EXPLOTACION DE BADBLUE Y CAMUFLAJE DE ARCHIVOS DESDE LA MAQUINA VIRTUAL DE WINDOWS XP

KEVIN STIVEN JARAMILLO CORDOBA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

EXPLOTACION DE BADBLUE Y CAMUFLAJE DE ARCHIVOS DESDE LA MAQUINA VIRTUAL DE WINDOWS XP

KEVIN STIVEN JARAMILLO CORDOBA
Estudiantes, IX semestre

ING. RAFAEL SANDOVAL MORALES
Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

Contenido

Tema……**Pagina**

1. Introducción 9
2. Objetivos 9
2.1. Objetivo General 9
2.2. Objetivos Específicos 10
3. Justificación 11
4. Planteamiento de la Actividad 12
5. Desarrollo del tema 13
5.1. Capitulo 1 13
5.1.1 Instalación de VirtualBox en Windows XP 13
5.1.2 Configuración de la Carpeta Compartida en VirtualBox 15
5.1.3 Verificación de la Carpeta Compartida 16
5.1.4 Acceso a la Carpeta Compartida 17
5.1.5 Archivos en equipo local 18
5.1.6 Acceso a los Archivos desde la Máquina Virtual 19
5.1.7 Instalación de Camouflage en Windows XP 20
5.1.8 Interfaz Web de BadBlue en Ejecución 21
5.1.9 Archivos Preparados para Camuflaje 22
5.1.10 Propiedades del Conjunto de Archivos de Prueba 23
5.1.11 Intento fallido de camuflaje 24

5.1.12 Selección de Archivos para Camuflaje en JPG 25

5.1.13 Configuración del Archivo Portador JPG 26

5.1.14 Proceso de Camuflaje Completado 27

5.1.15 Contraseña del Archivo Camuflado 28

5.1.16 Propiedades del Archivo JPG Camuflado 29

5.1.17 Verificación de Archivos Ocultos JPG Camuflado 30

5.1.18 Selección de Archivos para Camuflaje en PDF 31

5.1.19 Configuración del Archivo PDF Portador 32

5.1.20 Proceso de Camuflaje en PDF Completado 33

5.1.21 Propiedades del Archivo PDF Camuflado 34

5.1.22 Verificación de Archivos en el PDF Camuflado 35

5.1.23 Selección de Archivos para Camuflaje en Word 36

5.1.24 Configuración del Archivo Word 37

5.1.25 Creación del Archivo Word Camuflado 38

5.1.26 Propiedades del Archivo Word Camuflado 40

5.1.27 Selección de Archivos para Camuflaje en Excel 41

5.1.28 Selección del Archivo Excel Portador 42

5.1.29 Configuración del Archivo Excel Portador 43

5.1.30 Creación del Archivo Excel Camuflado 44

5.1.31 Propiedades del Archivo Excel Camuflado 45

5.1.32 Verificación Final de Archivos Ocultos en el Excel Camuflado 46

5.2. Capitulo #2 47

5.2.1 Escaneo de Red para Identificar BadBlue 47

5.2.2 Búsqueda de Exploits para BadBlue 2.7 49

5.2.3 Obtención y Preparación del Exploit 50

5.2.4 Configuración del Exploit 4784.pl 51

5.2.5 Personalización del Exploit BadBlue 52

5.2.6 Preparación Final del Exploit BadBlue 53

5.2.7 Explotación Exitosa de BadBlue 55

5.2.8 Enumeración del Sistema Comprometido 56

5.2.9 Análisis de Procesos en el Sistema Comprometido 57

6. Problemas encontrados 59

7. Recomendaciones 60

8. Conclusión 61

9. Bibliográfica 62

Tabla de Ilustración

Ilustración 1. Asistente de instalación de VirtualBox 13

Ilustración 2. VirtualBox como dispositivo de almacenamiento 14

Ilustración 3. Creación de una carpeta compartida. 15

Ilustración 4. Lista de carpetas compartidas en la configuración de la maquina 16

Ilustración 5. Mostrando la unidad correspondiente a la carpeta compartida. 17

Ilustración 6. Carpeta Doc dentro de otra carpeta en el equipo local 18

Ilustración 7. Contenido de la carpeta compartida desde el Windows XP 19

Ilustración 8. Icono de Camouflage en el escritorio de Windows XP. 20

Ilustración 9. Página principal del servidor BadBlue 21

Ilustración 10. Conjunto de archivo listos para ser camuflados. 22

Ilustración 11. Características del conjunto de archivos a camuflar. 23

Ilustración 12. Mensaje de error de Camouflage 24

Ilustración 13. Interfaz de Camouflage mostrando los archivos seleccionados. 25

Ilustración 14. Selección del archivo JPG que servirá como portador 26

Ilustración 15. Mensaje de finalización exitosa del proceso de camuflaje. 27

Ilustración 16. Configuración de contraseña para el archivo camuflado. 28

Ilustración 17. Propiedades del archivo JPG después del camuflaje. 29

Ilustración 18. Interfaz mostrando la lista de archivos extraíbles del JPG camuflado. 30

Ilustración 19. Interfaz mostrando archivos para ser ocultados dentro de un PDF. 31

Ilustración 20. Selección del archivo PDF como archivo para el camuflaje. 32

Ilustración 21. Archivo PDF camuflado resultante 33

Ilustración 22. propiedades del archivo PDF después del proceso de camuflaje. 34

Ilustración 23. Interfaz mostrando la lista de archivos extraíbles del PDF camuflado..... 35

Ilustración 24. Interfaz archivos para ser ocultados dentro de un documento Word..... 36

Ilustración 25. Selección del archivo para el camuflaje en Word..... 37

Ilustración 26. Configuración final para generar el archivo Word camuflado 38

Ilustración 27. propiedades del archivo WORD después del proceso de camuflaje. 39

Ilustración 28. propiedades del archivo Word después del proceso de camuflaje..... 40

Ilustración 29. Interfaz de archivos para ser ocultados dentro de una Excel. 41

Ilustración 30. selección del archivo como archivo realizar el camuflaje. 42

Ilustración 31. Confirmación de la selección como archivo para camuflaje 43

Ilustración 32. Configuración final para generar el archivo Excel camuflado. 44

Ilustración 33. Propiedades del archivo Excel después del proceso de camuflaje. 45

Ilustración 34. Interfaz mostrando los archivos extraíbles del Excel camuflada..... 46

Ilustración 35. Resultado del escaneo Nmap mostrando los servicios activos en la red .. 47

Ilustración 36. Escaneo Nmap mostrando los servicios activos en la red 192.128.100.7 48

Ilustración 37. Verificación del servidor BadBlue 49

Ilustración 38. Localización y copia del exploit 4784.pl..... 50

Ilustración 39. Edición del script de explotación BadBlue 2.72..... 51

Ilustración 40. Modificación del script de explotación..... 52

Ilustración 41. asignación de permisos de ejecución al script de explotación. 53

Ilustración 42. Verificación de permisos de ejecución al script de explotación. 54

Ilustración 43. Explotación de BadBlue y Obtención de Shell Remoto 55

Ilustración 44. Comandos de enumeración ejecutados en el sistema Windows XP 56

Ilustración 45. Lista de procesos en ejecución mediante tasklist..... 57

Ilustración 46. Salida de la configuración del sistema Windows XP víctima. 58

1. Introducción

El presente informe describe la explotación de la vulnerabilidad del servidor BadBlue y el uso de técnicas de camuflaje de archivos, llevadas a cabo desde una máquina virtual con Windows XP. El propósito fundamental fue comprender, mediante una simulación práctica, cómo los atacantes pueden aprovechar fallos en servicios desactualizados para comprometer un sistema, y de qué forma es posible ocultar información dentro de archivos cotidianos como imágenes y documentos.

2. Objetivos

2.1. Objetivo General

Explotar la vulnerabilidad del servidor BadBlue y aplicar técnicas de camuflaje de archivos desde una máquina virtual con Windows XP

2.2.Objetivos Específicos

- Identificar la vulnerabilidad del servidor BadBlue y configurar el entorno de explotación.
- Ocultar archivos en diferentes tipos de documentos usando herramientas de camuflaje.
- Registrar los pasos seguidos y los resultados obtenidos durante la práctica.

3. Justificación

La práctica realizada es relevante porque muestra la facilidad con que se pueden explotar servicios obsoletos y camuflar archivos. Esto refuerza la importancia de la actualización constante de sistemas y la capacitación en temas de seguridad

4. Planteamiento de la Actividad

Determinar la capacidad máxima de archivos que pueden ocultarse en formatos JPG, PDF, Word y Excel, evaluando límites de tamaño y cantidad. Paralelamente, ejecutar la explotación del servidor BadBlue 2.7 mediante payloads específicos para obtener acceso remoto, documentando el proceso completo de compromiso del sistema.

5. Desarrollo del tema

5.1.Capítulo #1

5.1.1 Instalación de VirtualBox en Windows XP

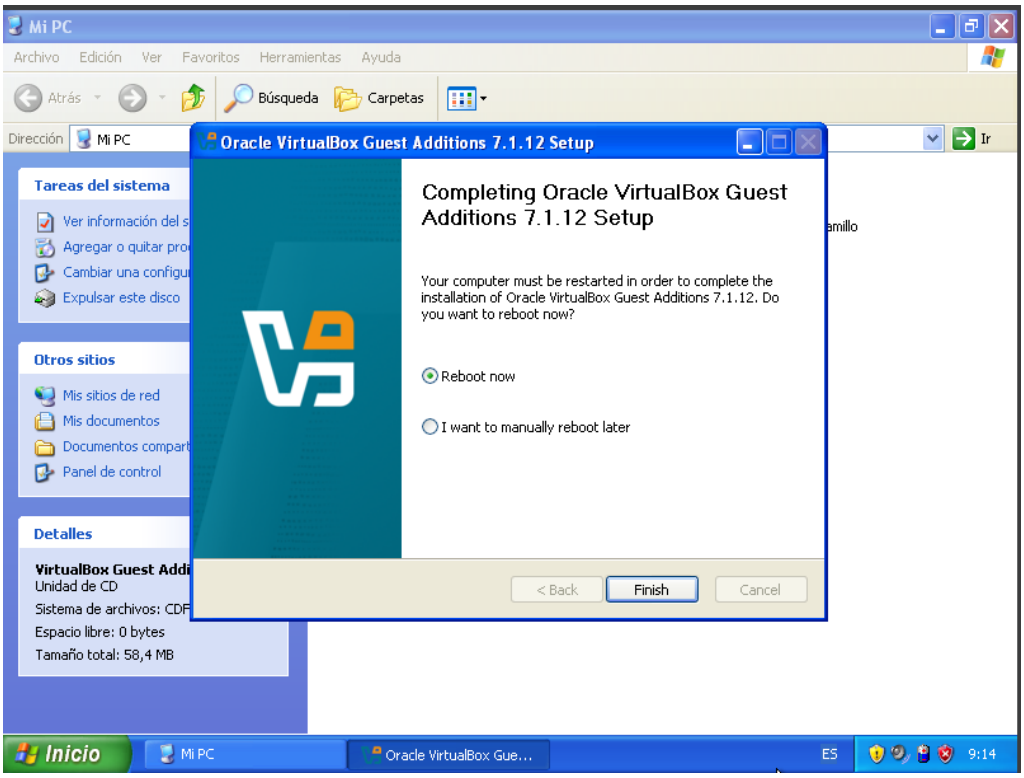

Ilustración 1. Asistente de instalación de VirtualBox

El primer paso para la práctica es preparar el entorno de la máquina virtual Windows XP instalando las VirtualBox, ya que habilita la funcionalidad de "Carpetas Compartidas", la cual permitirá transferir archivos de forma sencilla entre la máquina loca y la máquina virtual Windows XP para realizar las pruebas de camuflaje en BadBlue.

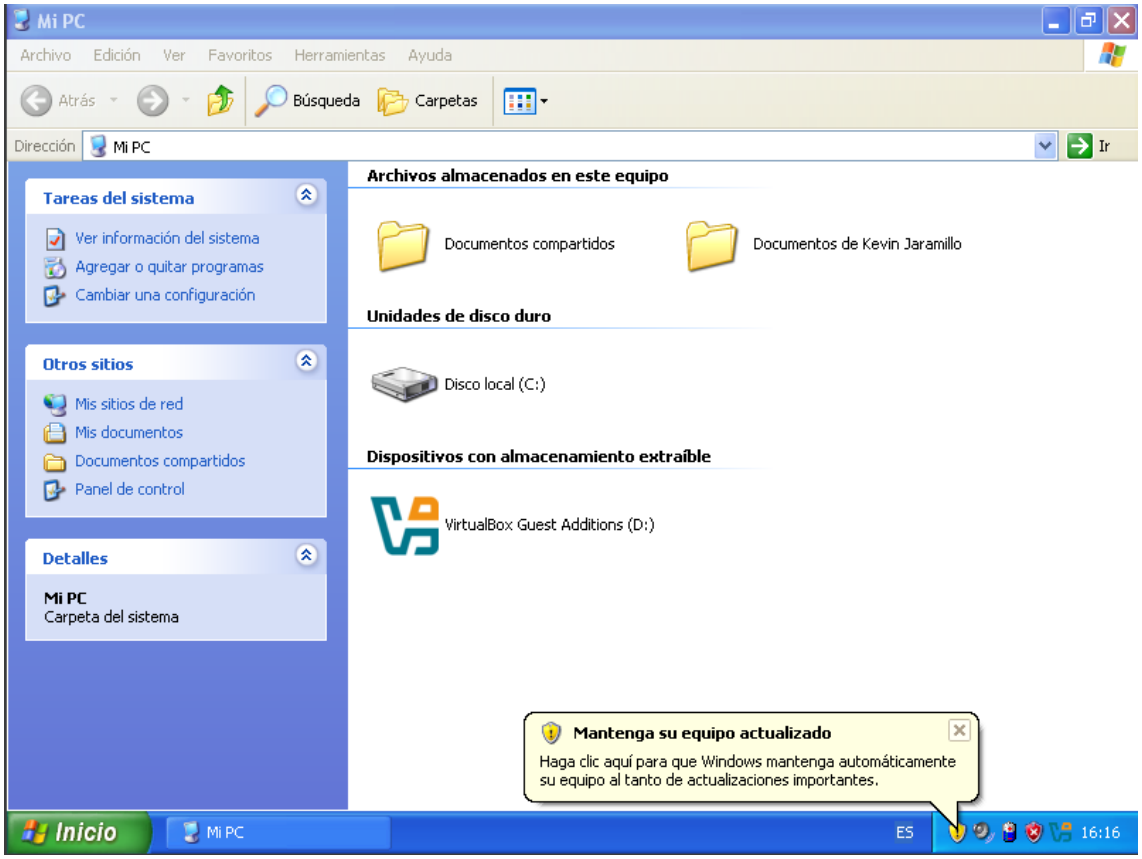

Ilustración 2. VirtualBox como dispositivo de almacenamiento

Una vez completada la instalación y el reinicio, se verifica el entorno de Windows XP. Es importante destacar la presencia de la unidad VirtualBox (D:), que corresponde al disco de instalación montado por VirtualBox.

5.1.2 Configuración de la Carpeta Compartida en VirtualBox

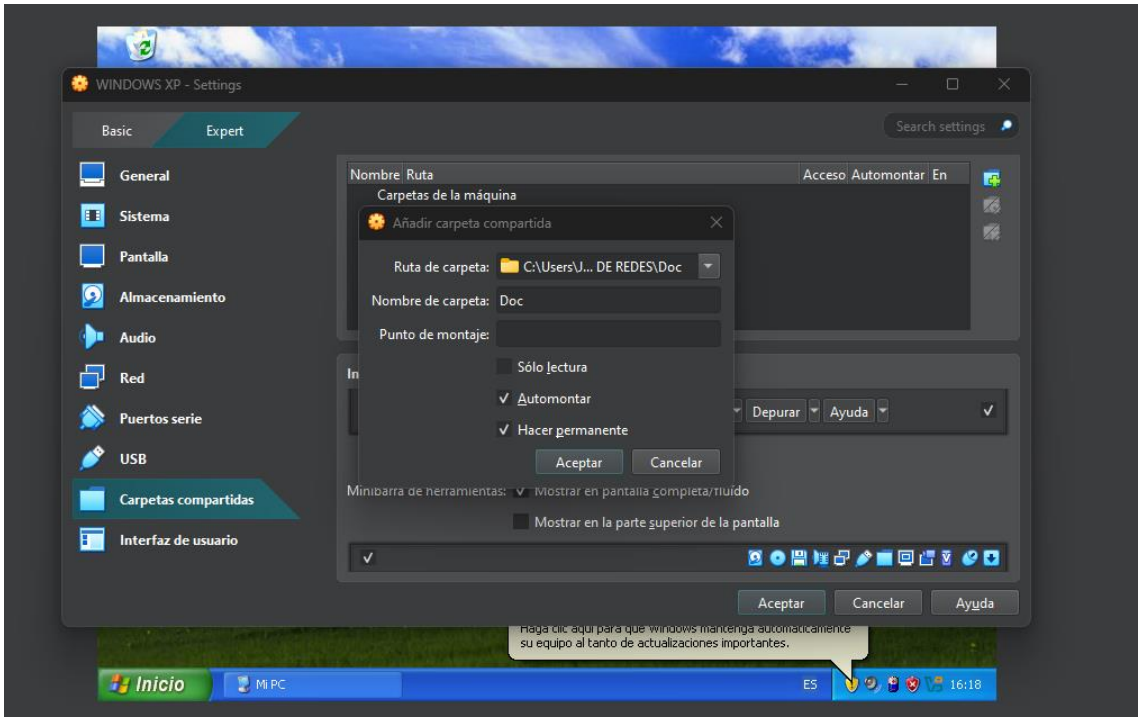

Ilustración 3. Creación de una carpeta compartida.

Para transferir los archivos desde el equipo host ("máquina loca") a la máquina virtual Windows XP, se configura una Carpeta Compartida.

Configuración de la VM donde se define una nueva carpeta compartida:

- **Ruta de carpeta:** C:\Users\...AUDITORIA DE REDES\Doc (Ruta del equipo local).
- **Nombre de carpeta:** Doc (Nombre con el que se identificará en la máquina virtual).
- **Las opciones** Automontar **y** Hacer permanente deben estar activadas, para que la carpeta esté disponible automáticamente cada vez que se inicie la máquina virtual.

5.1.3 Verificación de la Carpeta Compartida

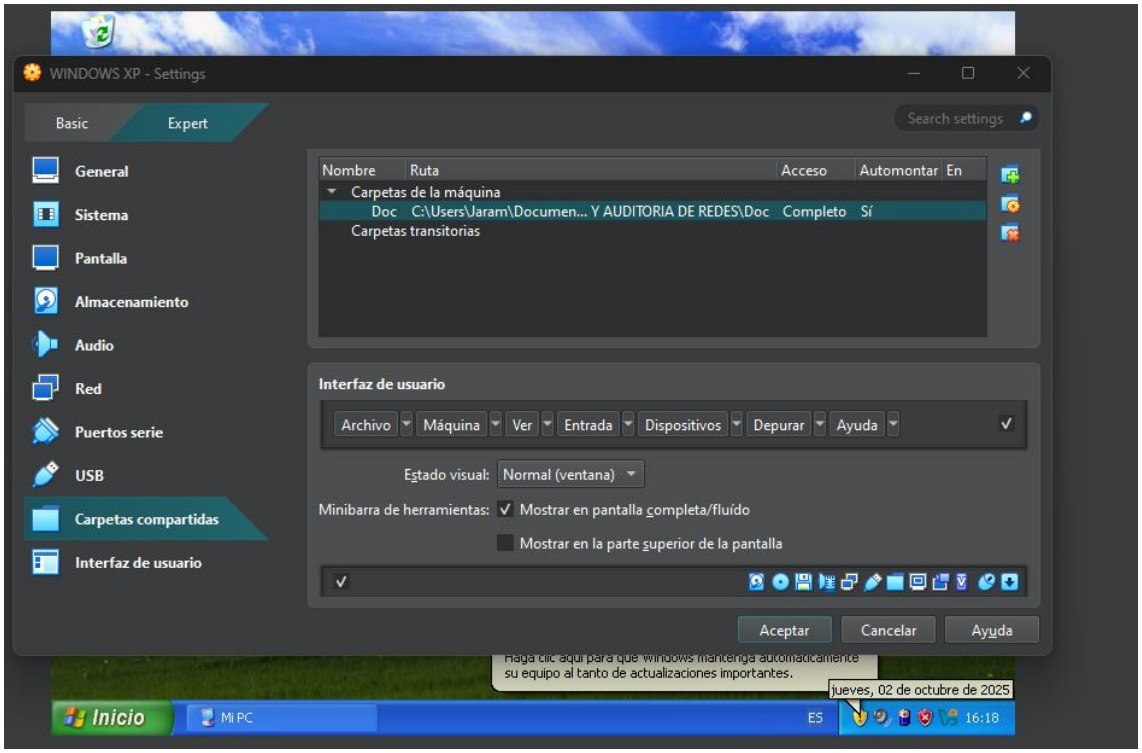

Ilustración 4. Lista de carpetas compartidas en la configuración de la maquina

Esta captura confirma que la carpeta compartida "Doc" se ha añadido correctamente a la configuración de la máquina virtual.

5.1.4 Acceso a la Carpeta Compartida

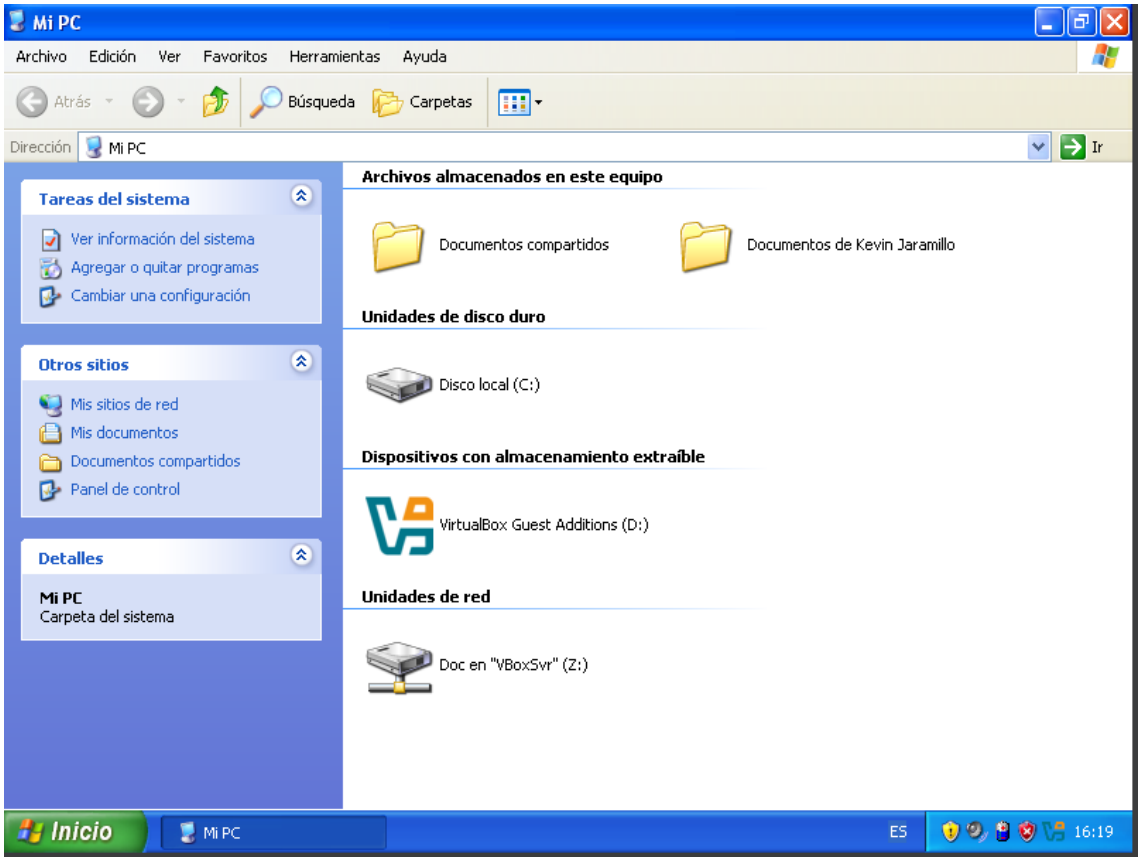

Ilustración 5. Mostrando la unidad correspondiente a la carpeta compartida.

Se observa la nueva Unidad como Doc en "VBoxSvr" (Z:). Esta unidad Z: es el punto de montaje de la carpeta compartida Doc configurada en los pasos anteriores.

5.1.5 Archivos en equipo local

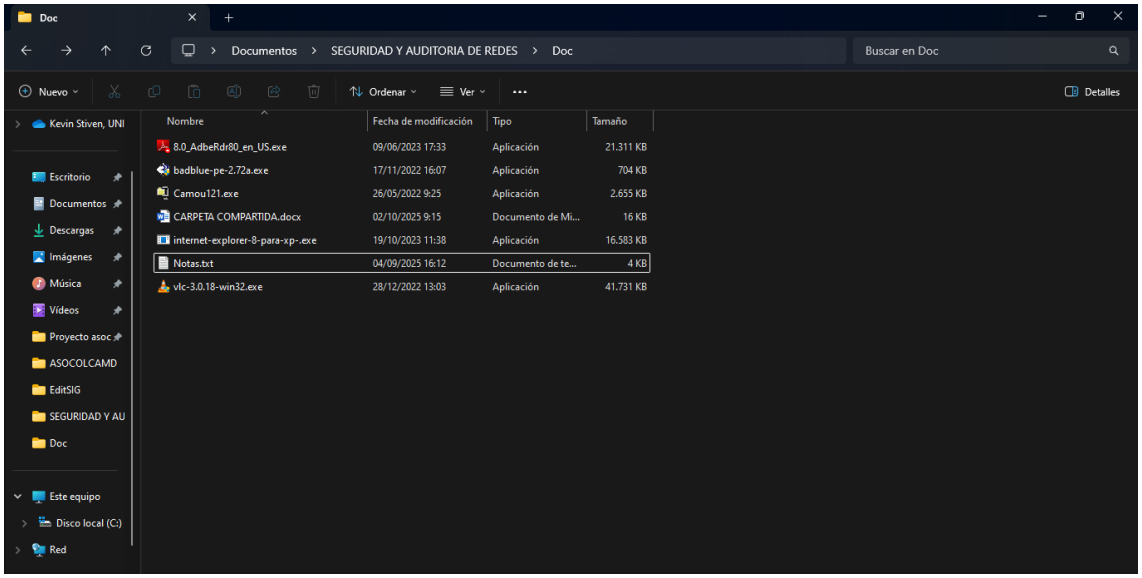

Ilustración 6. Carpeta Doc dentro de otra carpeta en el equipo local

Esta captura muestra el directorio de trabajo en la máquina loca donde se están unidos todas las herramientas y archivos necesarios para la práctica.

5.1.6 Acceso a los Archivos desde la Máquina Virtual

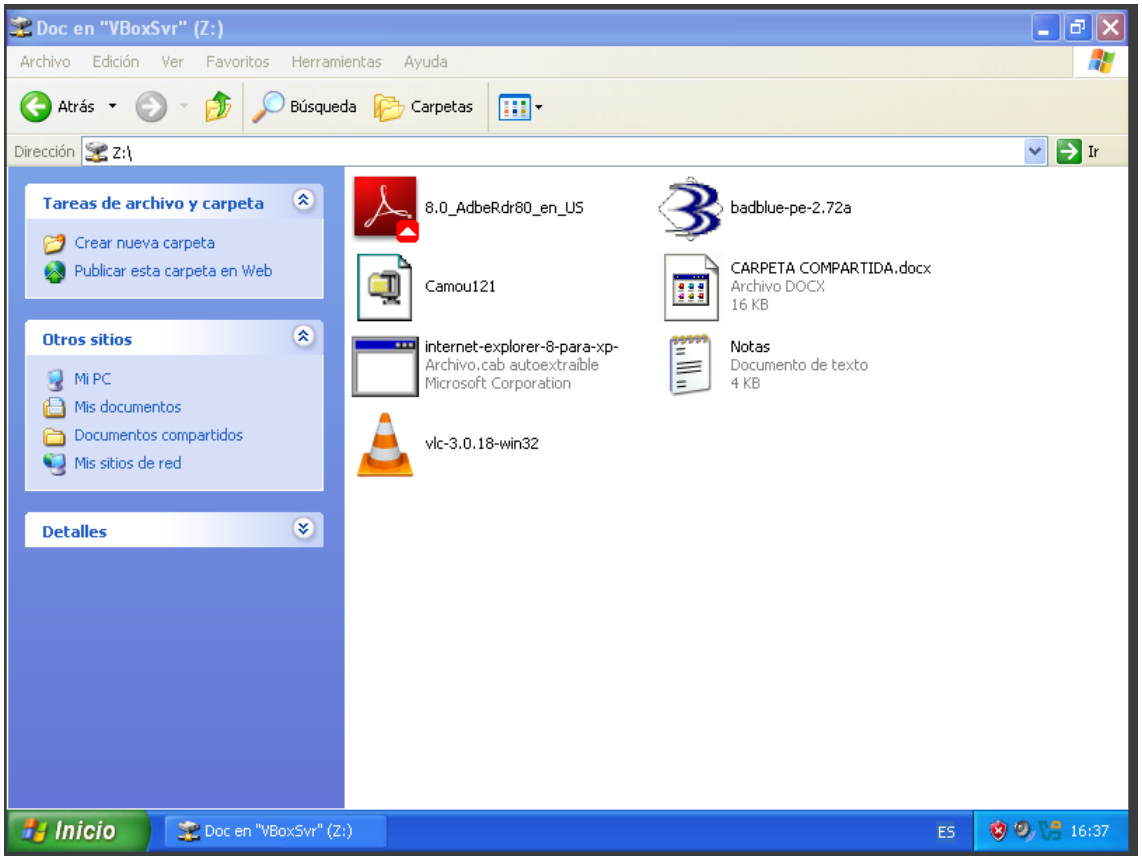

Ilustración 7. Contenido de la carpeta compartida desde el Windows XP

Desde dentro de la máquina virtual Windows XP, se accede a la unidad de red Z:, que corresponde a la carpeta compartida configurada.

5.1.7 Instalación de Camouflage en Windows XP

Ilustración 8. Icono de Camouflage en el escritorio de Windows XP.

Camou121.exe (la herramienta de camuflaje) evidenciada en el escritorio de Windows XP como ejecutable

5.1.8 Interfaz Web de BadBlue en Ejecución

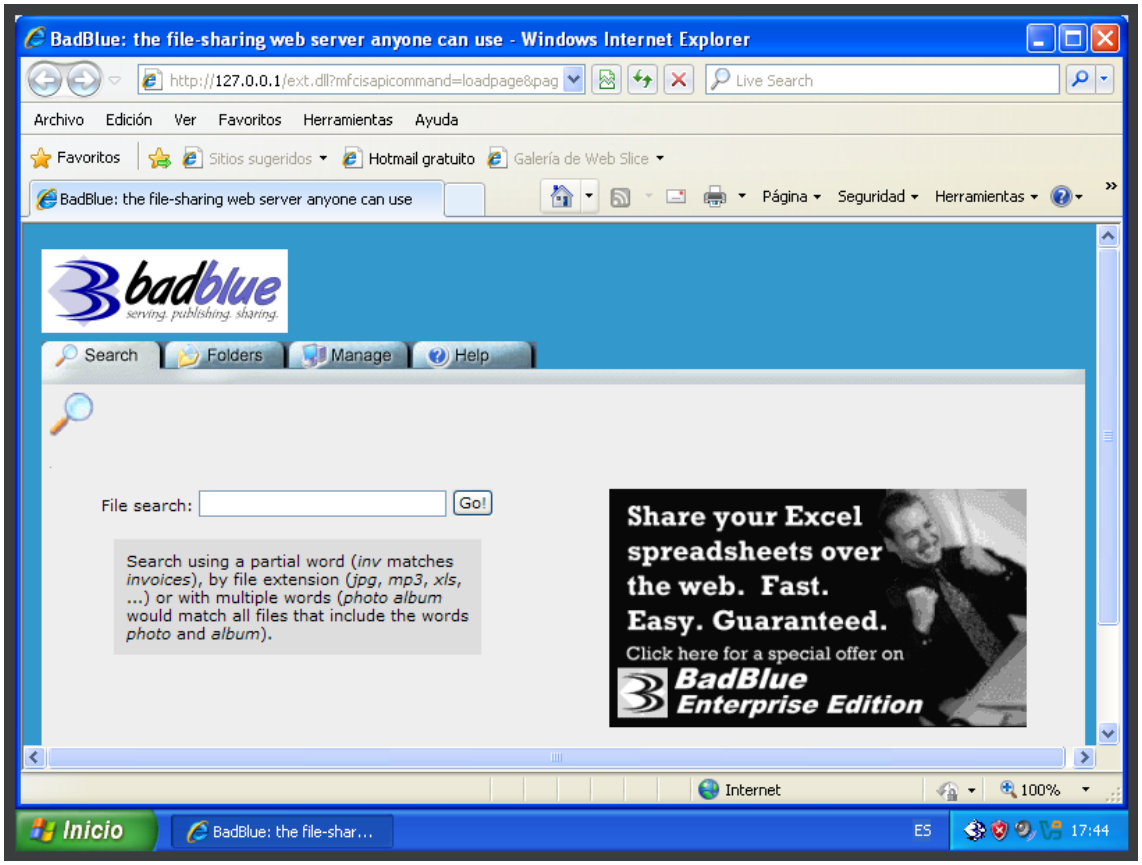

Ilustración 9. Página principal del servidor BadBlue

Esta captura confirma que el servidor web vulnerable BadBlue se está ejecutando correctamente en la máquina virtual Windows XP.

5.1.9 Archivos Preparados para Camuflaje

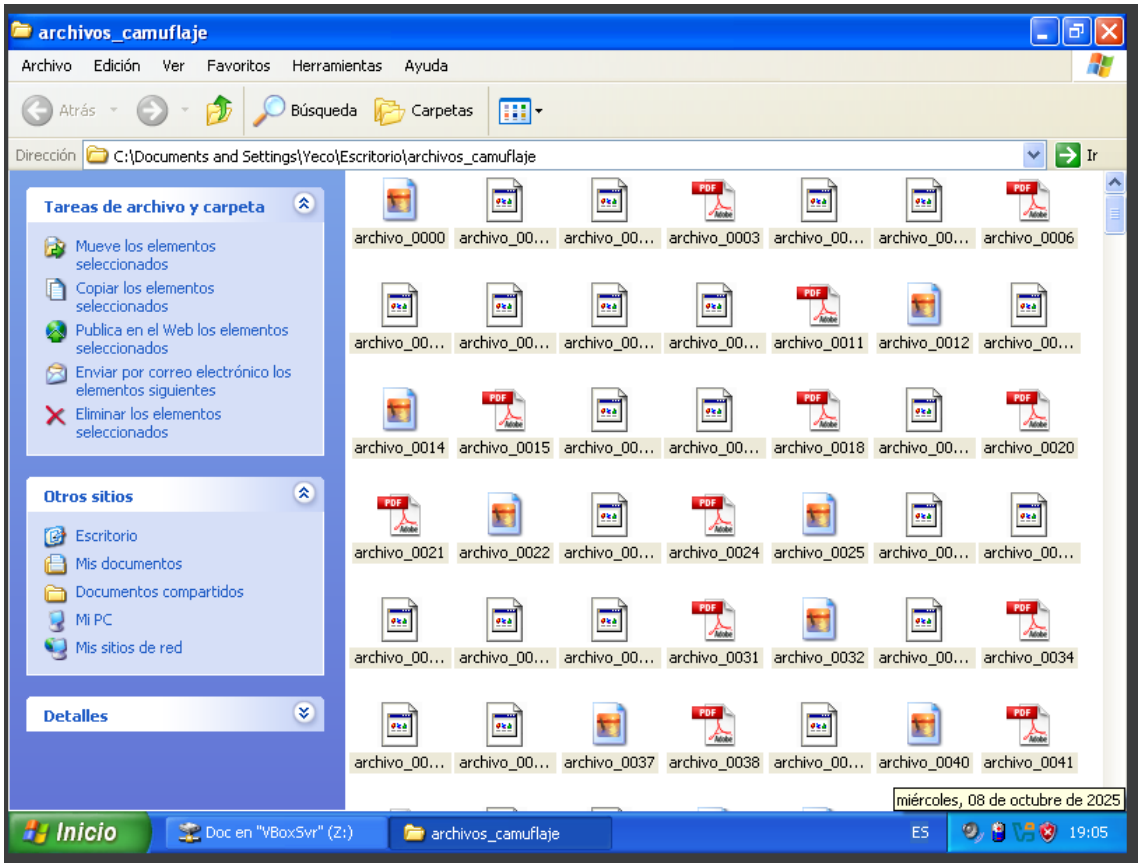

Ilustración 10. Conjunto de archivo listos para ser camuflados.

Esta captura muestra el conjunto de archivos que se utilizarán para probar las capacidades de camuflaje, que serán camuflados dentro de archivos como JPG, DOC, PDF, XLS utilizando la herramienta Camouflage.

5.1.10 Propiedades del Conjunto de Archivos de Prueba

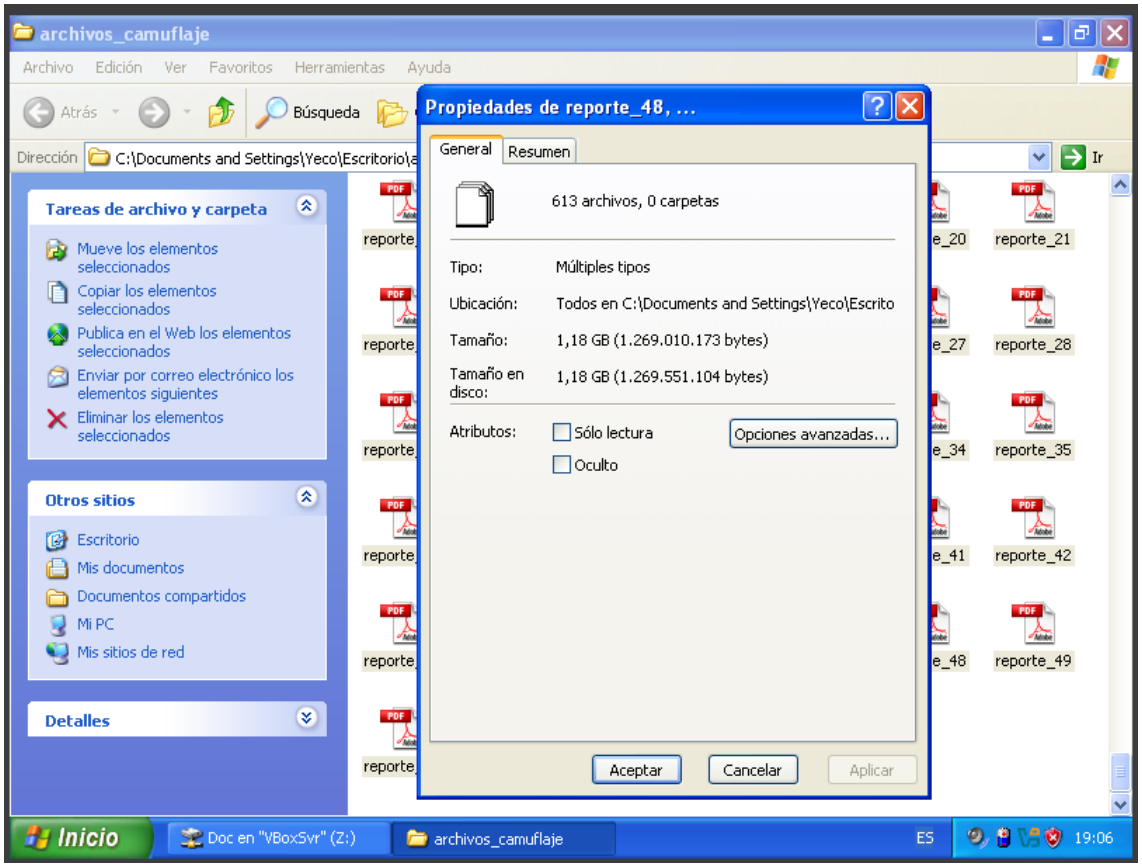

Ilustración 11. Características del conjunto de archivos a camuflar.

Antes de proceder con el camuflaje, se analizan las propiedades del conjunto de archivos de prueba.

- **Cantidad:** 613 archivos individuales.
- **Tamaño total:** 1.18 GB

5.1.11 Intento fallido de camuflaje

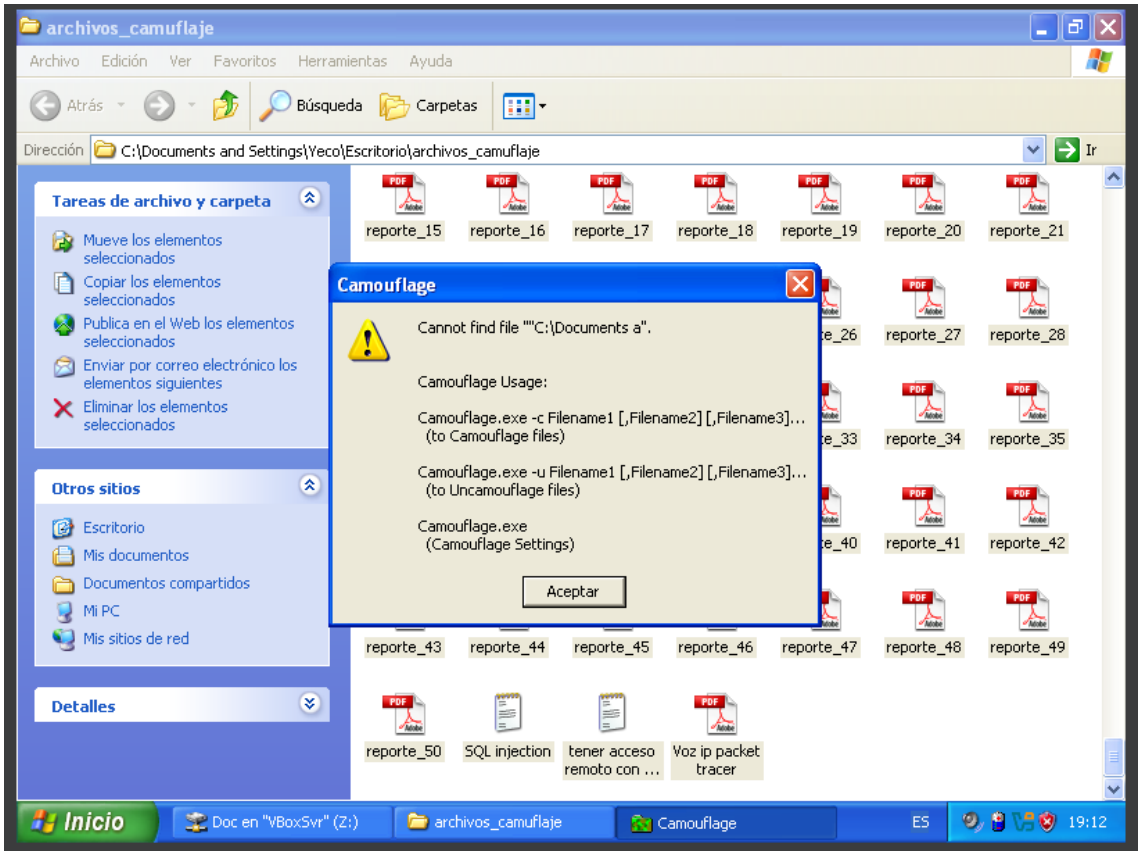

Ilustración 12. Mensaje de error de Camouflage

Al ejecutar la herramienta Camouflage sobre el conjunto de archivos de prueba, el programa devuelve un error. Indica que la herramienta no puede manejar el volumen total de archivos seleccionados.

La herramienta Camouflage tiene un límite en la cantidad o tamaño total de archivos que puede procesar en una sola operación, el cual es inferior a 1.18 GB

5.1.12 Selección de Archivos para Camuflaje en JPG

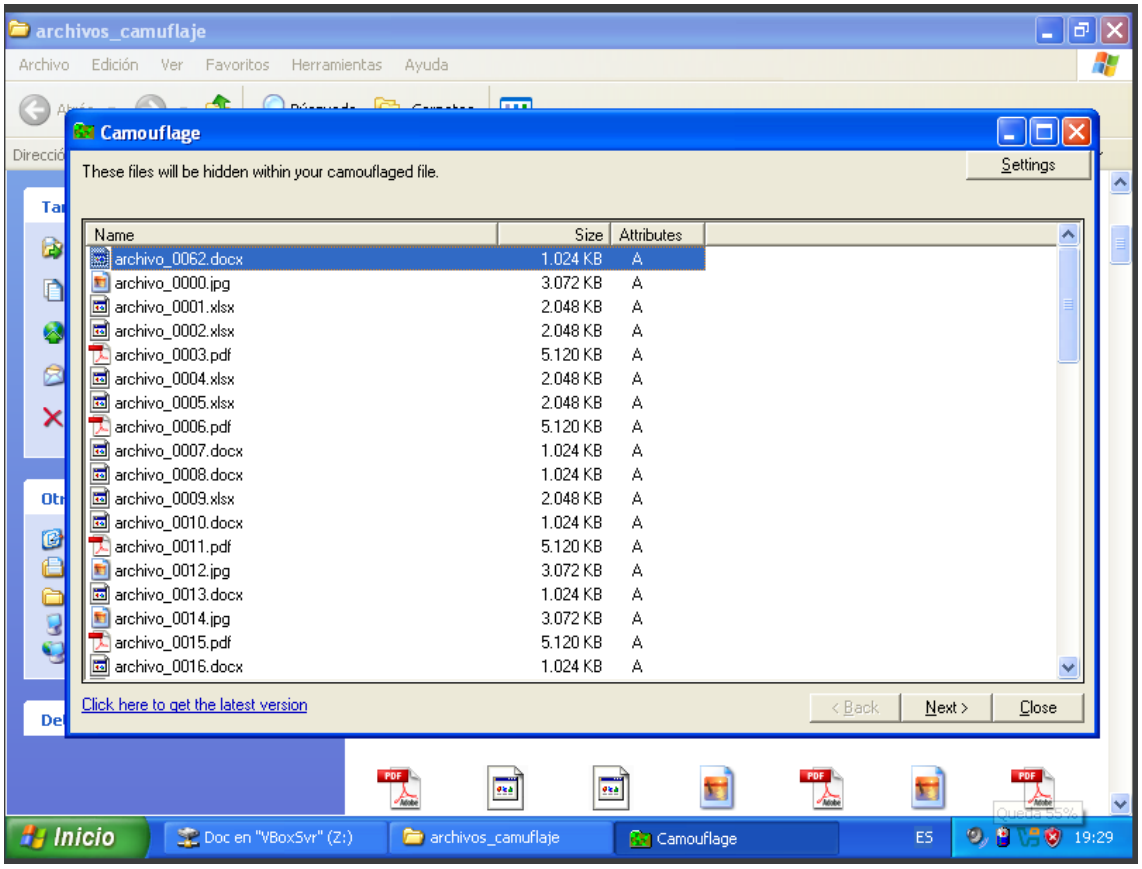

Ilustración 13. Interfaz de Camouflage mostrando los archivos seleccionados.

Tras el intento fallido con un volumen grande de datos, se procede con un conjunto más manejable de archivos. Esta captura muestra la interfaz de Camouflage donde se han seleccionado archivos de diferentes tipos para ser camuflados.

5.1.13 Configuración del Archivo Portador JPG

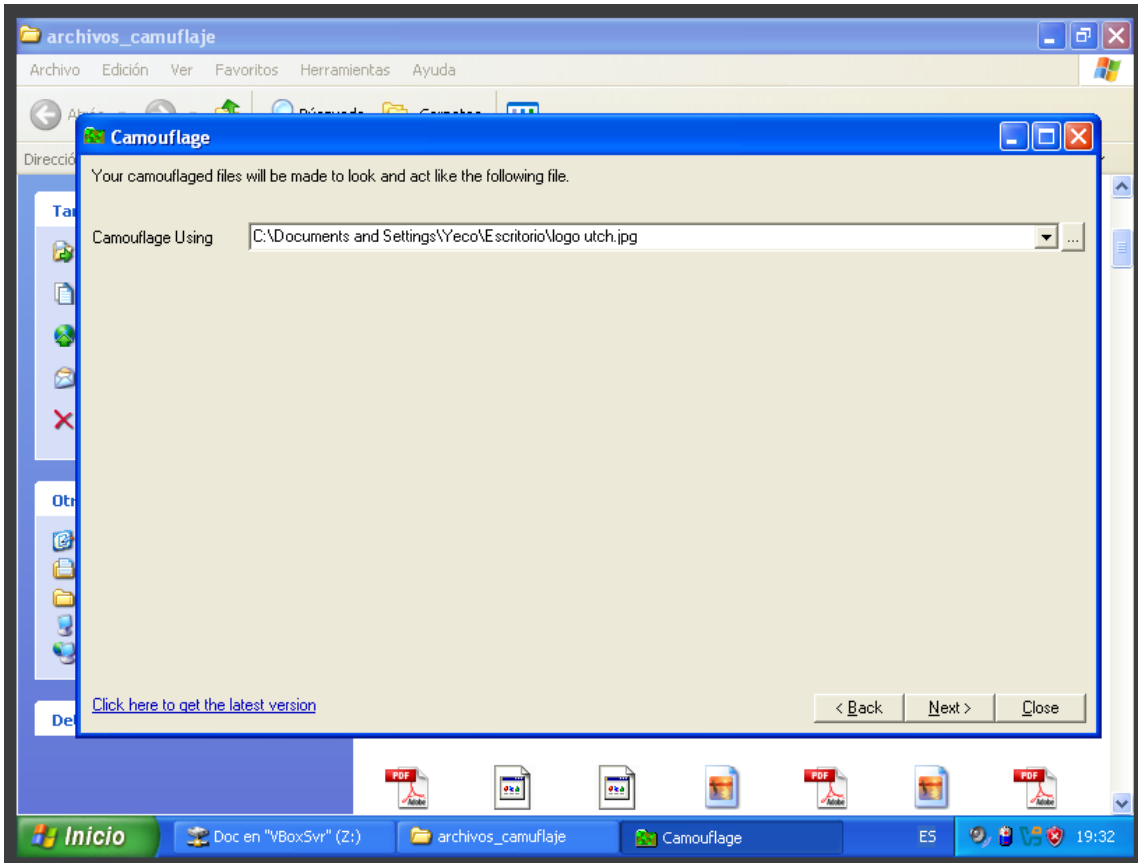

Ilustración 14. Selección del archivo JPG que servirá como portador

En este paso crucial, se configura el camuflaje seleccionando el archivo que actuará como portador.

5.1.14 Proceso de Camuflaje Completado

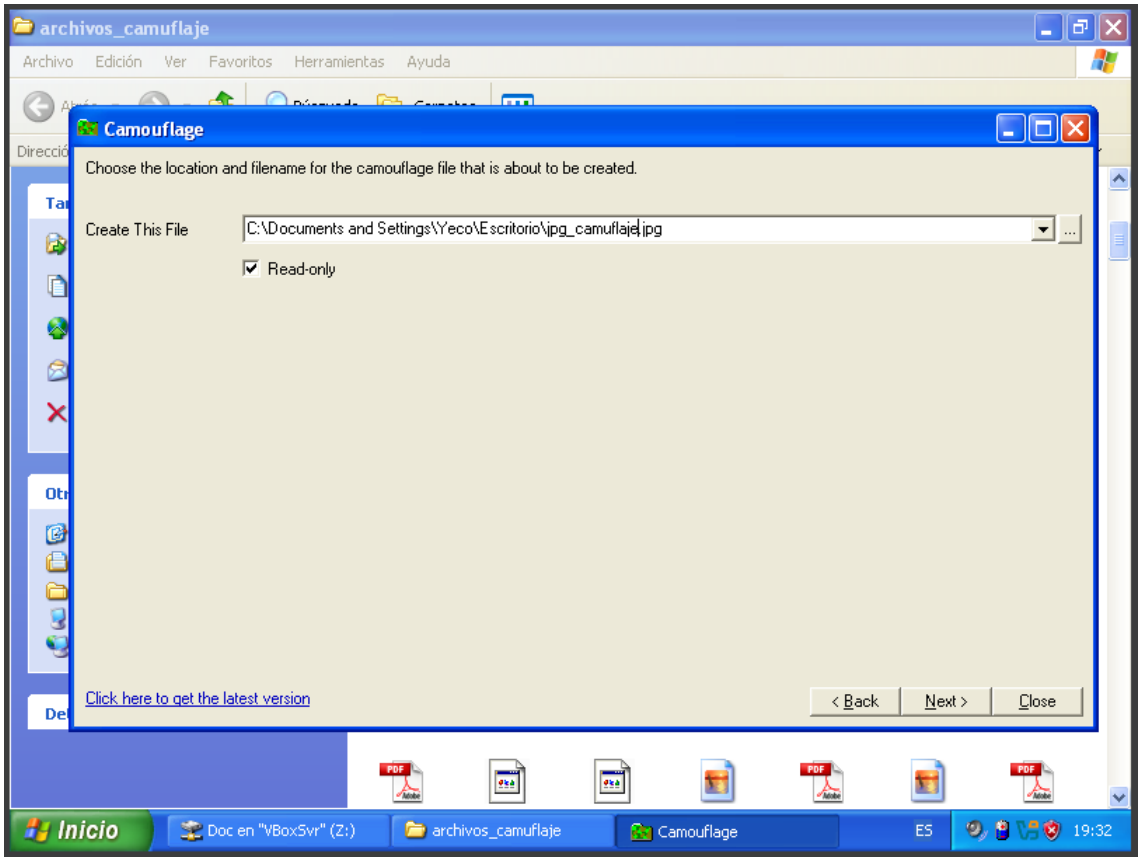

Ilustración 15. Mensaje de finalización exitosa del proceso de camuflaje.

Esta captura confirma que el proceso de camuflaje se ha completado exitosamente. La herramienta Camouflage ha generado un nuevo archivo llamado jpg_camuflage.jpg.

5.1.15 Contraseña del Archivo Camuflado

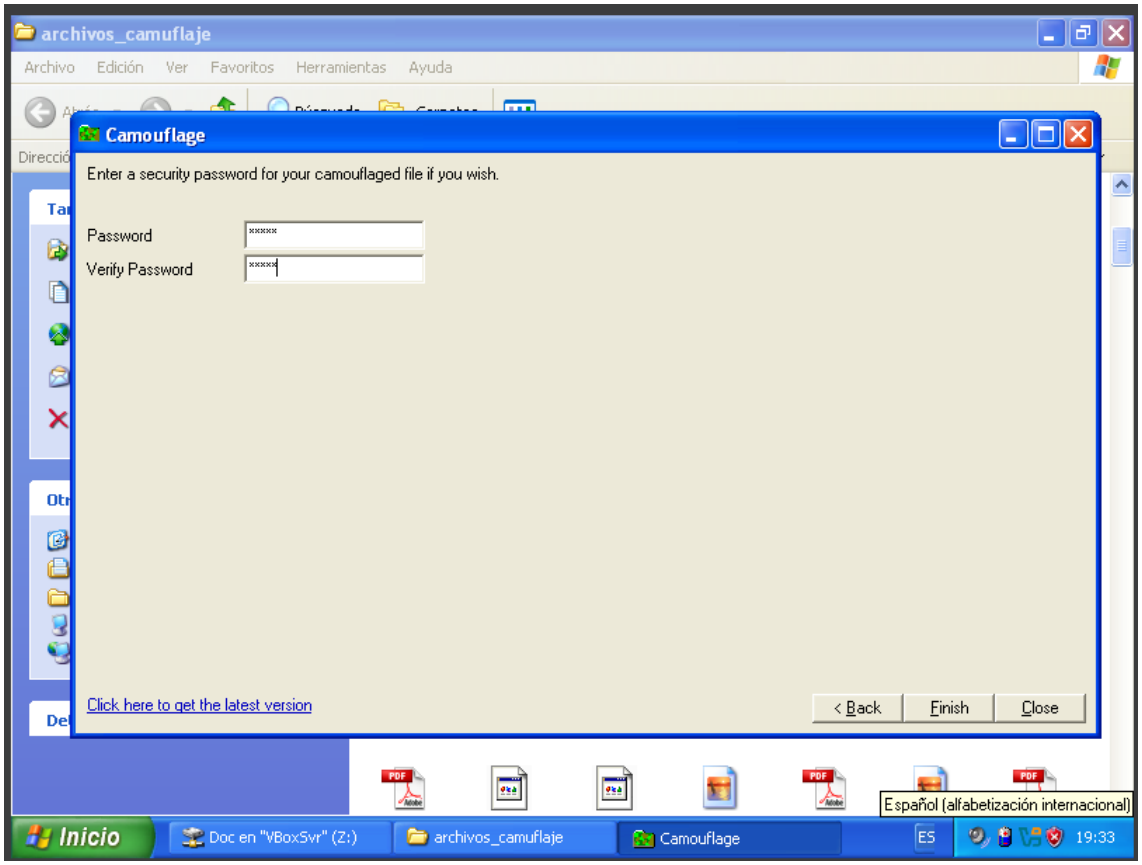

Ilustración 16. Configuración de contraseña para el archivo camuflado.

Esta captura muestra la ventana donde se puede establecer una contraseña de seguridad. Cuando se configura, cualquier intento de extraer los archivos ocultos del JPG requerirá ingresar esta contraseña.

5.1.16 Propiedades del Archivo JPG Camuflado

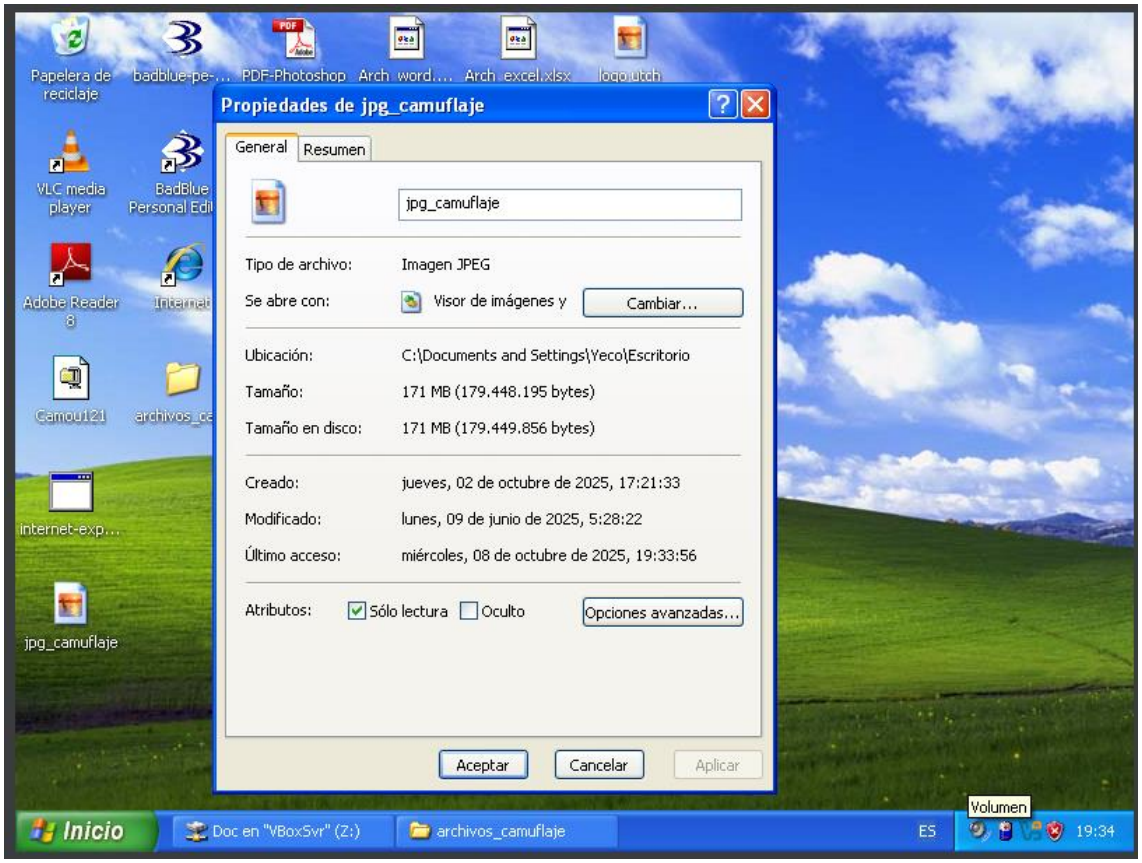

Ilustración 17. Propiedades del archivo JPG después del camuflaje.

Esta captura muestra las propiedades del archivo jpg_camuflaje después del proceso de ocultamiento.

Tamaño final: 171 MB

5.1.17 Verificación de Archivos Ocultos JPG Camuflado

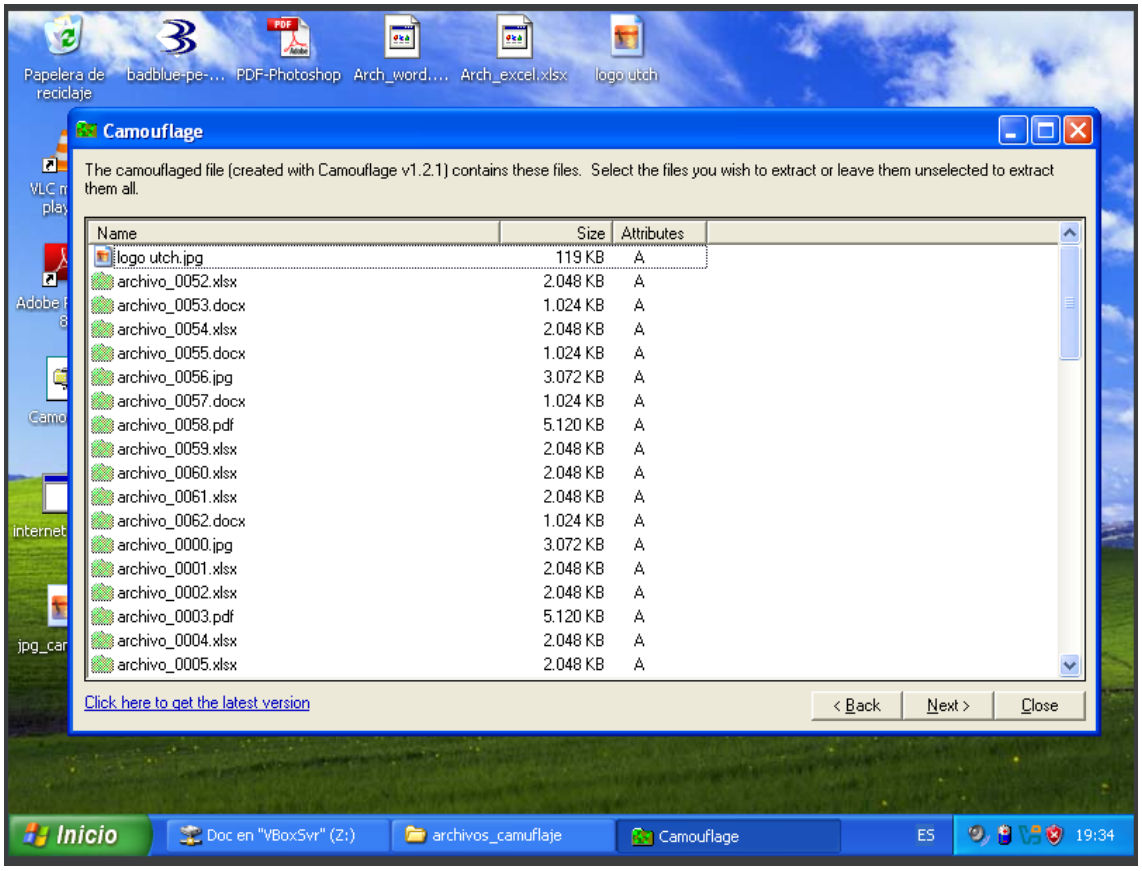

Ilustración 18. Interfaz mostrando la lista de archivos extraíbles del JPG camuflado.

Esta captura es la evidencia definitiva del éxito del camuflaje. Al abrir el archivo jpg_camuflaje con Camouflage, la herramienta muestra la lista completa de archivos que están ocultos dentro de la imagen.

5.1.18 Selección de Archivos para Camuflaje en PDF

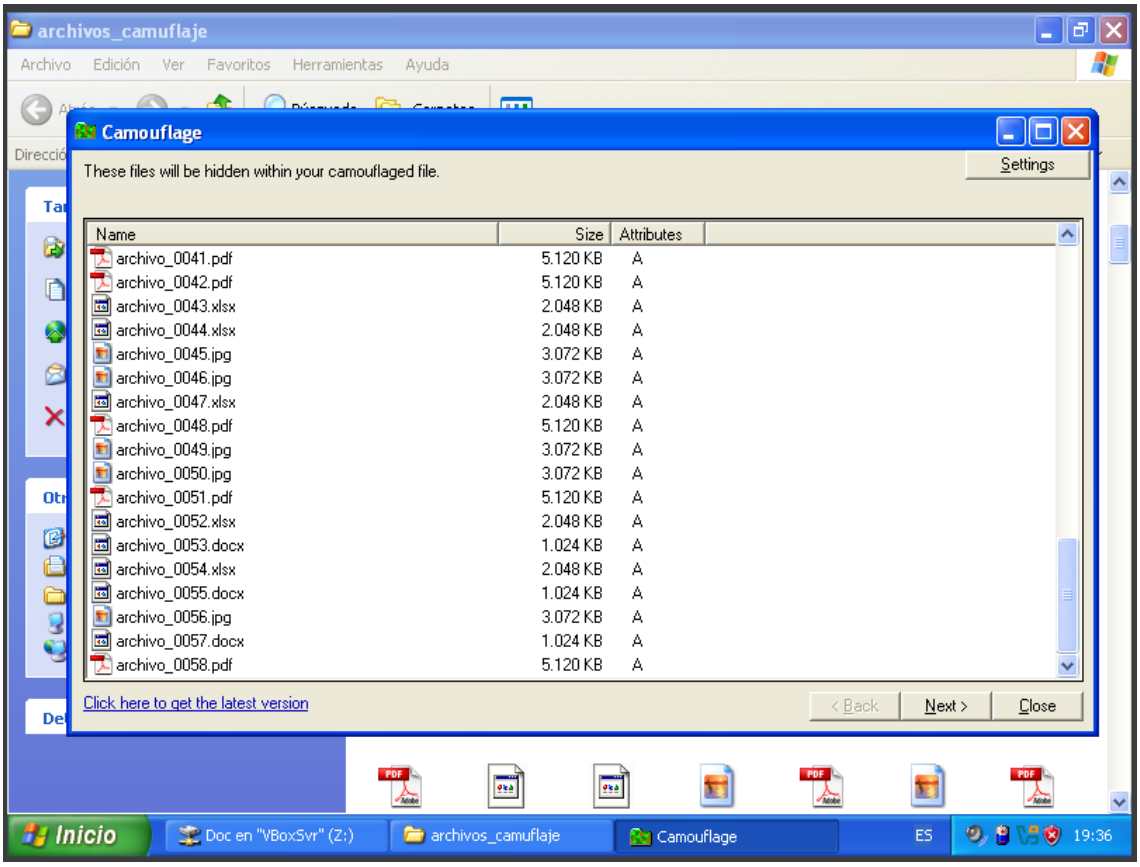

Ilustración 19. Interfaz mostrando archivos para ser ocultados dentro de un PDF.

Se observa la selección de archivos para ser camuflados dentro de un PDF.

5.1.19 Configuración del Archivo PDF Portador

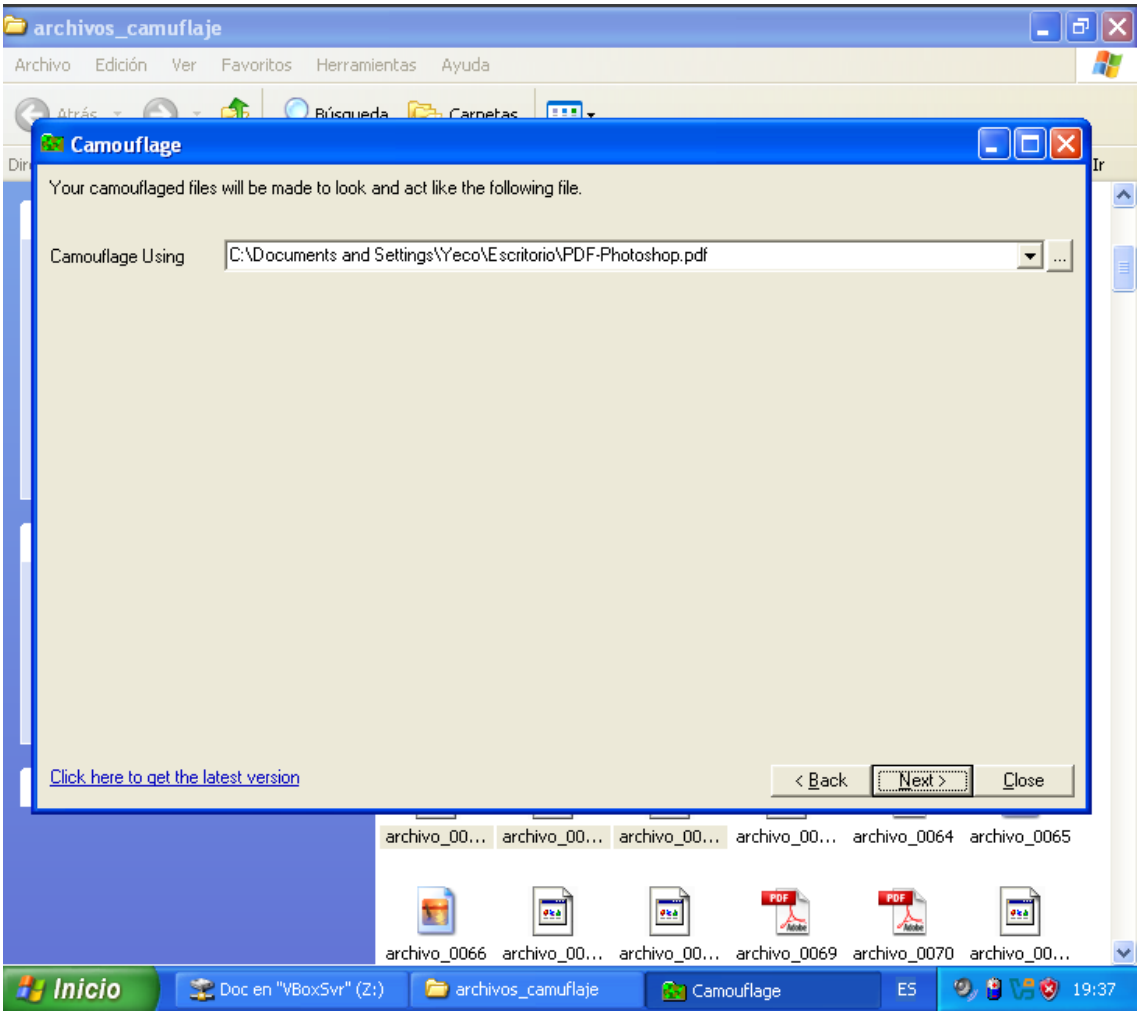

Ilustración 20. Selección del archivo PDF como archivo para el camuflaje.

En este paso, se configura un archivo PDF como el archivo portador para el camuflaje. Esto significa que todos los archivos seleccionados serán ocultados dentro de este documento PDF.

5.1.20 Proceso de Camuflaje en PDF Completado

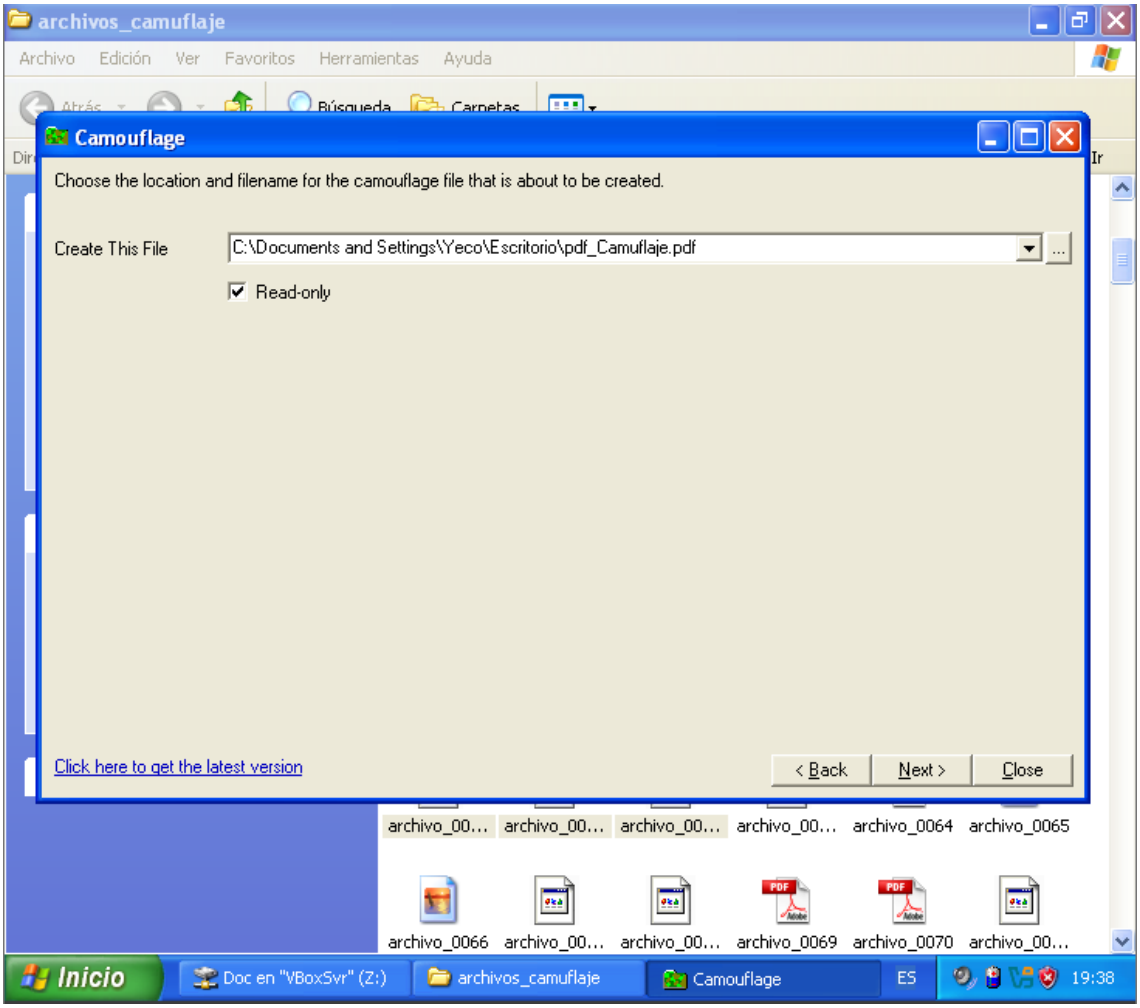

Ilustración 21. Archivo PDF camuflado resultante

Esta captura confirma la finalización exitosa del proceso de camuflaje usando un PDF como portador. Se ha generado el archivo pdf_Camuflaje.pdf que contiene todos los archivos seleccionados ocultos.

5.1.21 Propiedades del Archivo PDF Camuflado

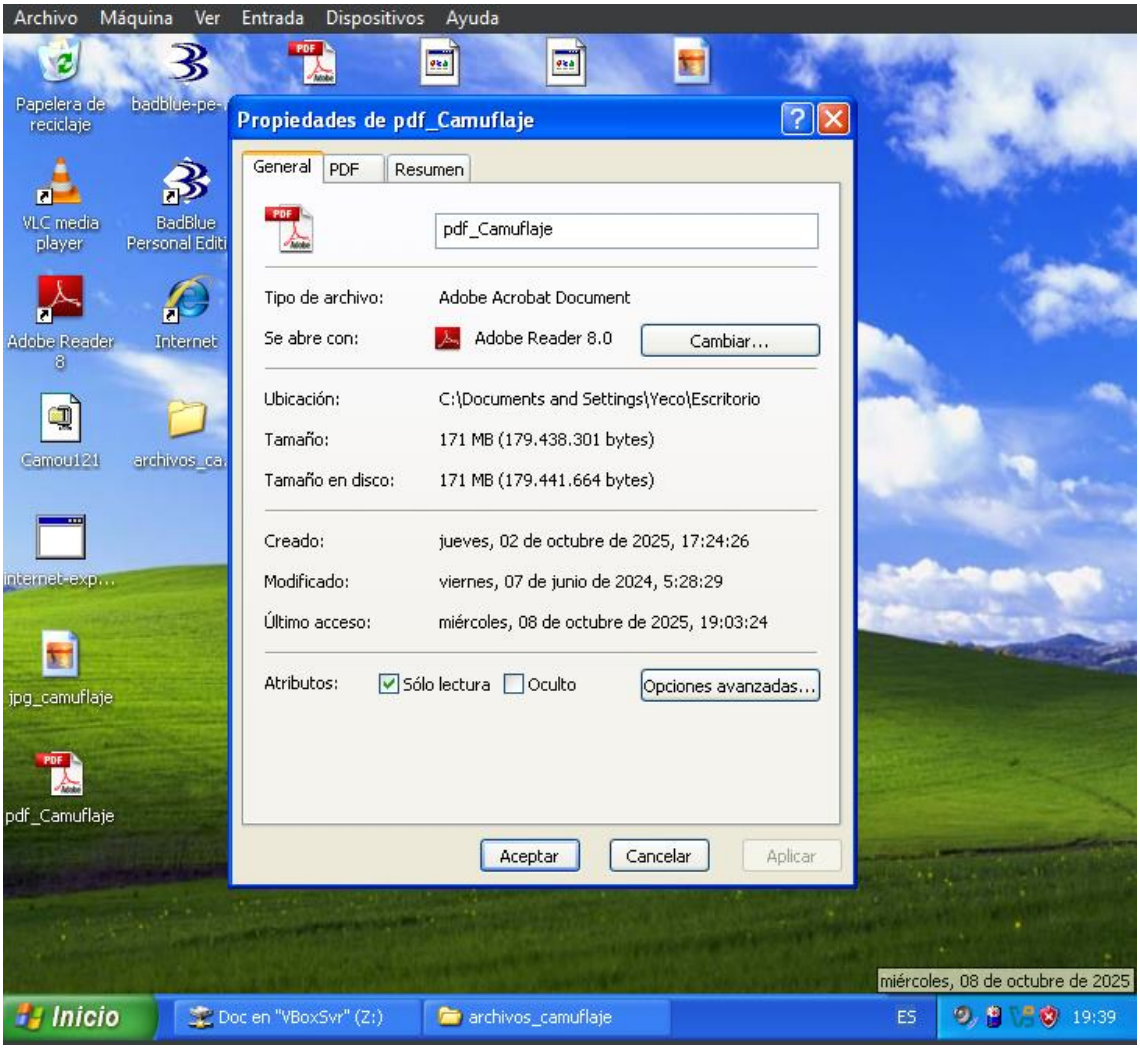

Ilustración 22. propiedades del archivo PDF después del proceso de camuflaje.

Esta captura muestra las propiedades técnicas del archivo pdf_Camuflaje.pdf después del proceso de ocultamiento.

5.1.22 Verificación de Archivos en el PDF Camuflado

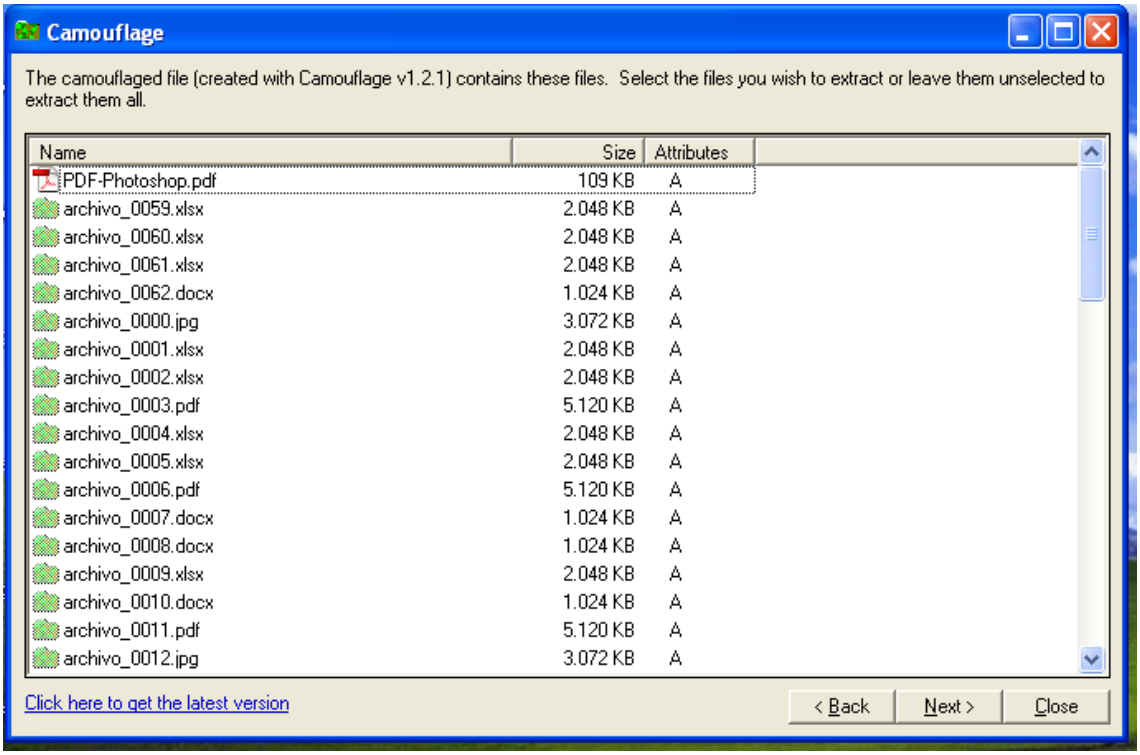

Ilustración 23. Interfaz mostrando la lista de archivos extraíbles del PDF camuflado

Esta es la verificación final y del camuflaje en PDF. Al abrir el archivo pdf_Camuflaje.pdf con Camouflage, la herramienta muestra la lista completa de archivos ocultos.

5.1.23 Selección de Archivos para Camuflaje en Word

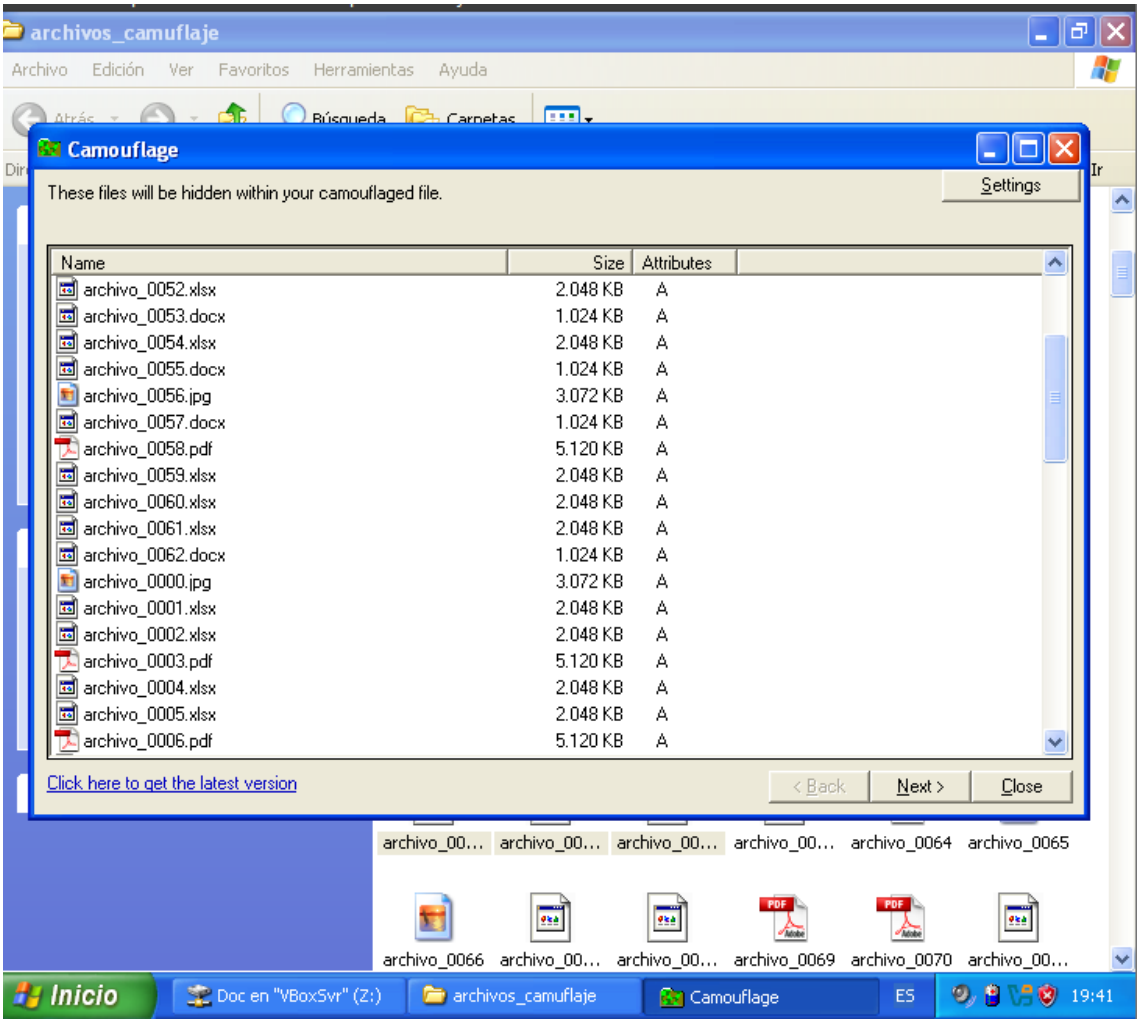

Ilustración 24. Interfaz archivos para ser ocultados dentro de un documento Word

Esta captura documenta otra prueba exitosa de camuflaje, esta vez utilizando un documento Word como portador.

5.1.24 Configuración del Archivo Word

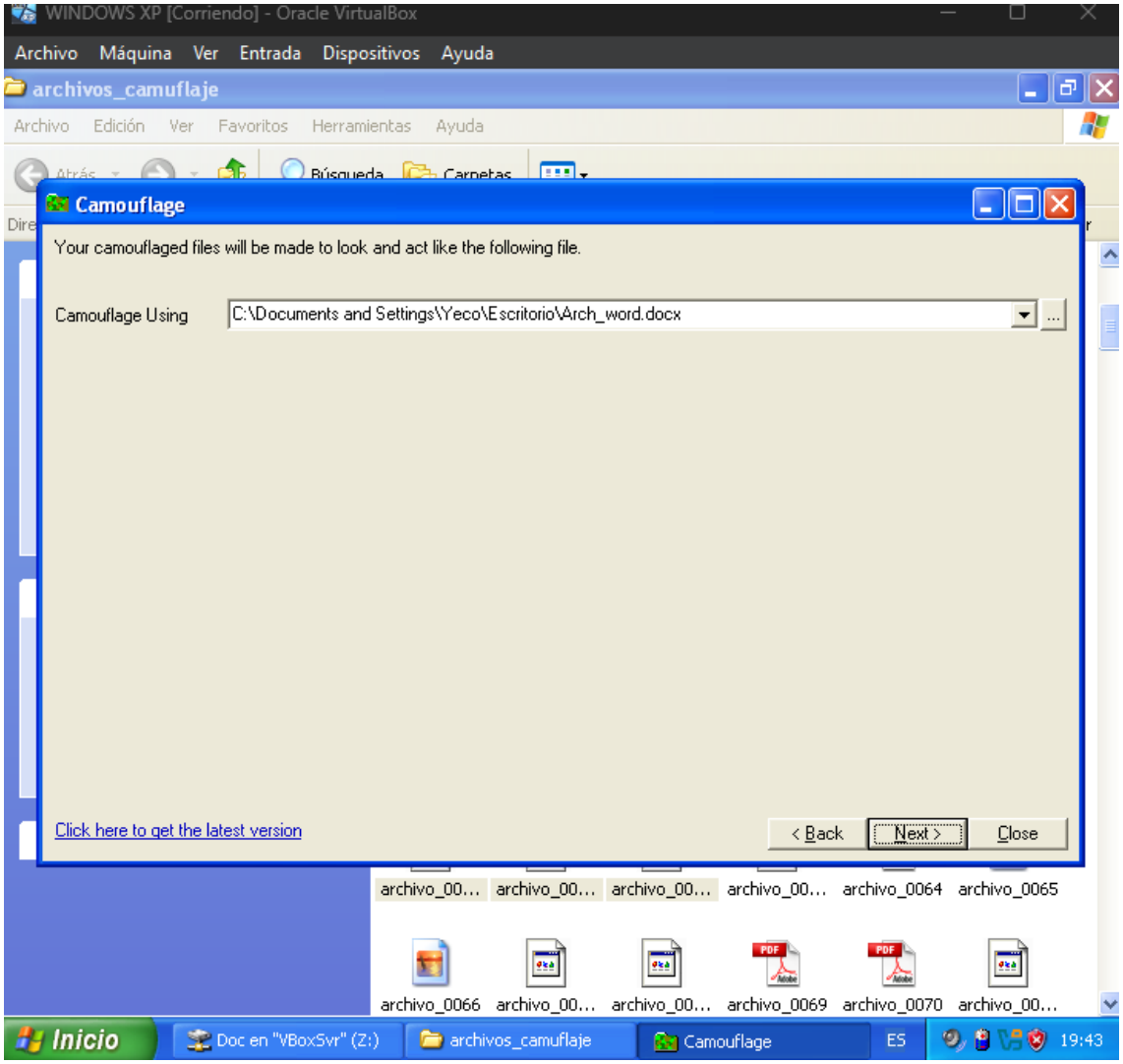

Ilustración 25. Selección del archivo para el camuflaje en Word.

En este paso, se configura un archivo Word como el archivo portador para el camuflaje. Esto significa que todos los archivos seleccionados serán ocultados dentro de este documento Word.

5.1.25 Creación del Archivo Word Camuflado

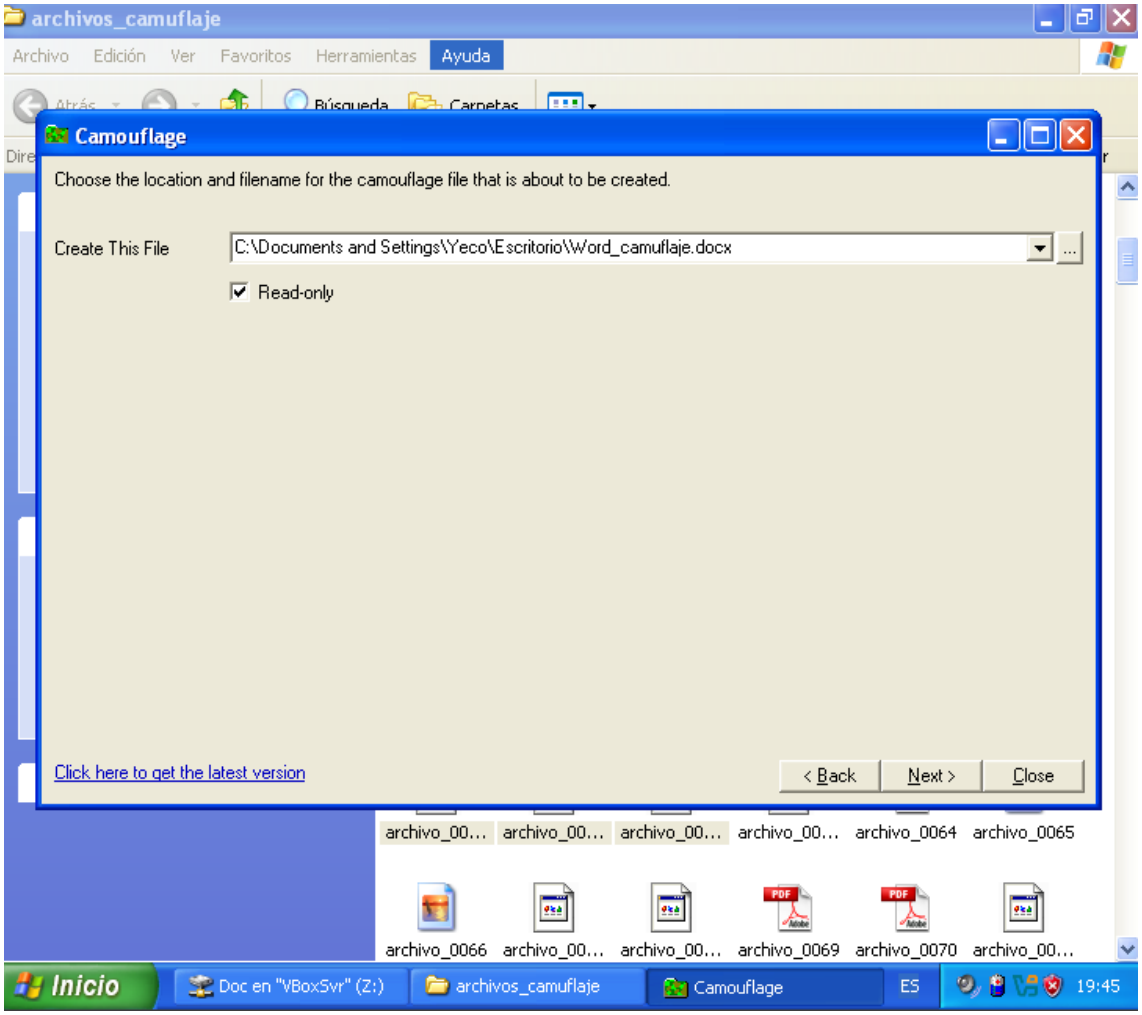

Ilustración 26. Configuración final para generar el archivo Word camuflado

Esta captura muestra la configuración final antes de generar el archivo camuflado.

Nombre del archivo: Word_camuflaje.docx

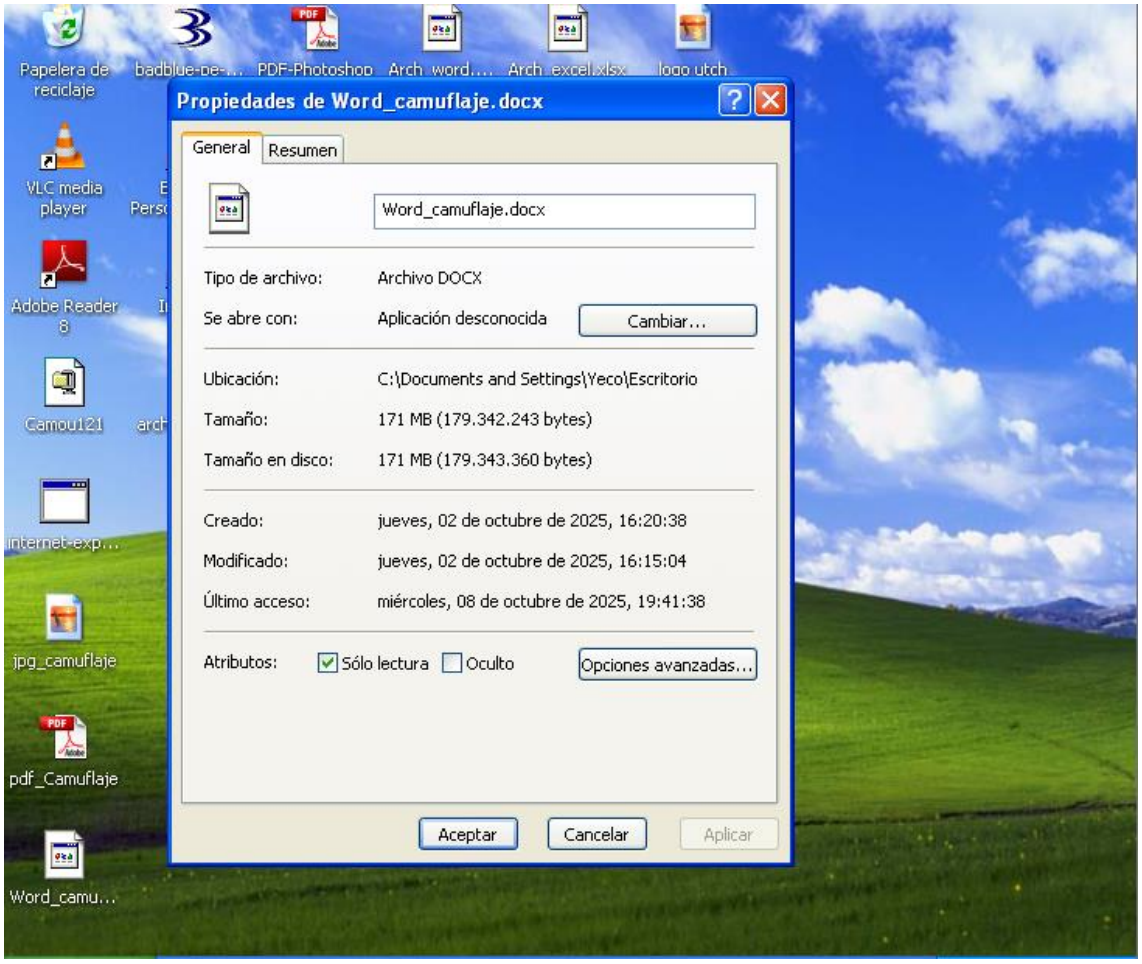

Ilustración 27. propiedades del archivo WORD después del proceso de camuflaje.

5.1.26 Propiedades del Archivo Word Camuflado

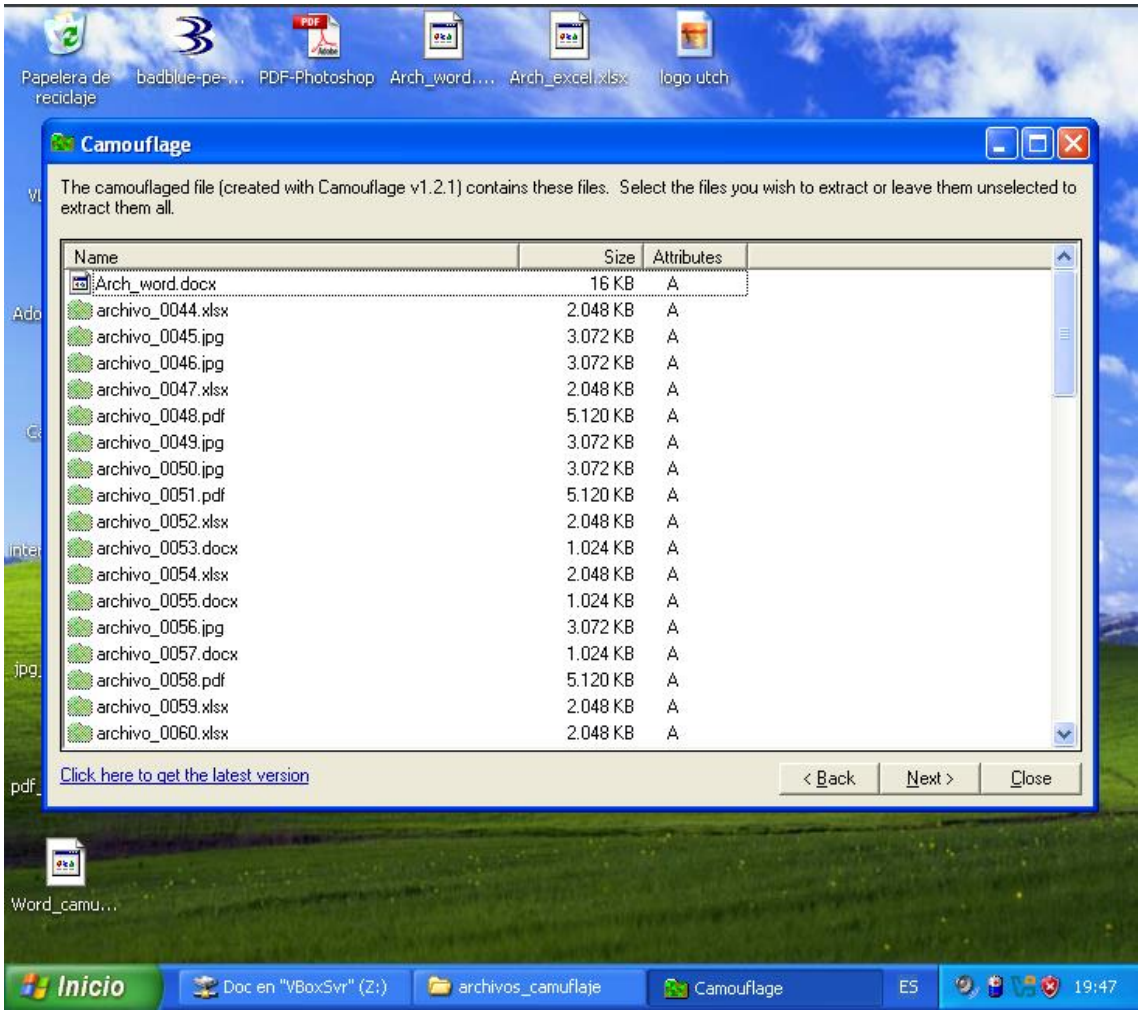

Ilustración 28. propiedades del archivo Word después del proceso de camuflaje.

Esta captura muestra las propiedades del archivo Word_camuflaje.docx después del proceso de ocultamiento.

5.1.27 Selección de Archivos para Camuflaje en Excel

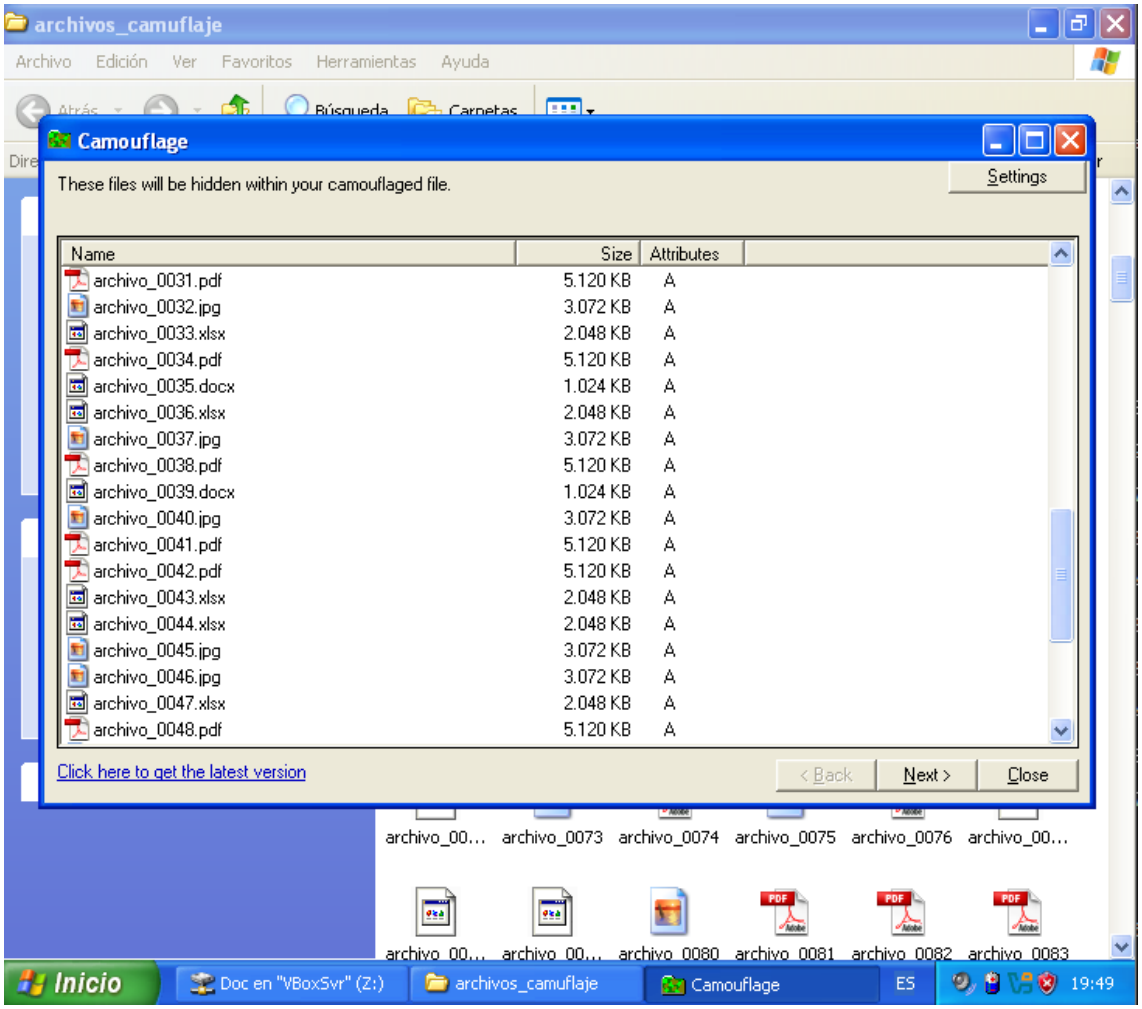

Ilustración 29. Interfaz de archivos para ser ocultados dentro de una Excel.

Se observa la selección de archivos, que incluyen:

- Formatos diversos: PDF, JPG, XLSX (Excel), DOCX (Word)
- Tamaños variados

5.1.28 Selección del Archivo Excel Portador

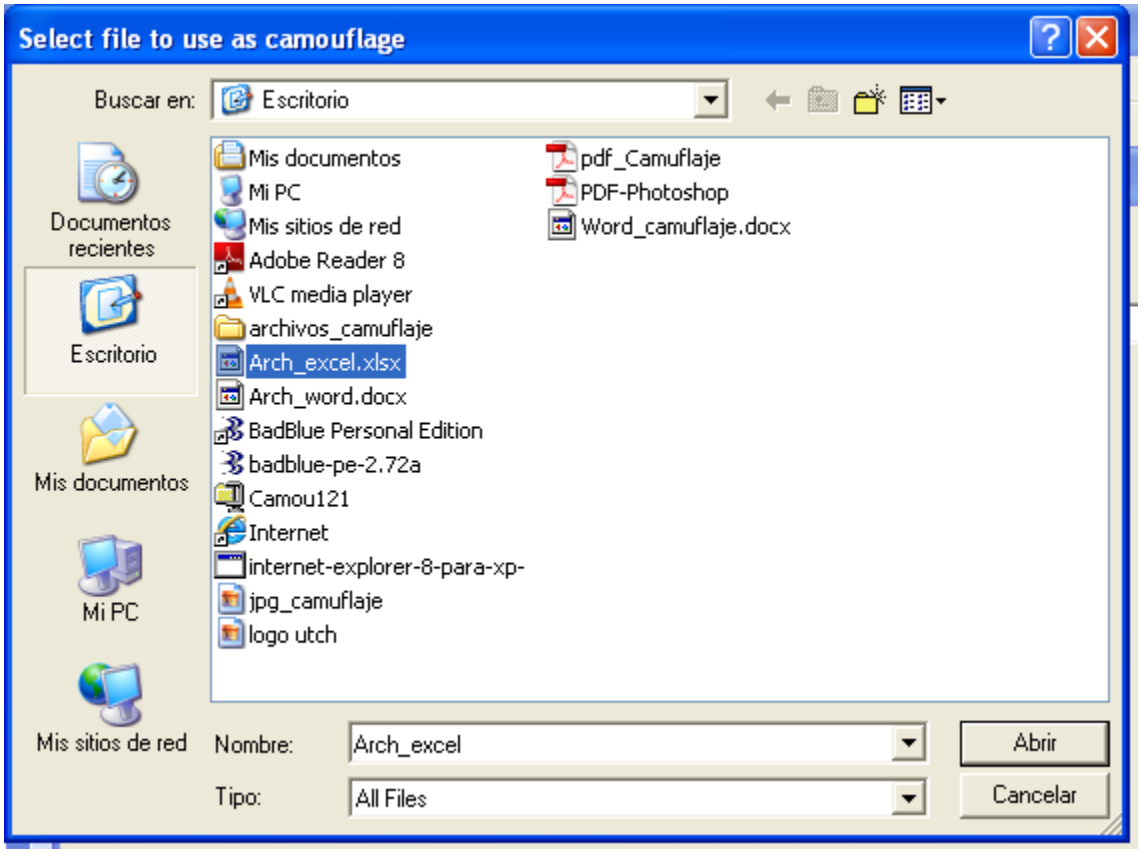

Ilustración 30. selección del archivo como archivo realizar el camuflaje.

En este paso, se navega a el archivo Excel ubicado en el escritorio como el archivo portador para el camuflaje. La interfaz muestra los archivos disponibles en el escritorio, incluyendo los archivos camuflados creados (jpg_camuflaje,).

5.1.29 Configuración del Archivo Excel Portador

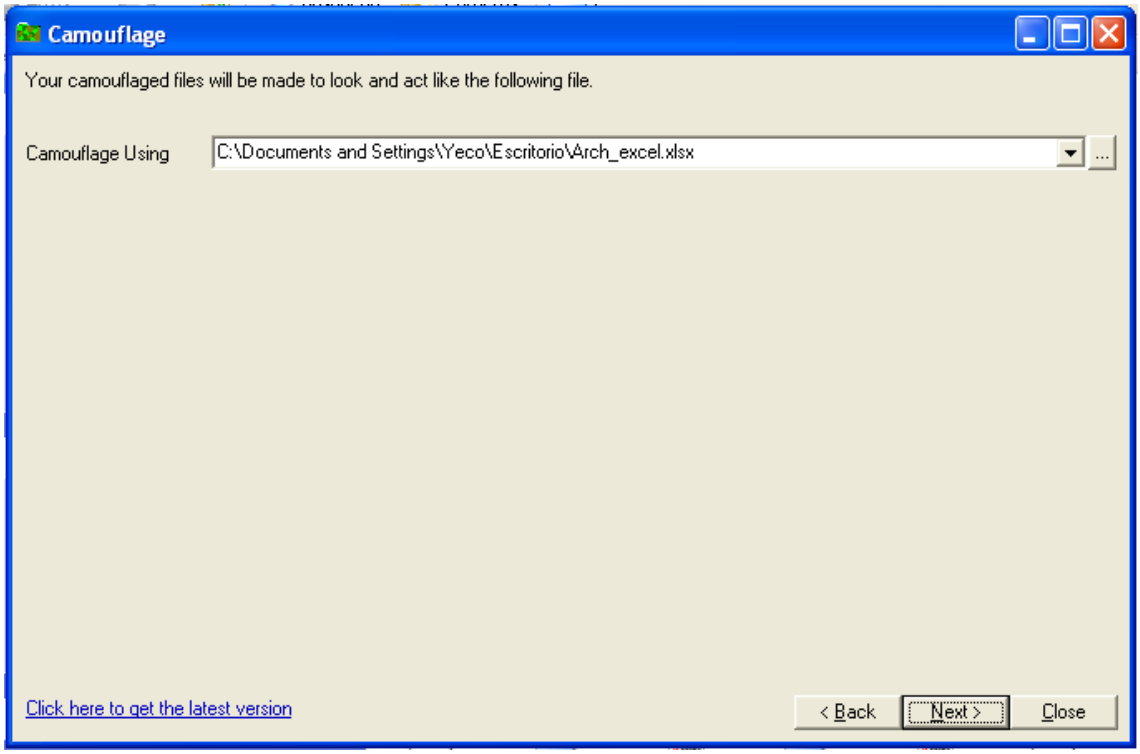

Ilustración 31. Confirmación de la selección como archivo para camuflaje

Esta captura confirma que se ha seleccionado el archivo como el archivo portador. Esto significa que todos los archivos seleccionados previamente serán ocultados dentro del Excel.

5.1.30 Creación del Archivo Excel Camuflado

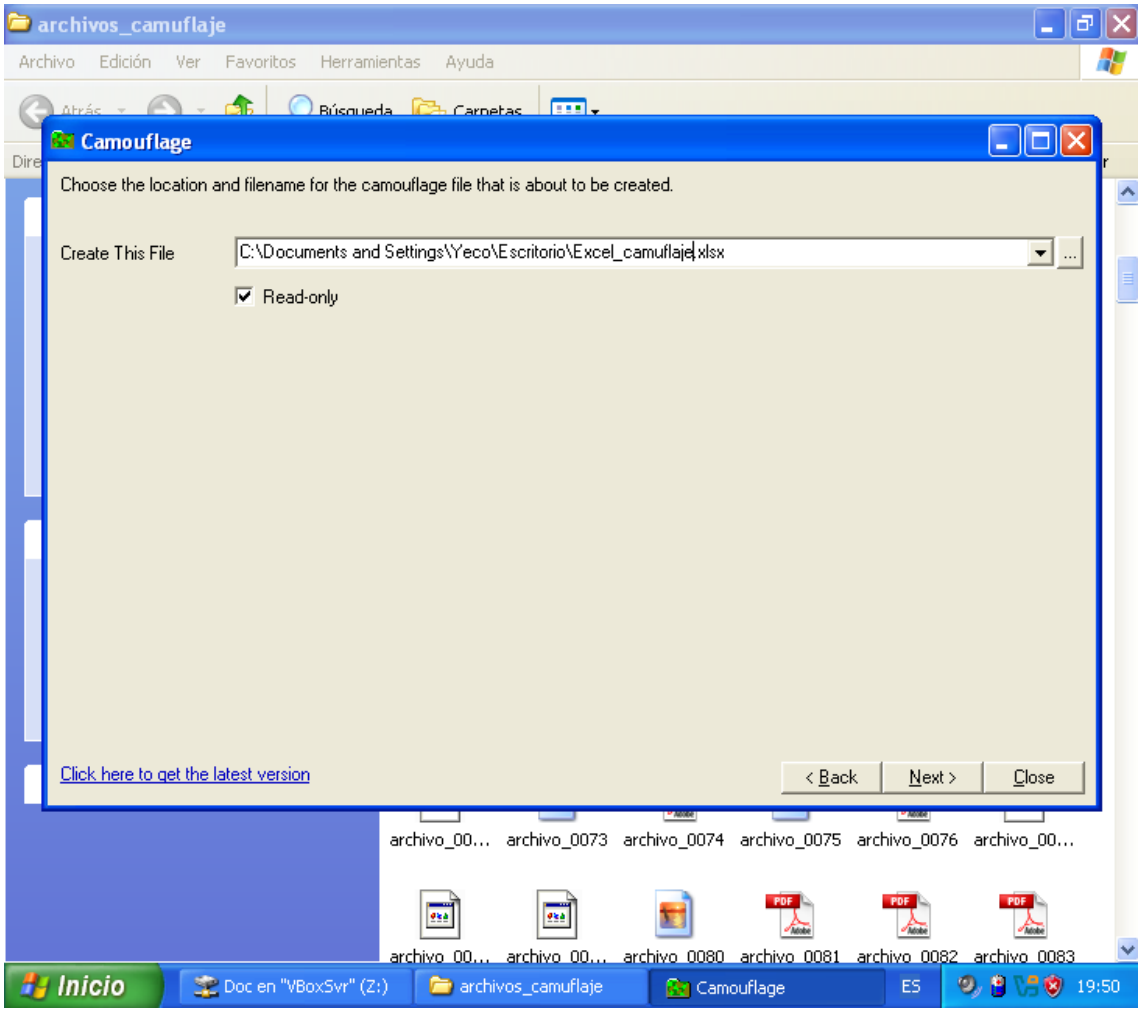

Ilustración 32. Configuración final para generar el archivo Excel camuflado.

Esta captura muestra la configuración final antes de generar el archivo camuflado.

5.1.31 Propiedades del Archivo Excel Camuflado

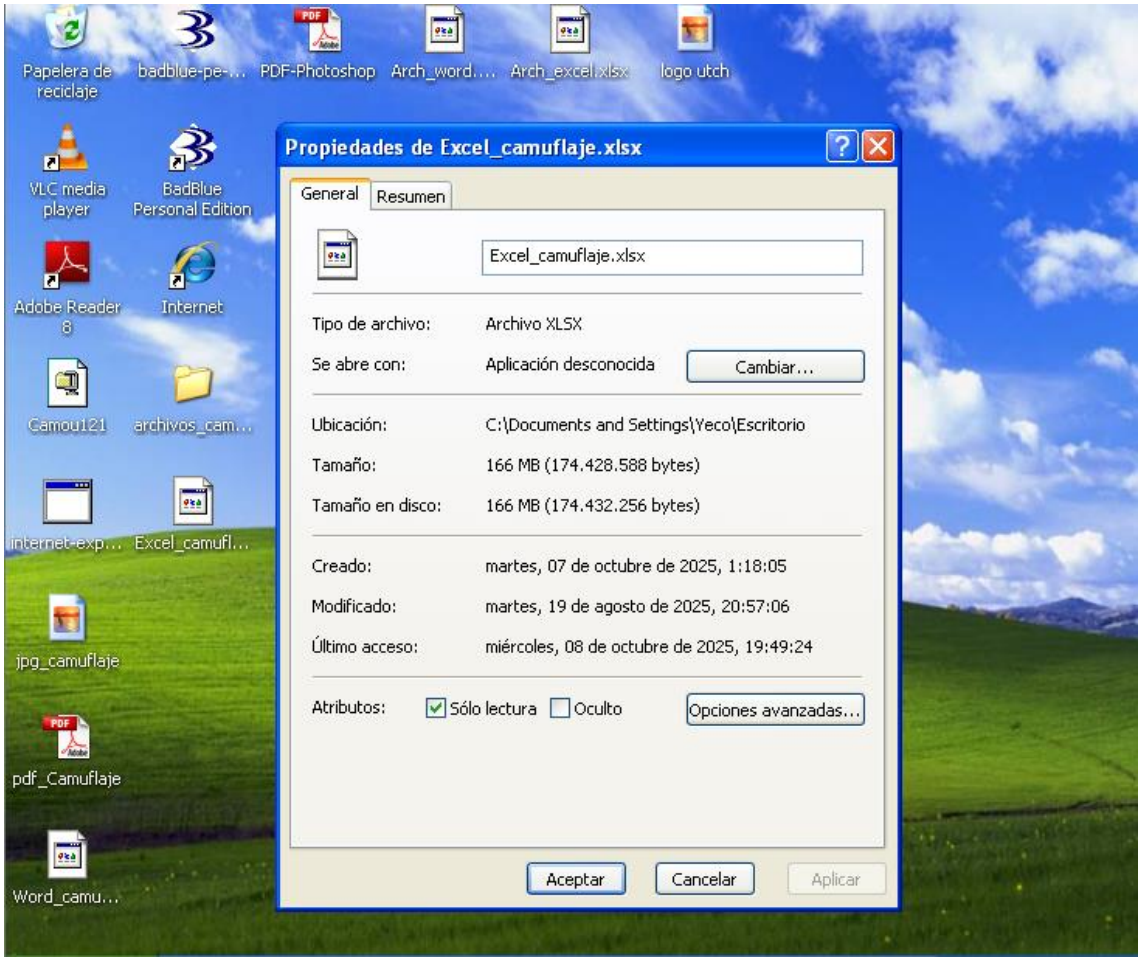

Ilustración 33. Propiedades del archivo Excel después del proceso de camuflaje.

Esta captura muestra las propiedades del archivo Excel_camuflaje.xlsx después del proceso de ocultamiento.

5.1.32 Verificación Final de Archivos Ocultos en el Excel Camuflado

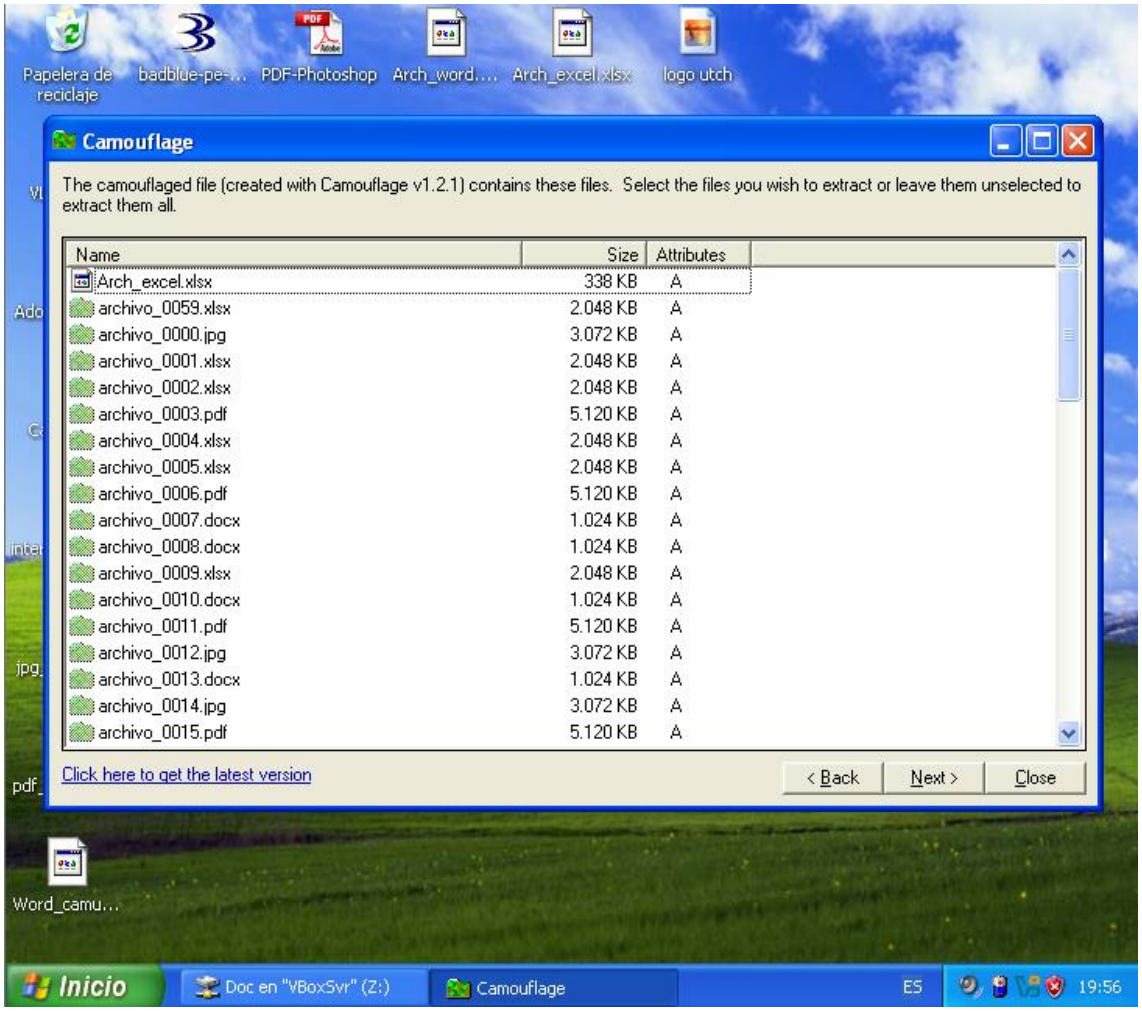

Ilustración 34. Interfaz mostrando los archivos extraíbles del Excel camuflada.

Esta es la verificación final del éxito del camuflaje en Excel. Al abrir el archivo Excel_camuflaje.xlsx con Camouflage, la herramienta muestra la lista completa de archivos ocultos.

5.2.Capitulo #2

5.2.1 Escaneo de Red para Identificar BadBlue

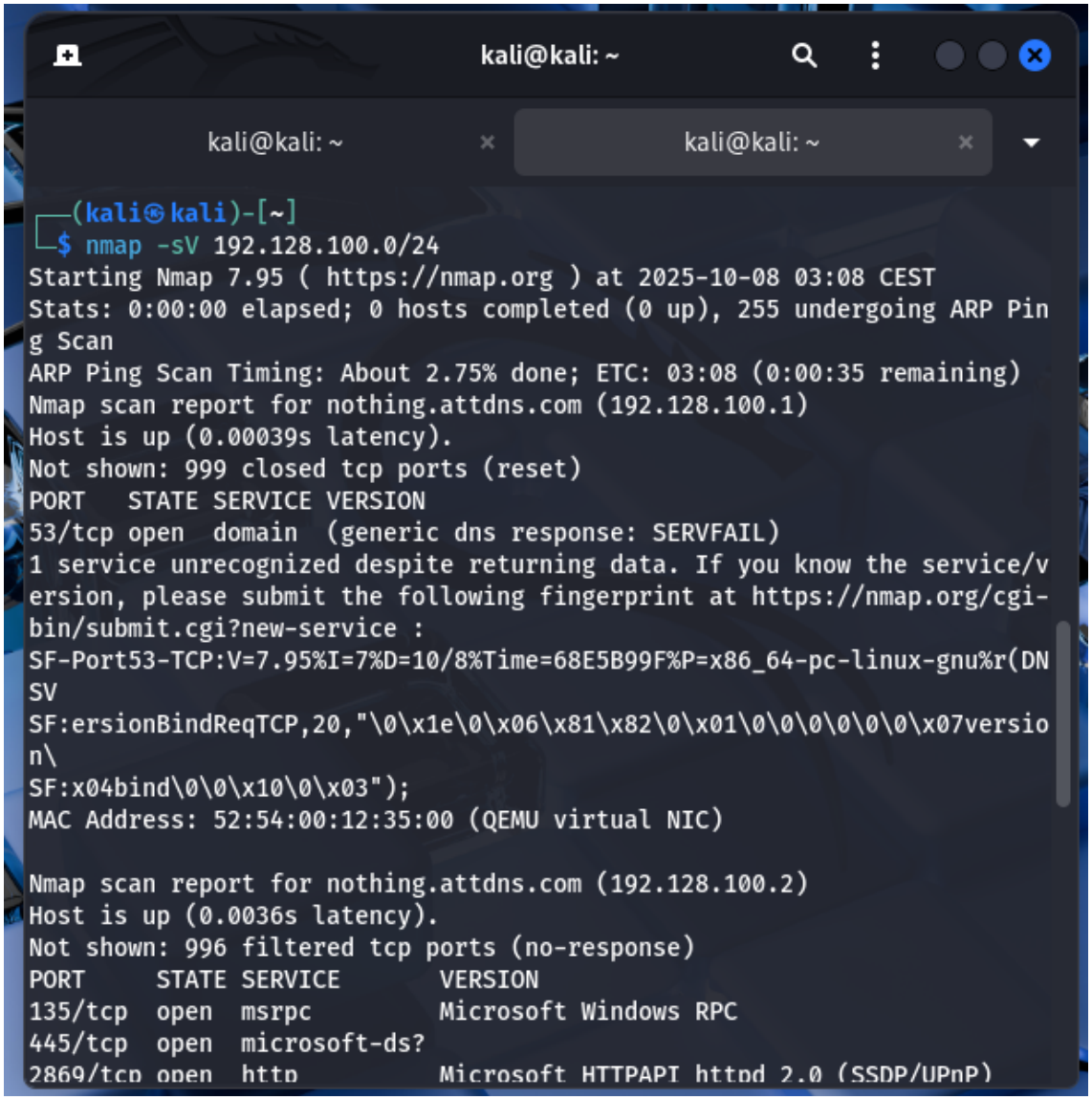

Ilustración 35. Resultado del escaneo Nmap mostrando los servicios activos en la red

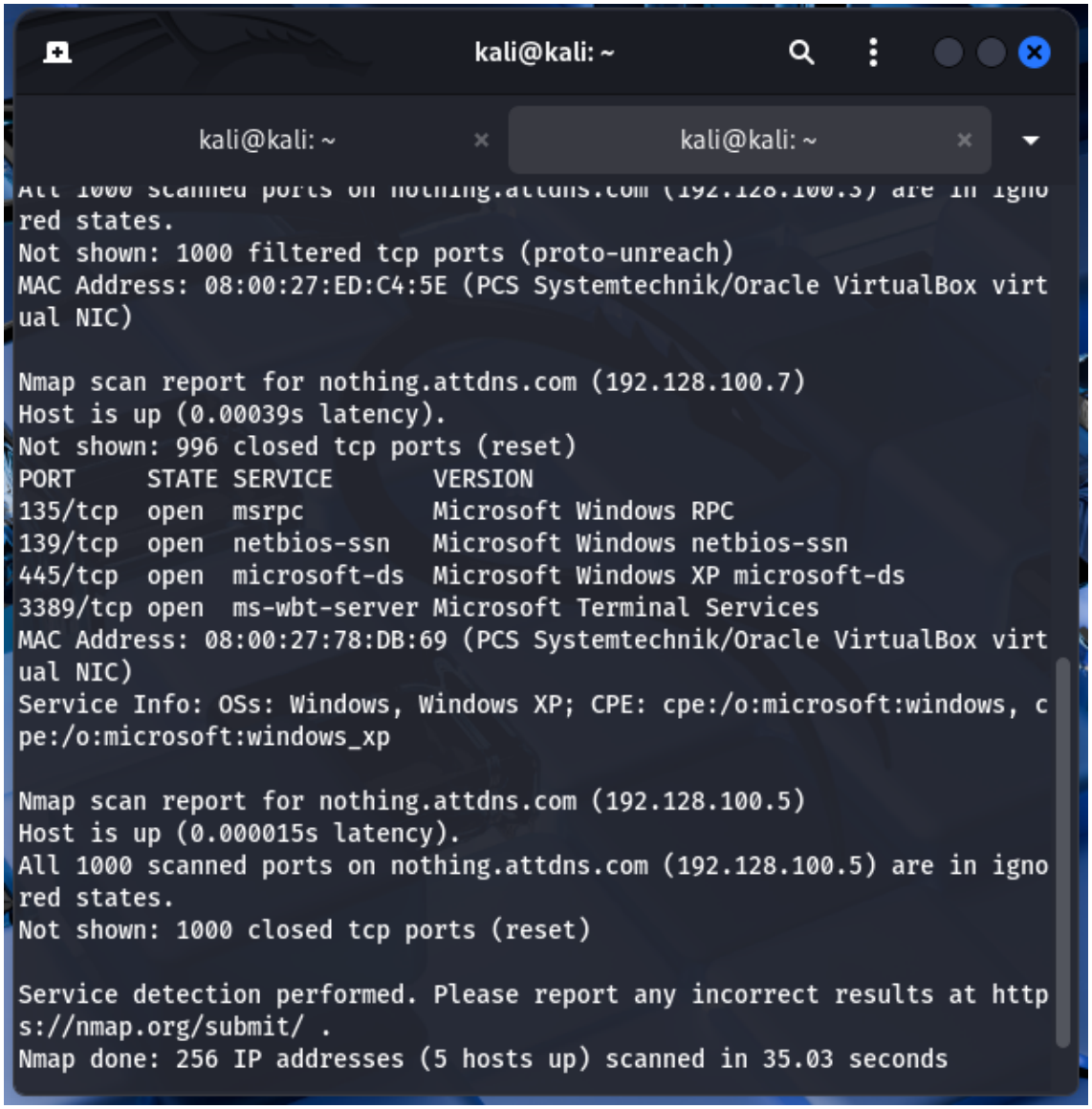

Ilustración 36. Escaneo Nmap mostrando los servicios activos en la red 192.128.100.7

El comando nmap -sV 192.128.100.0/24 escaneó toda la red y detectó varios hosts activos.

El hallazgo más relevante es el host 192.128.100.7 que ejecuta Windows XP.

5.2.2 Búsqueda de Exploits para BadBlue 2.7

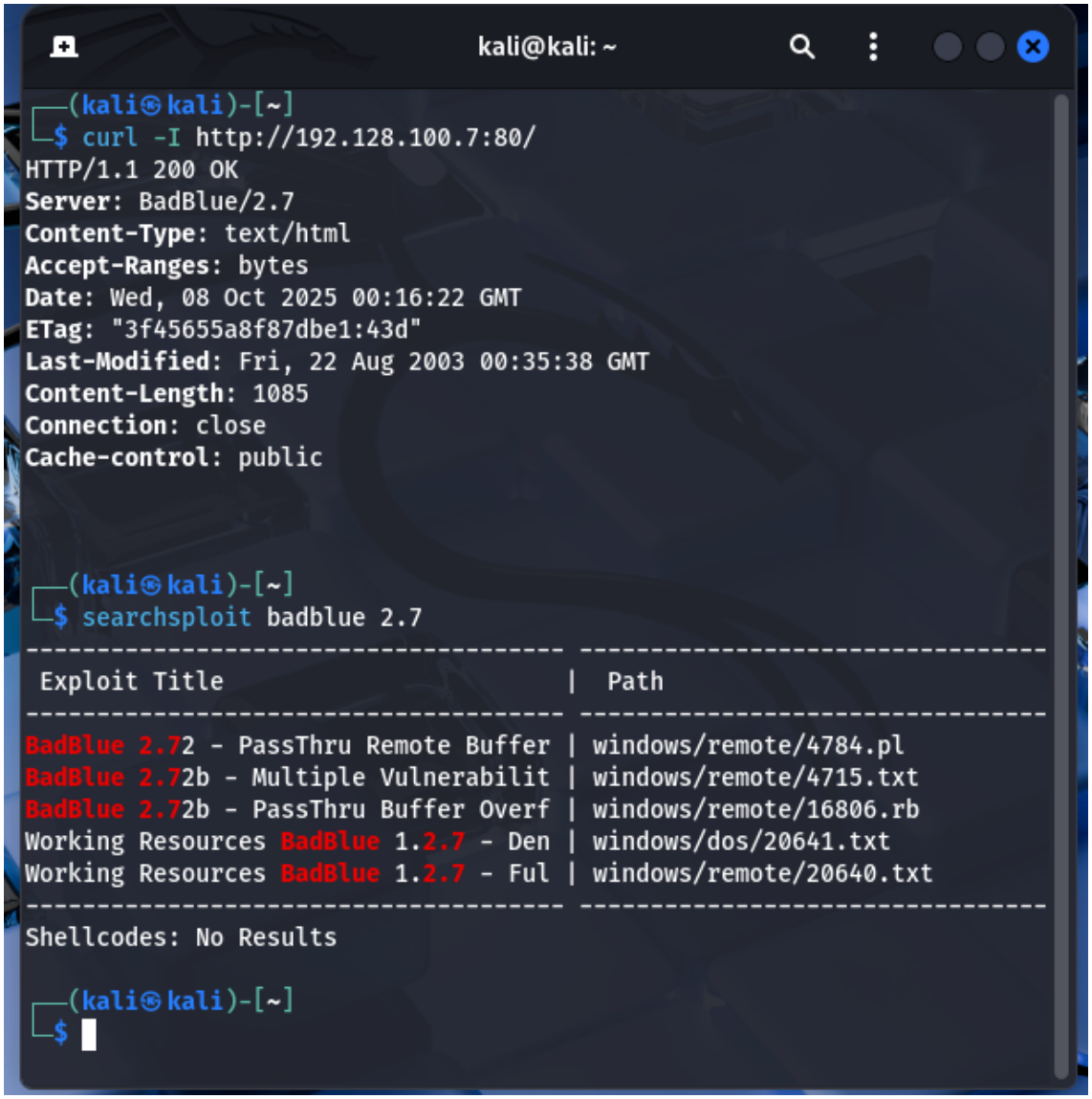

Ilustración 37. Verificación del servidor BadBlue

El comando curl -I http://192.128.100.7:80/ confirma que el servidor está ejecutando BadBlue/2.7

La búsqueda con searchsploit badblue 2.7 revela múltiples vulnerabilidades documentadas para esta versión, destacando el exploit BadBlue 2.72 - PassThru Remote Buffer Overflow (4784.pl) que permite ejecución remota mediante el componente PassThru de BadBlue.

5.2.3 Obtención y Preparación del Exploit

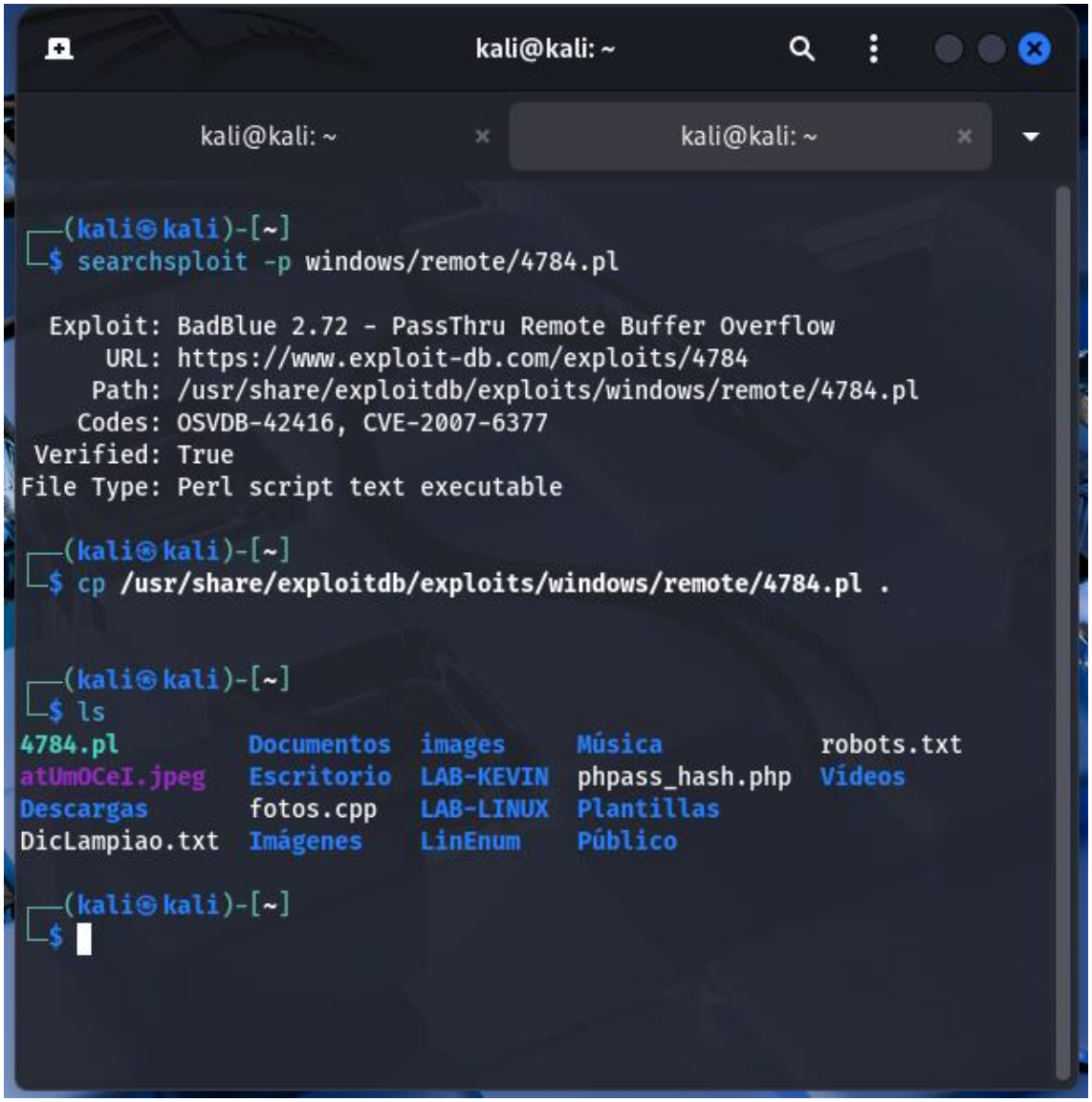

Ilustración 38. Localización y copia del exploit 4784.pl

El comando searchsploit -p windows/remote/4784.pl confirma la ubicación del archivo del exploit en el sistema (/usr/share/exploitdb/exploits/windows/remote/4784.pl)

5.2.4 Configuración del Exploit 4784.pl

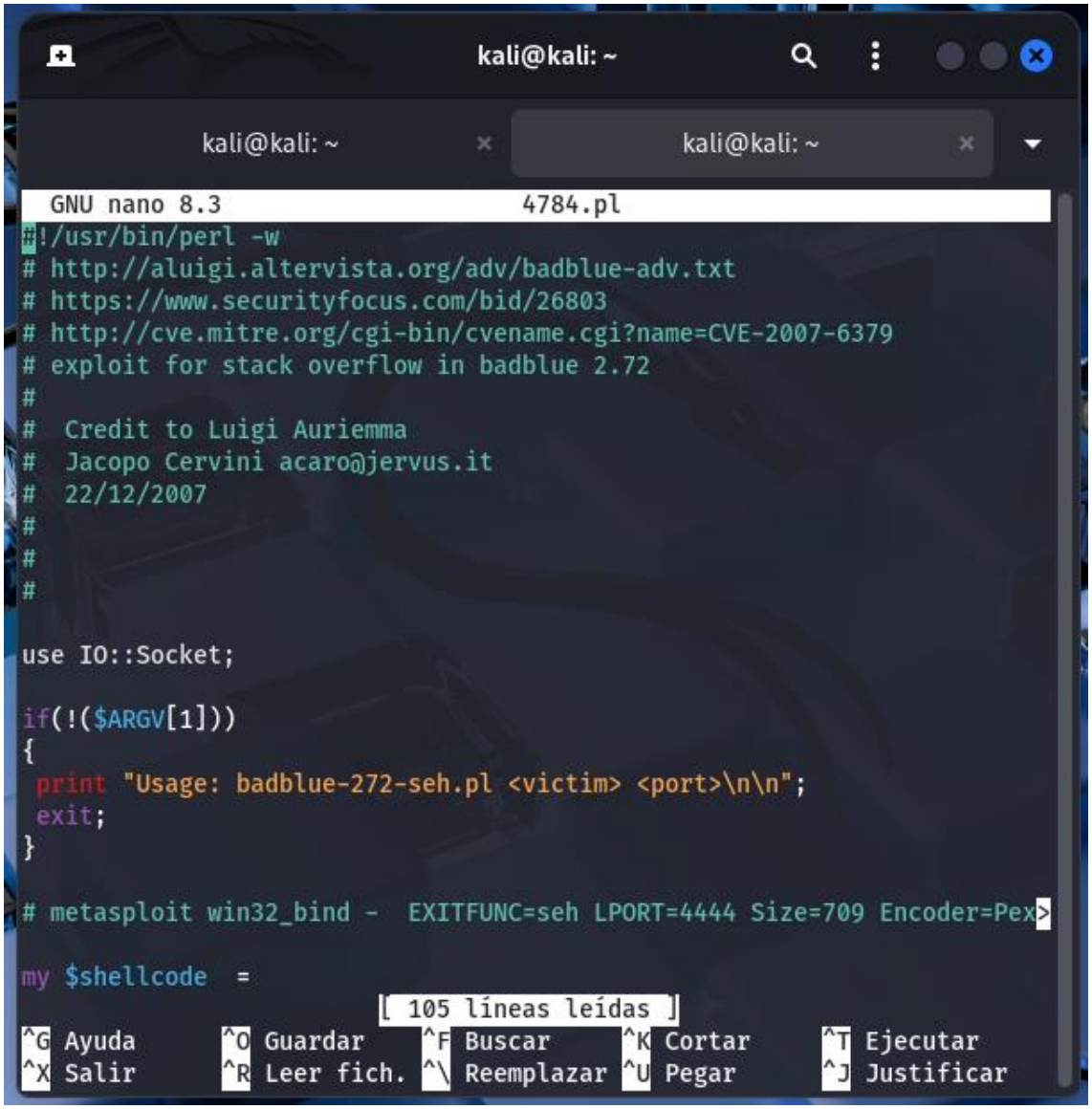

Ilustración 39. Edición del script de explotación BadBlue 2.72

Se procede a examinar y configurar el exploit 4784.pl utilizando el editor Nano.

5.2.5 Personalización del Exploit BadBlue

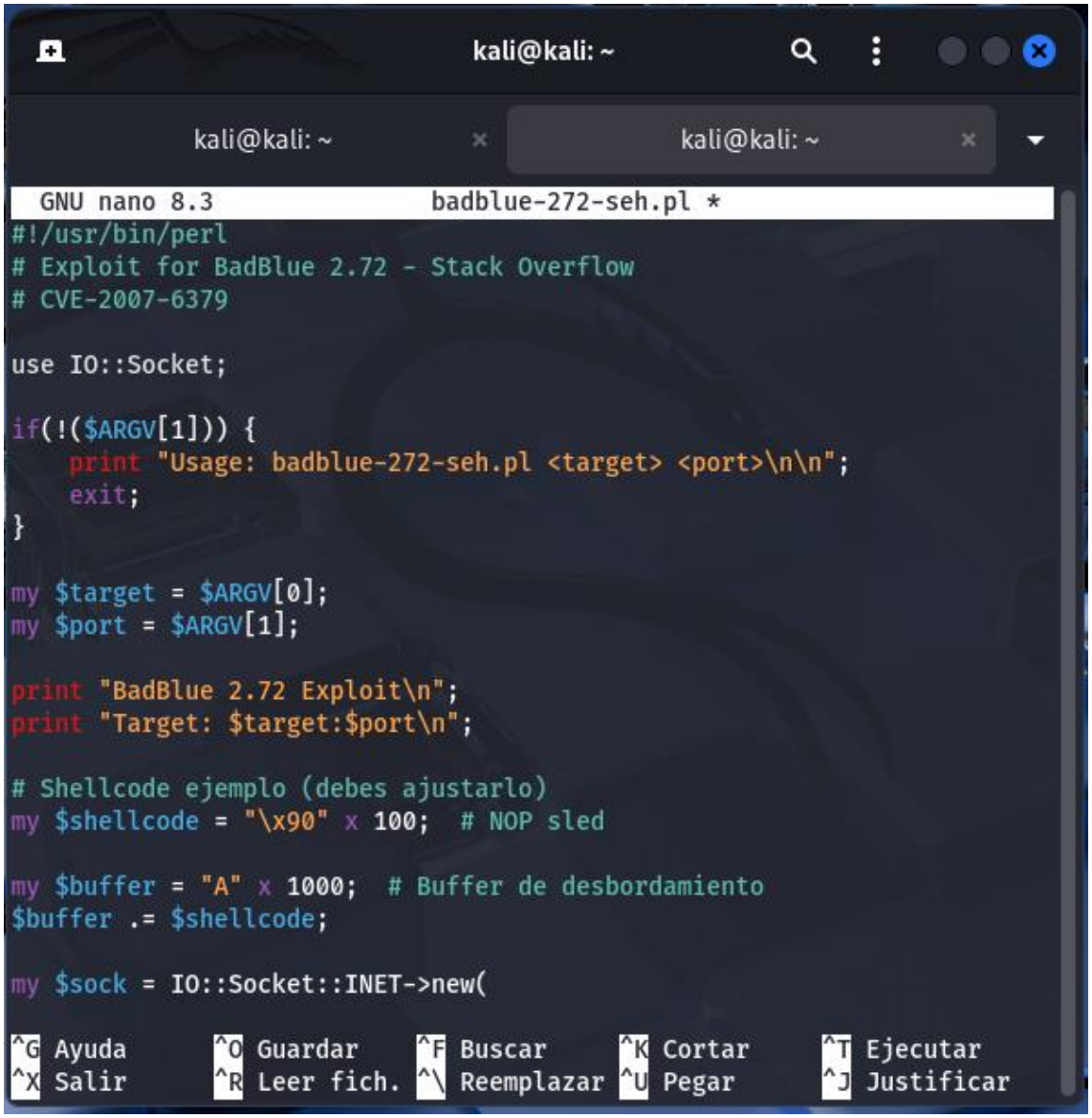

Ilustración 40. Modificación del script de explotación

Se muestra el proceso de personalización del exploit badblue-272-seh.pl para adaptarlo al entorno específico.

5.2.6 Preparación Final del Exploit BadBlue

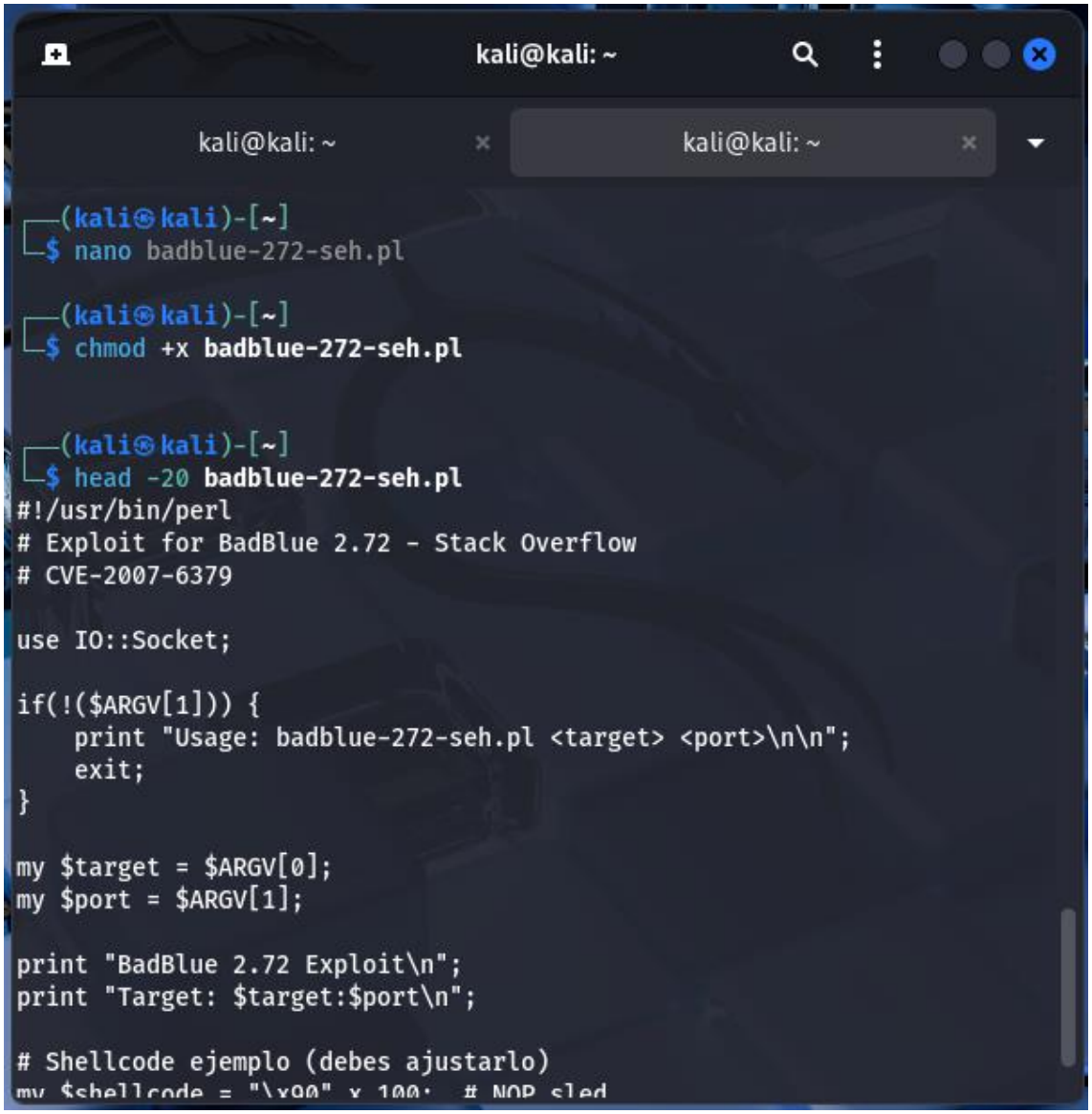

Ilustración 41. asignación de permisos de ejecución al script de explotación.

En esta fase final de preparación, se realizan los últimos ajustes al exploit badblue-272-seh.pl. El script es editado con Nano para asegurar su correcta configuración, luego se le asignan permisos de ejecución con chmod +x para permitir su ejecución. La verificación con head -20 confirma que el script contiene la estructura básica del exploit.

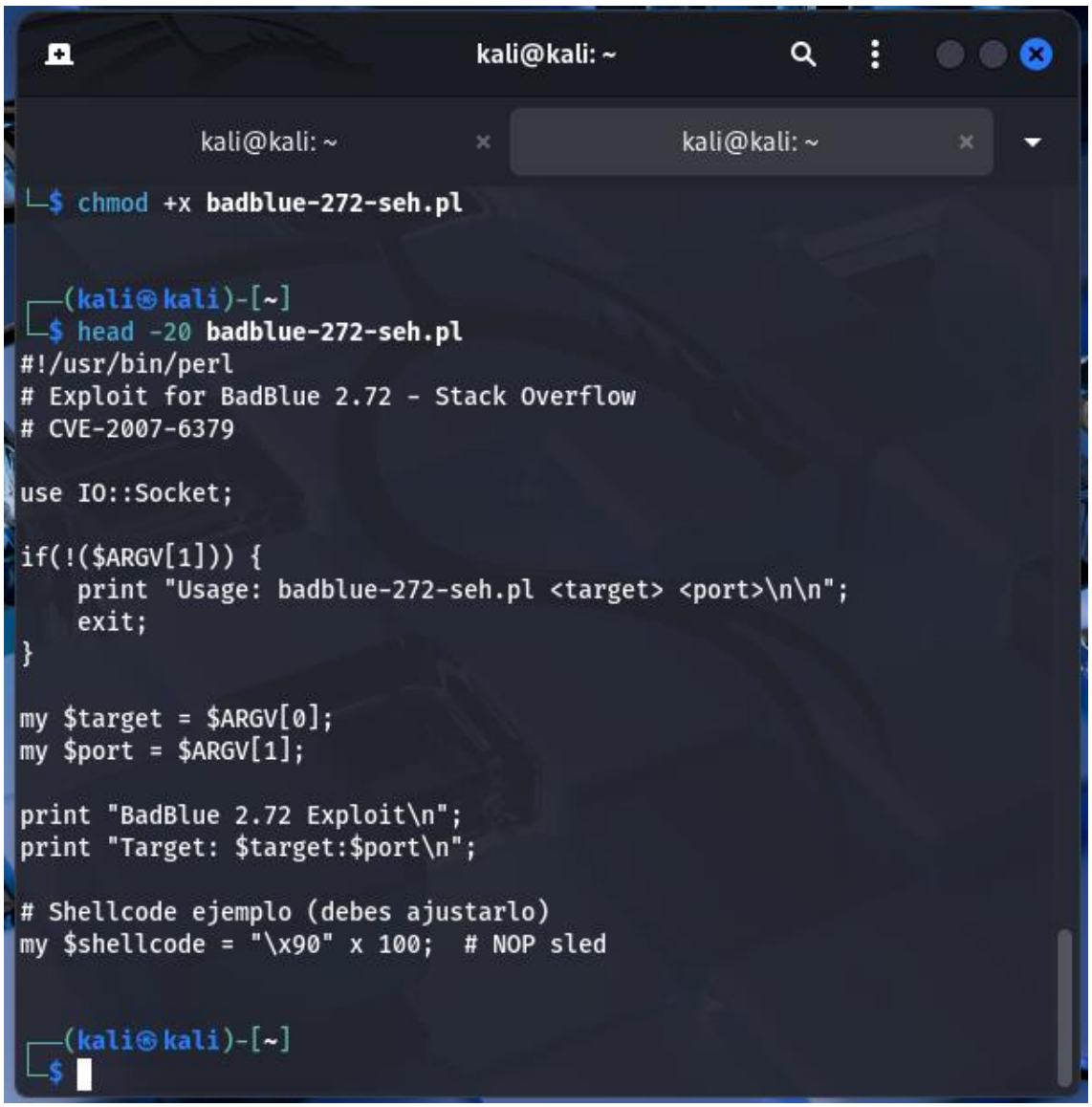

Ilustración 42. Verificación de permisos de ejecución al script de explotación.

5.2.7 Explotación Exitosa de BadBlue

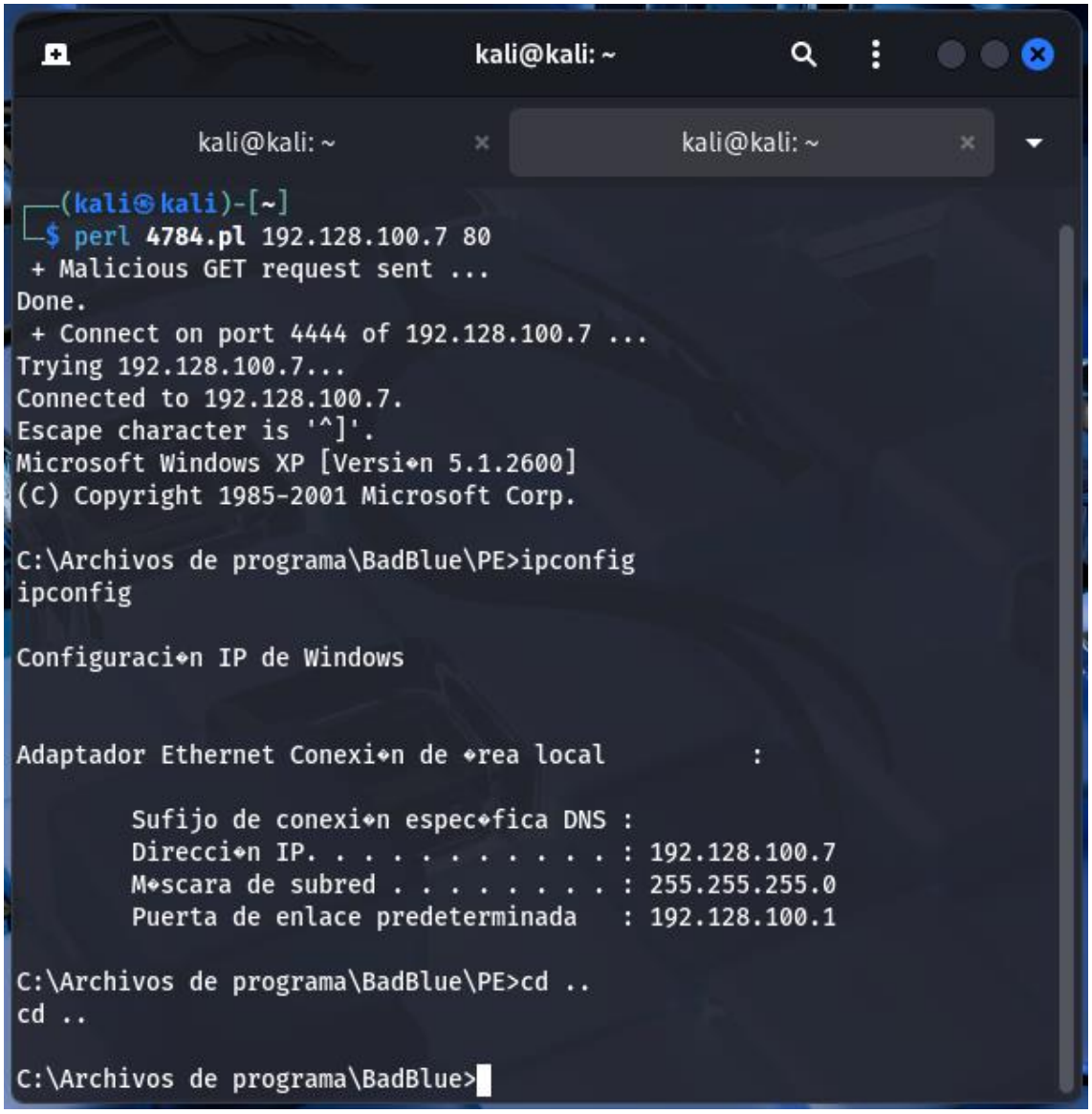

Ilustración 43. Explotación de BadBlue y Obtención de Shell Remoto

¡ÉXITO DE EXPLOTACIÓN! Esta captura documenta el final de la práctica: la explotación exitosa de la vulnerabilidad en BadBlue 2.72.

Al ejecutar perl 4784.pl 192.128.100.7 80, el exploit envía una petición GET maliciosa al componente PassThru de BadBlue.

5.2.8 Enumeración del Sistema Comprometido

Ilustración 44. Comandos de enumeración ejecutados en el sistema Windows XP

El comando dir en la unidad C: revela la estructura básica del sistema, mostrando los directorios principales: "Archivos de programa" (donde está instalado BadBlue), "Documents and Settings" (que contiene los archivos camuflados creados anteriormente) y "WINDOWS" (directorio del sistema operativo)

Se ejecuta systeminfo para obtener información detallada del sistema, incluyendo versión del SO, parches instalados y configuración de hardware.

5.2.9 Análisis de Procesos en el Sistema Comprometido

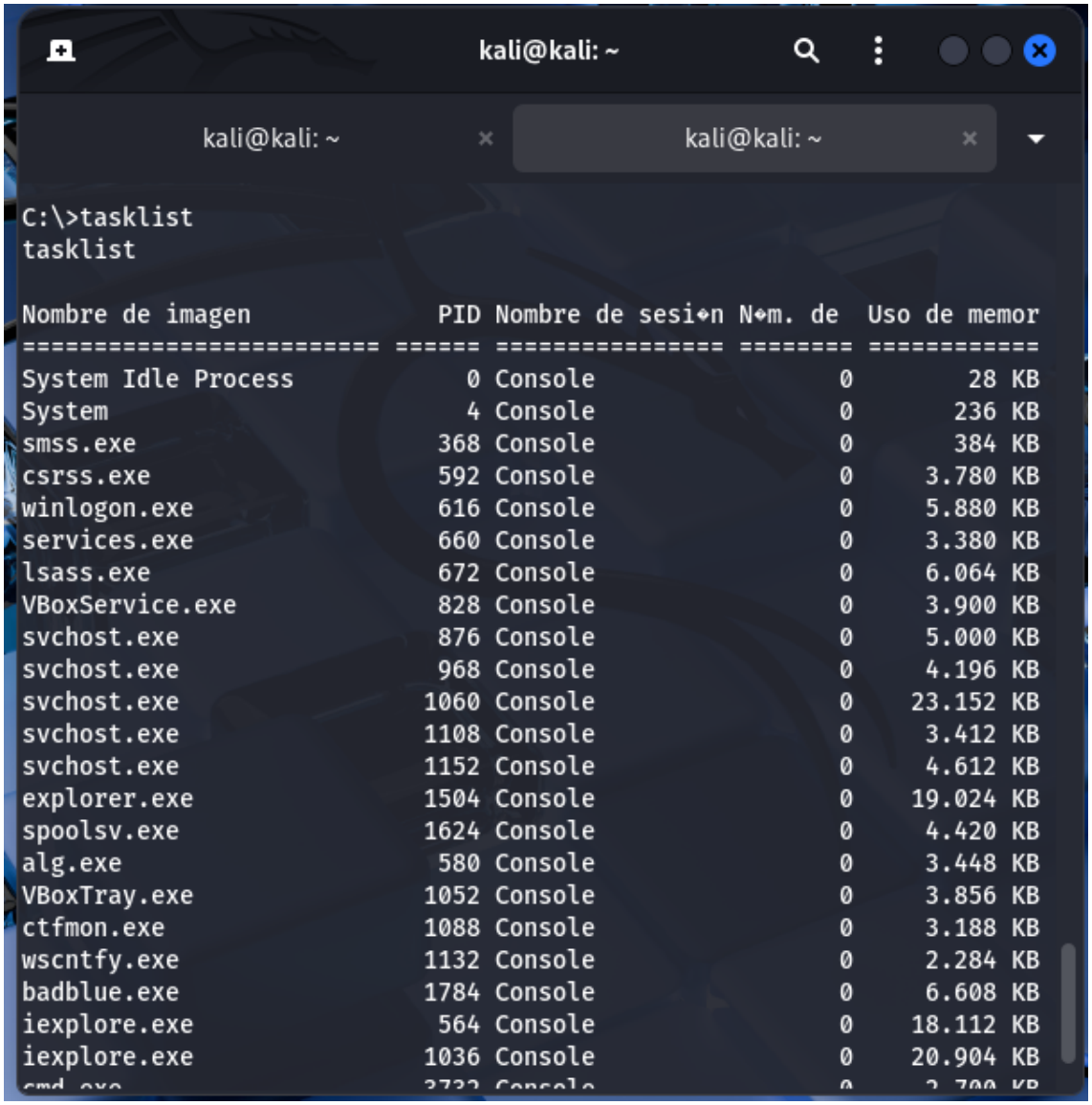

Ilustración 45. Lista de procesos en ejecución mediante tasklist

Se ejecuta el comando tasklist para analizar los procesos activos en el sistema Windows XP comprometido.

Ilustración 46. Salida de la configuración del sistema Windows XP víctima.

6. Problemas encontrados

- Dificultad para encontrar el payload correcto para explotar BadBlue, lo que generó varios intentos fallidos.
- Errores en la sintaxis de los comandos, lo que provocó respuestas inesperadas.
- Falta de claridad en algunos mensajes de error, lo que complicó la identificación de las causas reales de los fallos.

7. Recomendaciones

- Verificar sintaxis de comandos
- Anotar los comandos exitosos para replicarlos en futuros escenarios
- Probar comandos paso a paso
- leer los mensajes de error con atención

8. Conclusión

Concluyo diciendo que este laboratorio demostró la importancia de la seguridad mediante el análisis de técnicas de camuflaje en archivos y la explotación de vulnerabilidades. Se comprobó que formatos comunes como JPG, PDF, Word y Excel pueden ser utilizados para ocultar información, mientras que la explotación de BadBlue evidenció los riesgos de servicios no actualizados.

9. Bibliográfica

Rafael Sandoval Morales (2025). EXPLOTACION DE BADBLUE Y CAMUFLAJE DE ARCHIVOS DESDE LA MAQUINA VIRTUAL DE WINDOWS XP