



Universidad
Nacional
de Loja

FACULTAD DE ENERGÍA LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Ingeniería en Telecomunicaciones

LABORATORIO

Fundamentos de redes de datos

“Análisis del protocolo FTP”

Estudiantes: Luis Fernando Villalta Castillo, Santiago Alexander Roman Silva, Byron Alexander Herrera Martinez, Viviana Maricela Zambrano Romero.

Docente: Ing. John Tucker Mg.Sc.

Loja - Ecuador

2022

❖ INTRODUCCIÓN

El protocolo de transferencia de archivos (FTP) es uno de los protocolos más antiguos y ampliamente utilizados para la transferencia de archivos en redes de computadoras, el objetivo principal del FTP es permitir la transferencia eficiente de archivos entre un cliente y un servidor a través de una conexión de red. El cliente FTP se refiere a la aplicación utilizada por un usuario para acceder y transferir archivos, mientras que el servidor FTP es la máquina que aloja los archivos y responde a las solicitudes de transferencia.

Aunque el FTP ha sido ampliamente adoptado, presenta ciertas vulnerabilidades de seguridad, como la transmisión no cifrada de datos y la autenticación débil. Estas vulnerabilidades pueden exponer información sensible durante las transferencias de archivos y ser aprovechadas por atacantes.

❖ OBJETIVOS

En la siguiente práctica que se ha preparado se requiere conseguir:

O. Principal

Configurar y analizar una red para realizar transferencias de archivos utilizando un servidor FTP, mediante la herramienta Wireshark con el fin de obtener credenciales e información confidencial que circula en la red.

O. Específico:

- Crear el entorno de trabajo y diseñar un arquitectura de red
- Instalar y configurar los dispositivos para poder cumplir con los requerimientos del laboratorio
- Analizar los datos en la red desde la máquina atacante

❖ MATERIALES Y MÉTODOS

En la siguiente práctica se utilizará lo siguiente:

Materiales

- Switch para generar una red local.
- Software Wireshark (puede ser descargado de forma gratuita en <https://www.wireshark.org/>).
- Computadora como servidor FTP
- Computadoras como cliente FTP

Métodos

- Investigación

- Ejecución de herramientas

❖ DESARROLLO:

Una herramienta esencial para compartir archivos a través de redes informáticas es el Protocolo de Transferencia de Archivos (FTP). Su principal objetivo es hacer más eficaces las transferencias de archivos entre clientes y servidores a través de redes. FTP se ha utilizado ampliamente y ha sido esencial para el intercambio de archivos y la colaboración desde su introducción en la década de 1970.

La comunicación cliente-servidor es la base de la funcionalidad fundamental de FTP. El cliente FTP, que puede ser un programa informático o una aplicación, establece una conexión con el servidor FTP para realizar operaciones de transferencia de archivos. A continuación, los archivos se almacenan en el servidor FTP, que también responde a las peticiones del cliente.

A pesar de su uso generalizado, la transmisión de datos sin cifrar a través de FTP plantea peligros. Sin ningún tipo de cifrado, el material enviado a través de FTP es vulnerable a una probable interpretación y lectura ilegal. Esto implica que usuarios malintencionados o atacantes en la misma red podrían interceptar los datos[1]. La seguridad y la integridad de los archivos transferidos pueden verse comprometidas durante la transmisión de datos sin cifrar a través de FTP. Contraseñas, números de cuentas bancarias y otra información privada son ejemplos de datos sensibles que pueden ser fácilmente interceptados y explotados maliciosamente.

Una herramienta popular de captura y análisis de paquetes de red es Wireshark. Permite el análisis detallado del tráfico de red para reunir conocimientos importantes sobre los protocolos y las comunicaciones que tienen lugar en la red. Dado que permite examinar los paquetes de datos enviados y recibidos durante una sesión FTP, Wireshark es especialmente útil para examinar y comprender el funcionamiento del protocolo FTP.

Utilizando Wireshark, es posible capturar y examinar los paquetes de datos transmitidos a través del FTP, lo que brinda una visibilidad completa de las comunicaciones y ayuda a identificar cualquier posible vulnerabilidad o riesgo asociado con la transmisión de datos sin cifrar. Wireshark también permite filtrar y buscar información específica, lo que facilita el análisis y la identificación de posibles problemas de seguridad en las transferencias de archivos a través del FTP.

Configuración del entorno de laboratorio

Para llevar a cabo este laboratorio, se requiere realizar la configuración de las direcciones IP en cada una de las máquinas, como se muestra en la Figura 1. Esta configuración es esencial para garantizar que todas las máquinas se encuentren interconectadas en una red. Además, se utilizó un

switch para establecer la conexión entre dichas máquinas, asegurando así una comunicación eficiente y confiable.

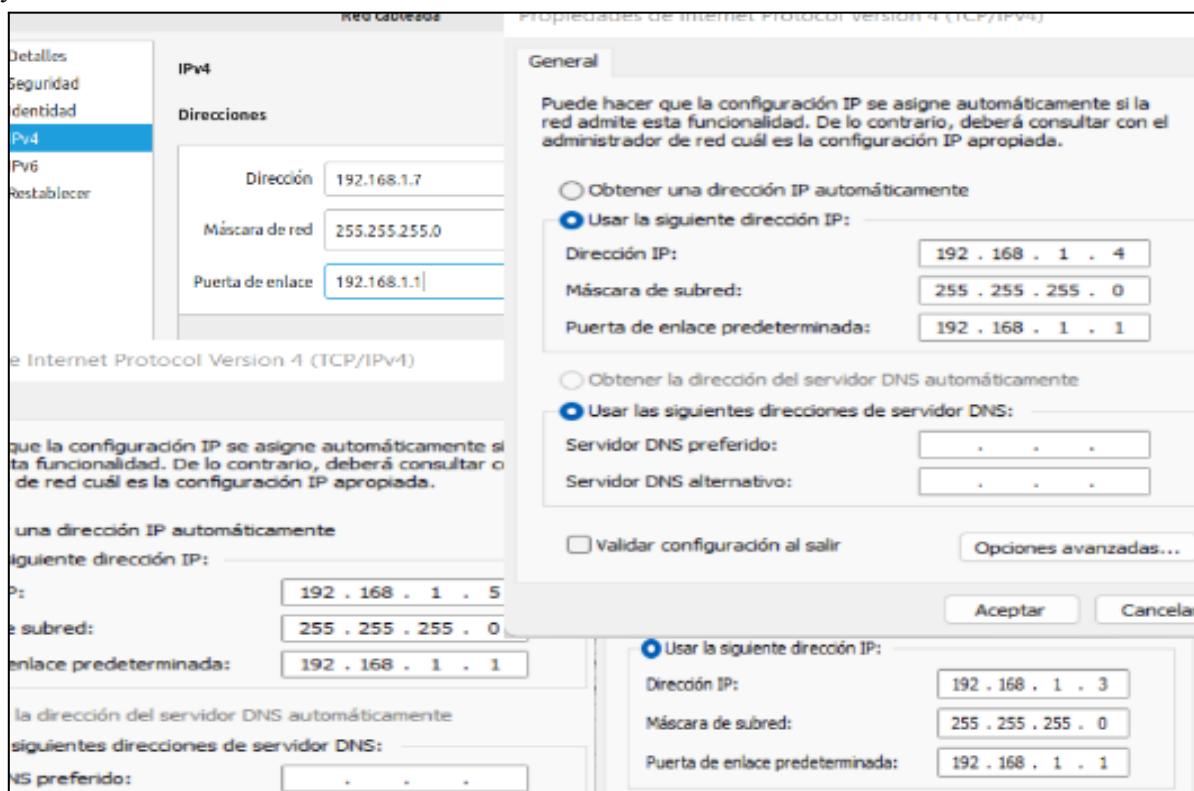


Figura 1. Configuración de dispositivos

Arquitectura de red

Para lograr establecer una conexión entre los 4 dispositivos, se hizo uso de la siguiente arquitectura Figura 2. Misma que permitió establecer una red estable para poder ejecutar el laboratorio Figura 3.

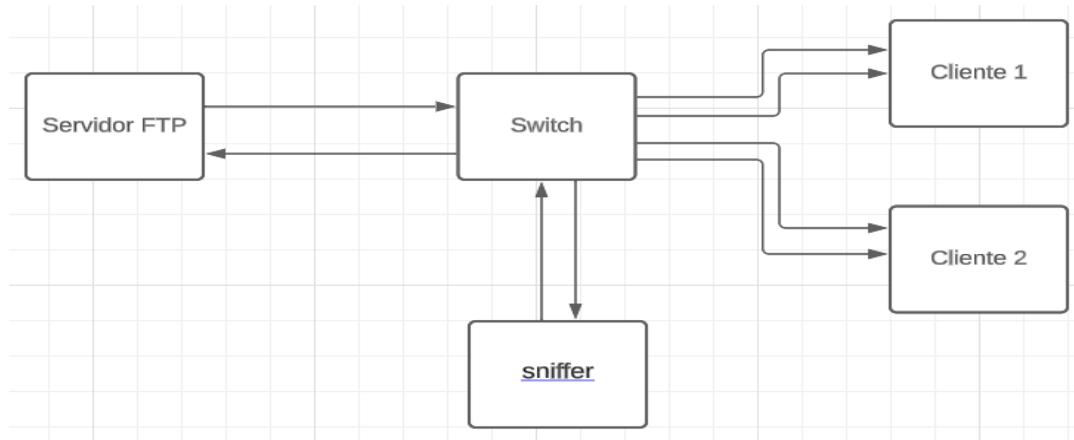


Figura 2. Arquitectura de la red



Figura 3. Comprobación de conexión en los equipos

Configuración del servidor FTP

- En la primera máquina con sistema operativo Windows, se configura un servidor FTP desde características de Windows como se ve en la Figura 4.

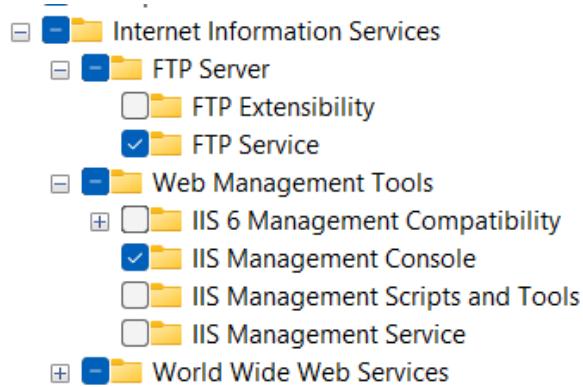


Figura 4. Activación de servicio de FTP

- Se establece un directorio como se ve Figura 5 para compartir archivos en el servidor FTP y configura las reglas para dar los permisos adecuados al usuario FTP como se puede observar en la Figura 6 .



Figura 5. Carpeta compartida FTP

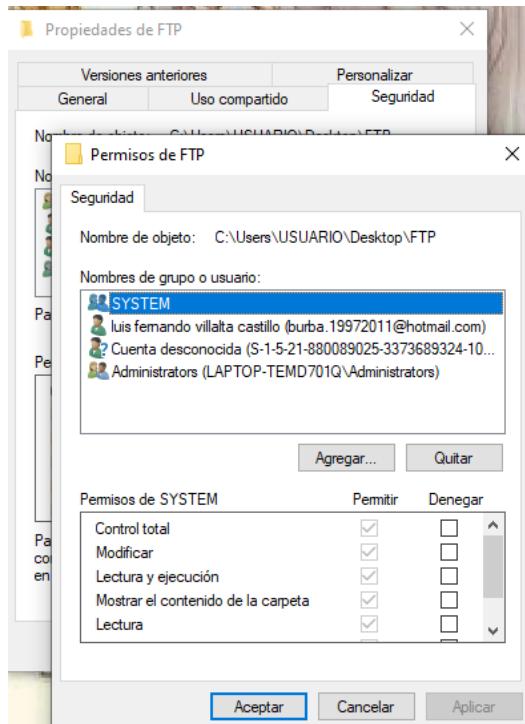


Figura 6. Configuración de permisos de la carpeta compartida FTP

Luego de activar las características de Windows debemos configurar un nuevo sitio FTP en el IIS, para ello seguimos los siguientes pasos:

- Crear el sitio FTP, en esta parte se le asigna un nombre al server y a continuación se selecciona la carpeta con la que va a trabajar el servidor, ver Figura 7.

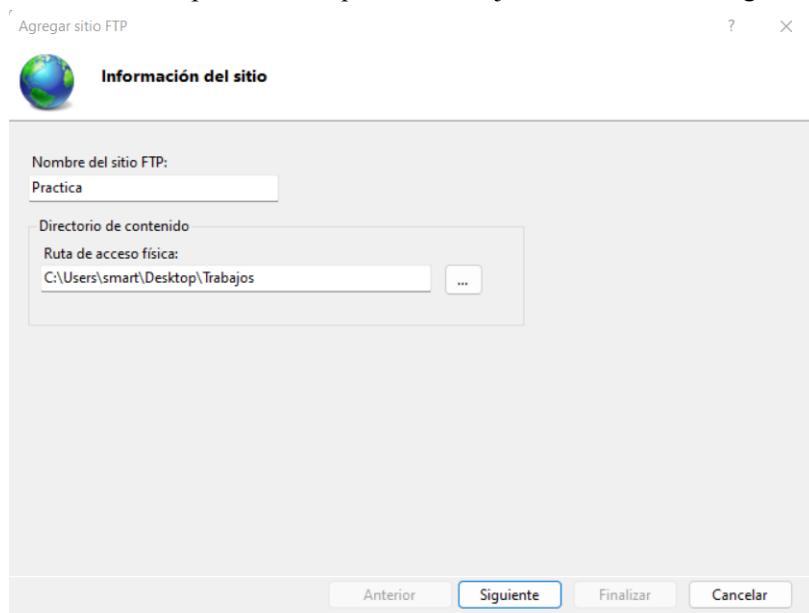


Figura 7. Creación de Server FTP

- Se establecen parámetros de autenticación, para el acceso al servidor, además de otorgar los permisos para el usuario asignado ver Figura 8.

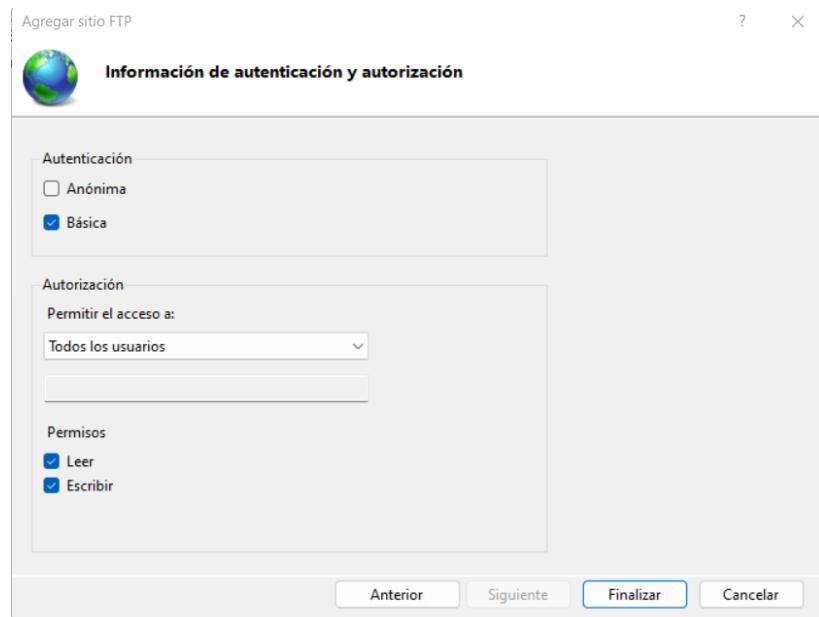


Figura 8. Configuración de autenticación y permisos

Configuración de la máquina atacante

- En la segunda máquina el atacante tendrá instalado previamente la herramienta de análisis de red llamada Wireshark, ver Figura 9.

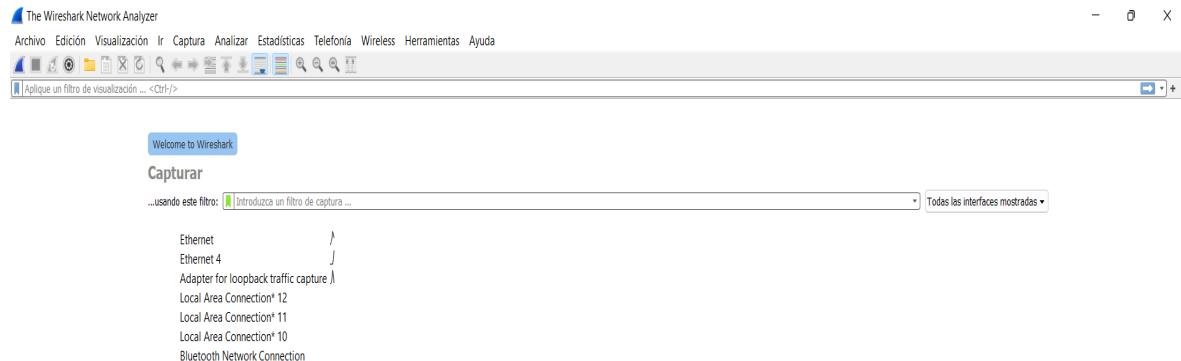


Figura 9. Configuración de la herramienta Wireshark

- Una vez detectada la interfaz de ethernet se procederá a ejecutar el análisis en el cual se capturaron todos los paquetes que circulan en la red, ver Figura 10.

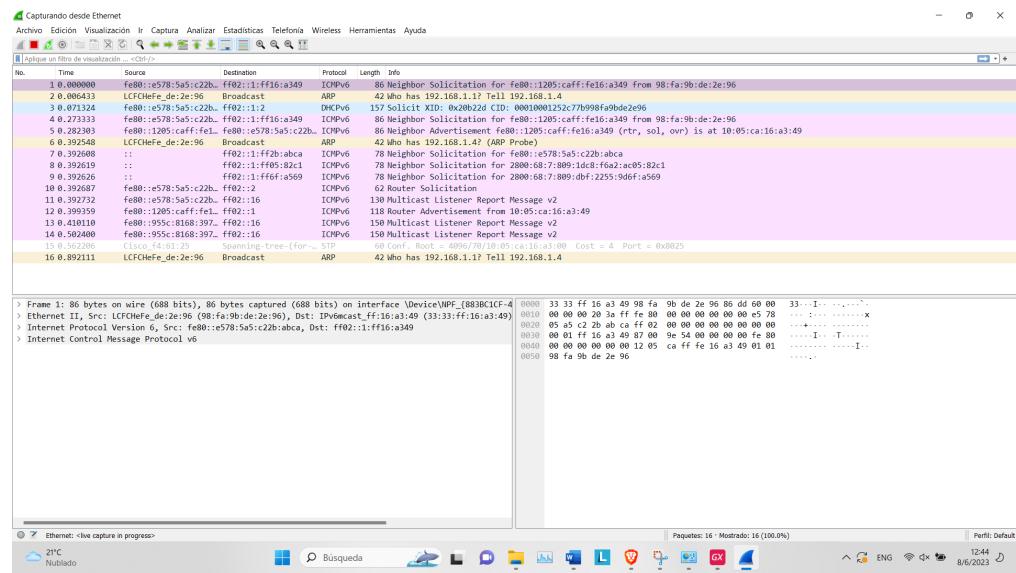


Figura 10. Ejecución de análisis de red

Conexión de las máquinas cliente

- En la tercera y cuarta máquina, configura un cliente FTP (puede ser el cliente de línea de comandos, ver figura 11 y 12 o un cliente gráfico, ver figura 13) para conectarse al servidor FTP.

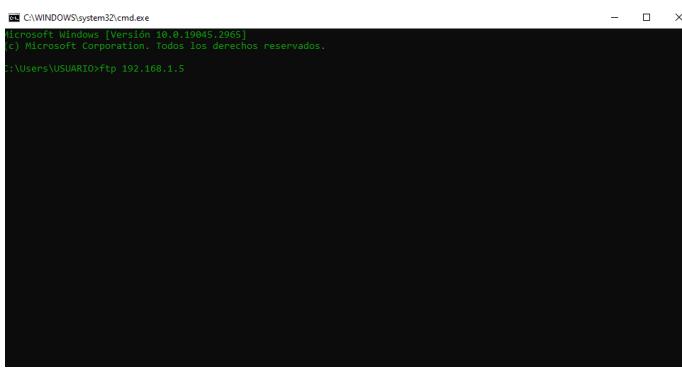


Figura 11. Configuración de máquina 3 como cliente FTP

- Utiliza las credenciales adecuadas para establecer la conexión con el servidor FTP desde ambas máquinas cliente.

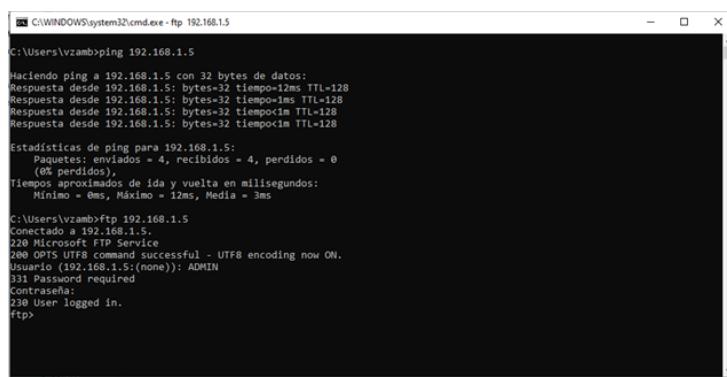


Figura 12. Configuración de máquina 4 utilizando credenciales para establecer conexión mediante consola

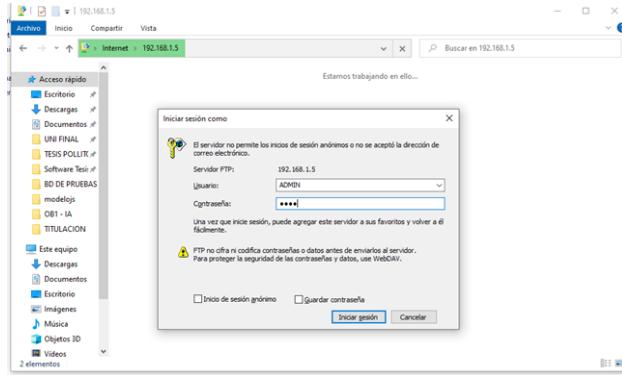


Figura 13. Configuración de máquina 3 utilizando credenciales para establecer conexión mediante cliente gráfico

5. Ejecución del ataque de sniffeo:

- Inicia la captura de paquetes en la máquina atacante utilizando la herramienta de sniffeo de red configurada anteriormente, ver figura 14.

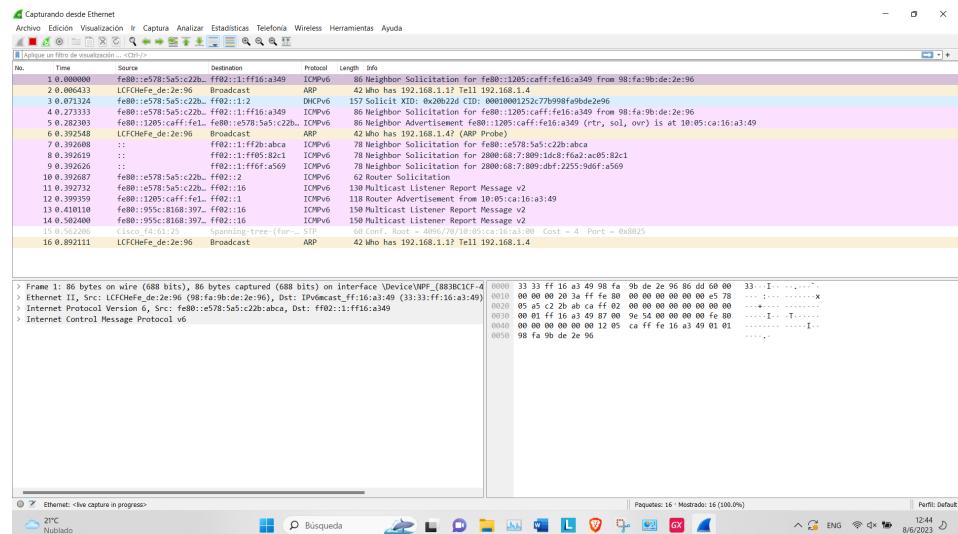


Figura 14. Herramienta Wireshark en funcionamiento

- Asegúrate de que la captura de paquetes incluya el tráfico de red entre las máquinas cliente y el servidor FTP, ver figura 15.

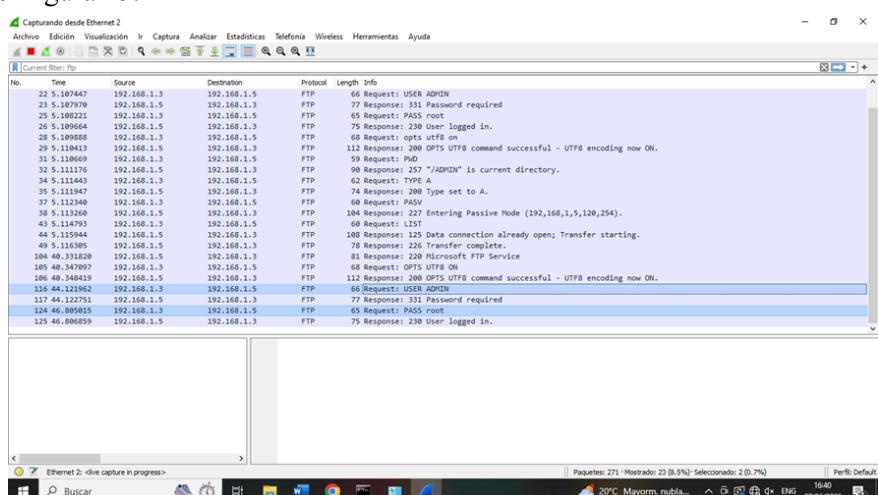


Figura 15. Captura de tráfico FTP

6. Transferencia de archivos y captura de datos:

- En las máquinas cliente, realiza transferencias de archivos entre las máquinas cliente y el servidor FTP, ver figura 16.

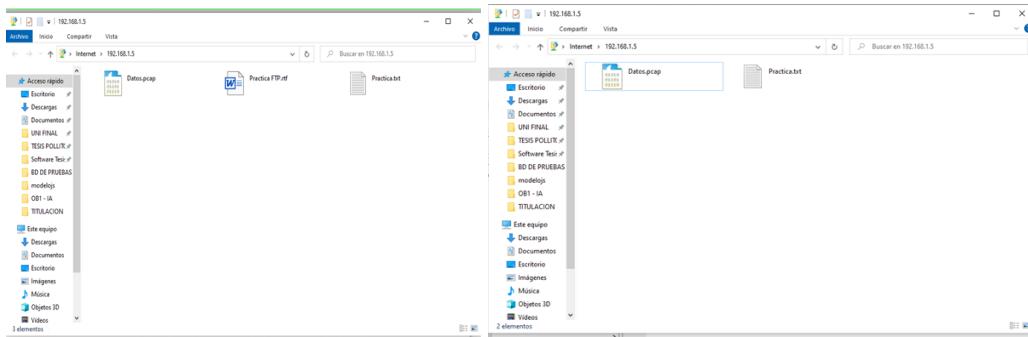


Figura 16. Transferencia de archivos entre cliente y servidor

- Durante las transferencias de archivos, la máquina atacante capturará los paquetes de red que contienen las credenciales e información plana, ver figura 17.

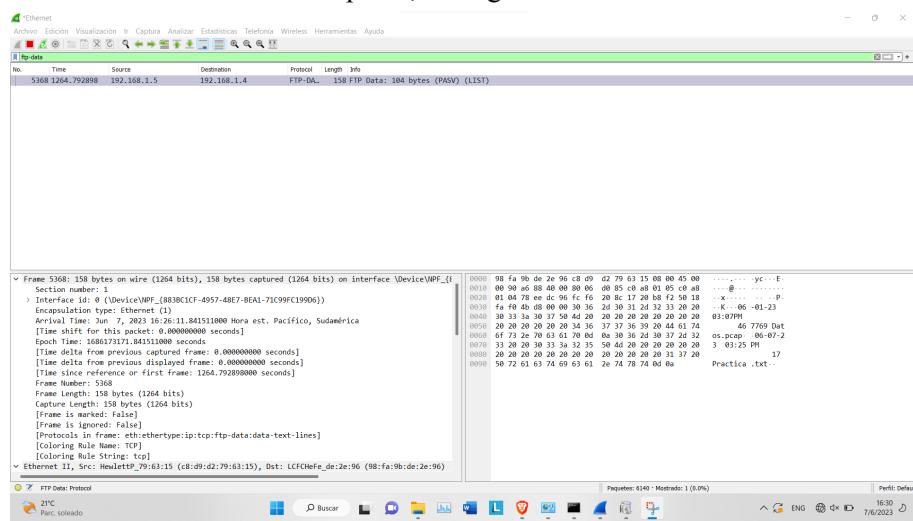


Figura 17. Herramienta Wireshark captura la transferencia de credenciales

7. Análisis de los datos capturados:

- Detén la captura de paquetes en la máquina atacante, ver imagen 18.

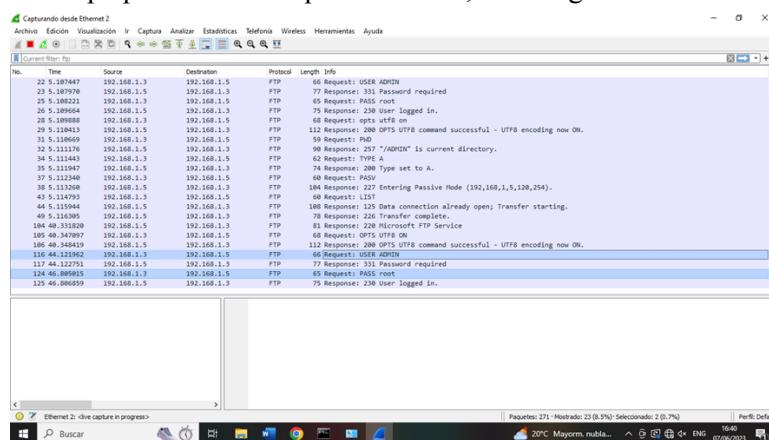


Figura 18. Herramienta Wireshark captura la transferencia FTP

- Utiliza la herramienta de sniffeo de red para analizar los datos capturados y extraer la información relevante, como las credenciales de inicio de sesión y otros datos sensibles, ver figura 19.

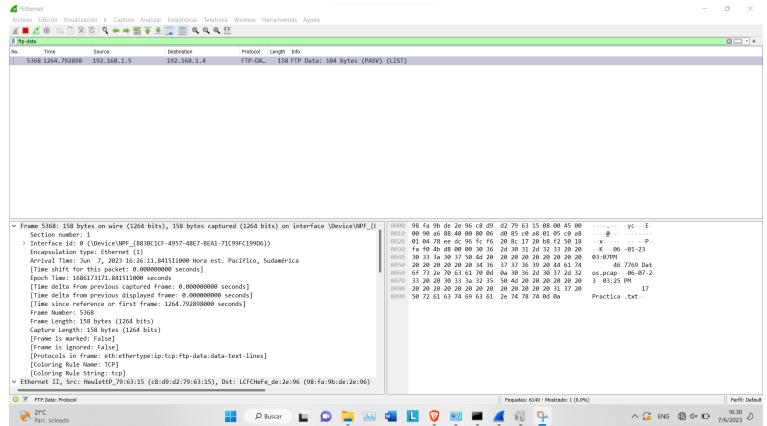


Figura 19. Extracción de información mediante herramienta wireshark

Es importante tener en cuenta que este laboratorio debe llevarse a cabo en un entorno controlado y legal, como una red local privada y con el consentimiento y autorización de los propietarios de los dispositivos involucrados.

❖ CONCLUSIONES

- La instalación de FTP, en la actualidad puede ser tediosa ya que requiere de una configuración minuciosa en los dispositivos, debido a que existen parches de seguridad que bloquean los puertos .
- El Protocolo de Transferencia de Archivos (FTP) es una herramienta esencial en el intercambio de archivos a través de redes de computadoras. Sin embargo, la transmisión de datos sin cifrar a través del FTP conlleva riesgos de seguridad. Es importante utilizar versiones seguras del FTP y herramientas como Wireshark para garantizar la confidencialidad e integridad de las transferencias de archivos y mitigar los riesgos asociados con la interceptación y lectura no autorizada de los datos.
- Hemos visto y comprobado como Windows 10 nos da las herramientas necesarias son útiles y simples, para crear nuestro servidor FTP y así compartir diversos elementos a través de la red con las prestaciones y seguridad que FTP nos da.

❖ BIBLIOGRAFÍA

- [1] “¿Cómo configurar el servidor FTP en Windows 10? – informaticamadridmayor”, *informaticamadridmayor.es*, 04-abr-2022. [En línea]. Disponible en: <https://informaticamadridmayor.es/admin/como-configurar-el-servidor-ftp-en-windows-10-informaticamadridmayor/>. [Consultado: 08-jun-2023].
- [2] “CÓMO ENTRENAR EL FTP CON ANÁLISIS DE DATOS”, *Planifica tus Pedaladas con Chema Arguedas*, 20-nov-2019. [En línea]. Disponible en: <https://chemaarguedas.com/2019/11/20/como-entrenar-el-ftp-con-analisis-de-datos/>. [Consultado: 08-jun-2023].