través de la red física hacia su destino dentro de la red local.



2. *Capa de Internet (Capa 3 en OSI)*

La capa Internet se encuentra justo encima de la capa de acceso a red.

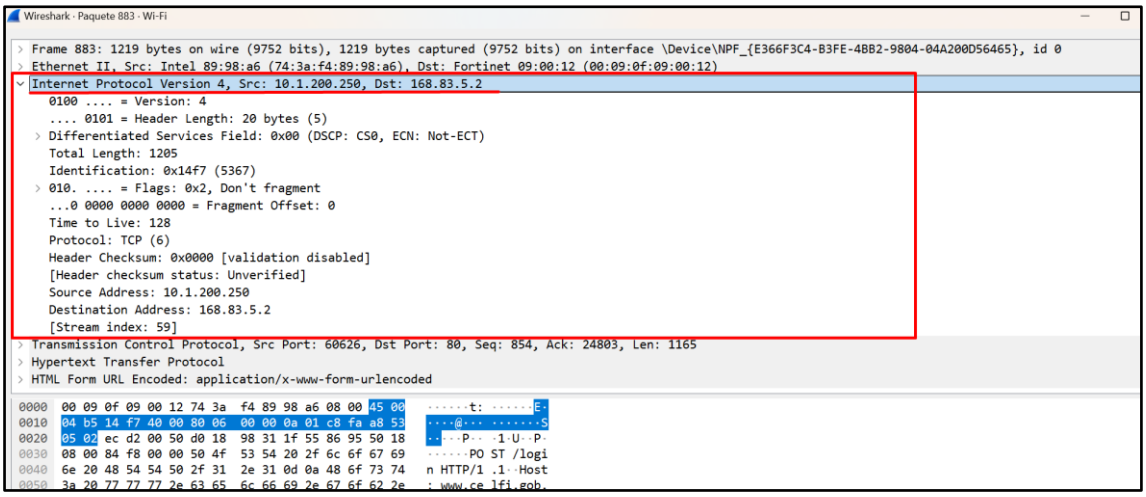
Protocolo: IP (Internet Protocol)

La capa de Internet se encarga de enrutar los paquetes desde el origen hasta el destino, utilizando direcciones IP.

En la captura, se puede observar la dirección IP del dispositivo que realiza el login y la dirección IP del servidor.

¿Cuál es la función de la capa en la trama capturada?

Asegura que los paquetes viajen entre redes y lleguen al servidor HTTP responsable de la autenticación. Además, determina la mejor ruta para los paquetes a través de la red, proporcionando los servicios necesarios para que los dispositivos finales puedan intercambiar datos entre diferentes redes.



3. *Capa de Transporte (Capa 4 en ambos modelos)*

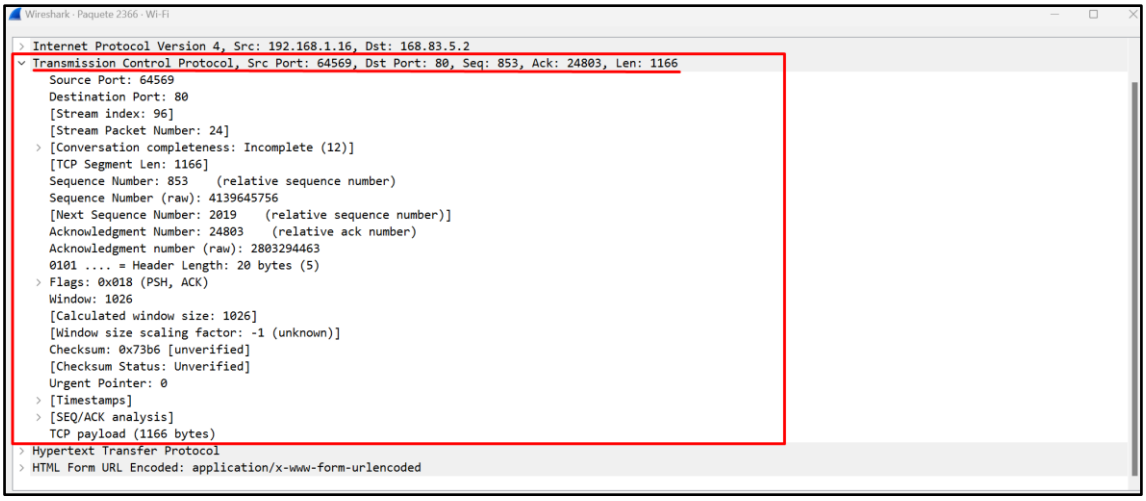
En la **Capa de Transporte** se definen los protocolos **TCP** (Transmission Control Protocol) y **UDP** (User Datagram Protocol). Esta capa es responsable de asegurar que los datos se transmitan correctamente entre el cliente y el servidor.

- **Protocolo: TCP (Transmission Control Protocol)**

En la trama capturada, se utiliza el protocolo **TCP**. Este protocolo garantiza una transmisión **confiable** y **secuenciada** de los paquetes de datos. TCP se asegura de que los paquetes lleguen en el orden correcto y sin errores, mediante el uso de confirmaciones y renvío de segmentos del paquete en el caso necesario.

- **¿Cuál es la función de la capa en la trama capturada?**

Al analizar la captura de tráfico en Wireshark, podemos ver los **números de puerto** de origen y destino. En este caso, el **puerto de destino** es el **80**, lo que indica que se está utilizando el protocolo **HTTP**, que transmite datos sin cifrado.



4. *Capa de Aplicación (Capa 7 en OSI / Aplicación en TCP/IP)*

Esta es la capa más alta dentro de la estructura jerárquica del protocolo TCP/IP y es donde se encuentran las aplicaciones y los procesos que permiten la interacción entre el cliente y el servidor.

En el caso de una captura de tráfico HTTP, la capa de aplicación es la encargada de gestionar las solicitudes y respuestas del protocolo **HTTP**.

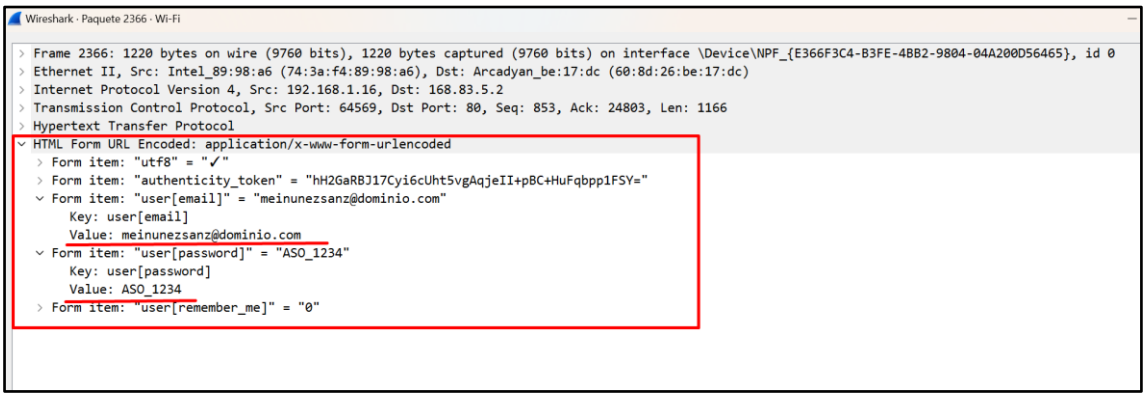
- **Protocolo: HTTP (Hypertext Transfer Protocol)**

HTTP permite la comunicación entre un servidor web y un navegador, facilitando la entrega de contenido web a los usuarios. Sin embargo, al no contar con cifrado, los datos transmitidos, como credenciales o información personal, se envían en **texto plano**, lo que deja la información expuesta a posibles intercepciones.

- **¿Cuál es la función de la capa en la trama capturada?**

En la trama capturada en Wireshark, al expandir la sección **HTTP**, podemos observar la solicitud **POST**. Este método se utiliza para enviar los datos de un formulario de autenticación, incluyendo el correo electrónico y la contraseña.

Dado que HTTP no proporciona cifrado, esta información se transmite en **texto plano**, lo que la expone a posibles interceptaciones por parte de atacantes.



- **¿Por qué es Vulnerable?**

El uso de HTTP (a través del **puerto 80**) hace que la comunicación sea vulnerable porque:

1. **Texto plano**: Los datos sensibles, incluidas las credenciales de acceso, se transmiten sin cifrado. Cualquier atacante que intercepte el tráfico podrá ver esta información fácilmente.

2. **Falta de cifrado**: A diferencia de **HTTPS** (que utiliza el **puerto 443** y añade seguridad mediante cifrado SSL/TLS), **HTTP** no garantiza la confidencialidad ni la integridad de los datos transmitidos exponiendo la información.

- **Función de los Puertos en la Comunicación**

1. **Puerto 80**: Es el puerto estándar para HTTP, utilizado para transmitir páginas web en texto plano, lo que implica que la comunicación no está protegida frente a robo de información.

2. **Puerto 443**: Utilizado para HTTPS, que proporciona una capa de seguridad adicional mediante cifrado SSL/TLS, asegurando que los datos transmitidos no puedan ser leídos ni manipulados por terceros.

En una comunicación entre un cliente (navegador web) y un servidor, los **puertos** actúan como puntos lógicos de entrada y salida para los datos. Para que esta transmisión sea posible, se utiliza un **socket**, que combina una **dirección IP** con un **número de puerto**, creando un canal de comunicación que permite el intercambio de información entre ambos dispositivos.

6. Conclusiones:

1. Captura de Tráfico HTTP:

La captura del tráfico HTTP mediante herramientas como Wireshark nos informa cómo se transmiten las solicitudes y respuestas entre el navegador web y el servidor.

La captura de tráfico en HTTP permite observar los detalles de la comunicación, incluyendo información vulnerable como credenciales de acceso, en texto plano.

2. Vulnerabilidad de HTTP:

Información en Texto Plano: HTTP no proporciona cifrado para los datos transmitidos. Esto expone cualquier información mostrándola en texto plano y fácilmente interceptada por un atacante.

Falta de Seguridad: Sin mecanismos de cifrado, los datos están expuestos a posibles ataques de "sniffing", técnica utilizada en redes que puede ser empleada con intenciones maliciosas para capturar y analizar los paquetes de datos que viajan a través de una red. Esto pone en riesgo la confidencialidad y la integridad de la información transmitida.

3. Comparación con HTTPS:

HTTPS: Utiliza el puerto 443 y proporciona una capa adicional de seguridad mediante cifrado SSL/TLS. Esto garantiza que los datos se transmitan de forma segura, impidiendo que sean leídos o manipulados por terceros.

Puertos y Sockets: Los puertos actúan como puntos lógicos para la transmisión de datos. HTTP usa el puerto 80, mientras que HTTPS utiliza el puerto 443. Los sockets combinan direcciones IP con números de puerto para crear canales de comunicación segura.

4. Importancia de la Seguridad en la Comunicación Web:

La práctica expone la necesidad crítica de utilizar HTTPS en lugar de HTTP para proteger la información sensible y asegurar las comunicaciones web. Al tratarse de un sitio sin cifrado, las credenciales de acceso se transmiten en **texto plano**, lo que representa una

vulnerabilidad crítica que puede ser explotada por atacantes para interceptar información sensible.

Utilizar HTTPS, que emplea cifrado SSL/TLS, proporciona una capa de seguridad adicional al cifrar la información antes de su transmisión. Este cifrado garantiza la integridad de los datos y autenticación de la identidad del servidor, impidiendo que los datos sean leídos por atacantes y protegiendo que la comunicación entre el cliente y el servidor sea segura.

En resumen, la práctica muestra la vulnerabilidad en el uso de HTTP para la transmisión de datos sensibles. La implementación de HTTPS es necesaria para asegurar la comunicación web y proteger la información de posibles amenazas y ataques.

7. Bibliografía:

Cisco Networking Academy. (n.d.). *Instalación de Wireshark*. Recuperado de

https://contenthub.netacad.com/courses/itn-dl/_common/3.7.9-lab---install-wireshark_es-XL.pdf

Universidad Tecnológica de El Salvador. (n.d.). *Instalando Wireshark*. Recuperado de

https://www.studocu.com/latam/document/universidad-tecnologica-de-el-salvador/redes-de-datos-i/instalando-wireshark/32689484

Wireshark. (n.d.). *Descarga Wireshark*. Recuperado de

https://www.wireshark.org/download.html

Wireshark. (n.d.). *Guía de instalación de Wireshark en Windows*. Recuperado de

https://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallWinInstall.html

McGraw-Hill. (n.d.). *Capítulo sobre redes de datos*. Recuperado de

https://www.mheducation.es/bcv/guide/capitulo/8448199766.pdf

CCNA desde cero. (n.d.). *¿Qué es TCP/IP?* Recuperado de

https://ccnadesdecero.es/que-es-tcp-ip/#3_Capas_del_modelo_TCPIP