Universidad Tecnológica del Chocó
Diego Luis Córdoba

INFORME SOBRE LA EXPLOTACIÓN DE BADBLUE Y EL CAMUFLAJE DE ARCHIVOS

JOHAN CAMILO GARCIA CARO

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA

INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA

IX-NIVEL

SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE IMÁGENES

INTRODUCCIÓN

Este informe aborda el análisis de vulnerabilidades en sistemas que ejecutan el servicio BadBlue, así como el uso de técnicas de camuflaje de archivos como mecanismo de ocultamiento digital. En un entorno de laboratorio controlado, se simularon escenarios de explotación y manipulación de archivos para evaluar el impacto potencial sobre la seguridad de la información. Este estudio combina prácticas de auditoría de red, análisis de exploits y esteganografía aplicada, con el fin de identificar riesgos técnicos y operativos que comprometen la integridad de los sistemas.

RESUMEN

Durante la práctica se detectó la presencia activa del servicio BadBlue en un host objetivo, confirmando su versión vulnerable (2.7/2.72). Se localizó un exploit público asociado (EDB-4784) y se ejecutó en condiciones controladas, logrando acceso remoto al sistema. Paralelamente, se identificó el uso de herramientas de camuflaje que permiten incrustar archivos sensibles dentro de formatos comunes como imágenes, documentos y hojas de cálculo. Esta combinación de vulnerabilidades y técnicas de ocultamiento representa un riesgo significativo para la detección forense y la protección de activos digitales.

PALABRAS CLAVE

Badblue, Exploit, Camuflaje, análisis, archivos

OBJETIVO GENERAL

Analizar el comportamiento del servicio BadBlue frente a vulnerabilidades conocidas y evaluar el impacto del camuflaje de archivos como técnica de ocultamiento en sistemas comprometidos.

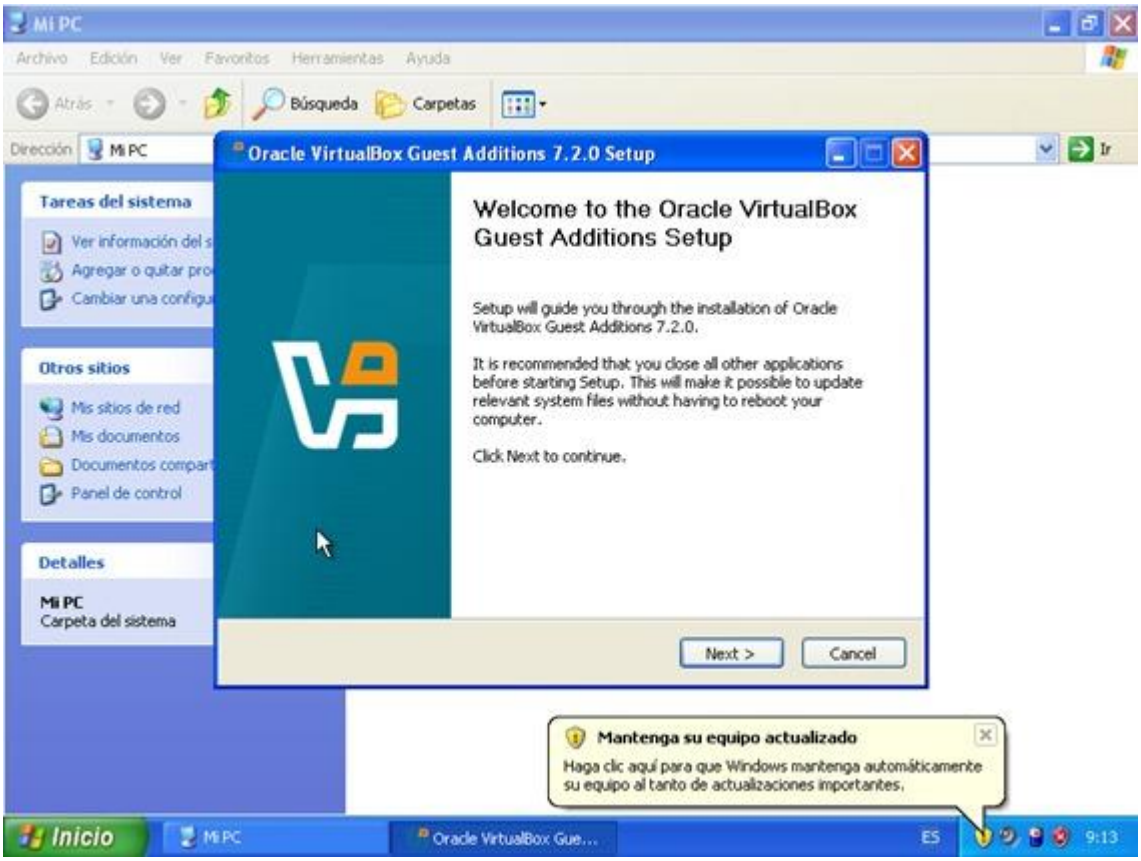
OBJETIVOS ESPECÍFICOS

- Detectar y validar la versión del servicio BadBlue en el entorno de prueba.
- Identificar y documentar exploits públicos aplicables a dicha versión.
- Ejecutar pruebas controladas de explotación y registrar evidencia técnica.
- Evaluar el uso de herramientas de camuflaje sobre distintos tipos de archivos

1. DESARROLLO

A continuación, se documenta el procedimiento seguido para crear la carpeta compartida e instalar los programas. Y camuflar archivos.

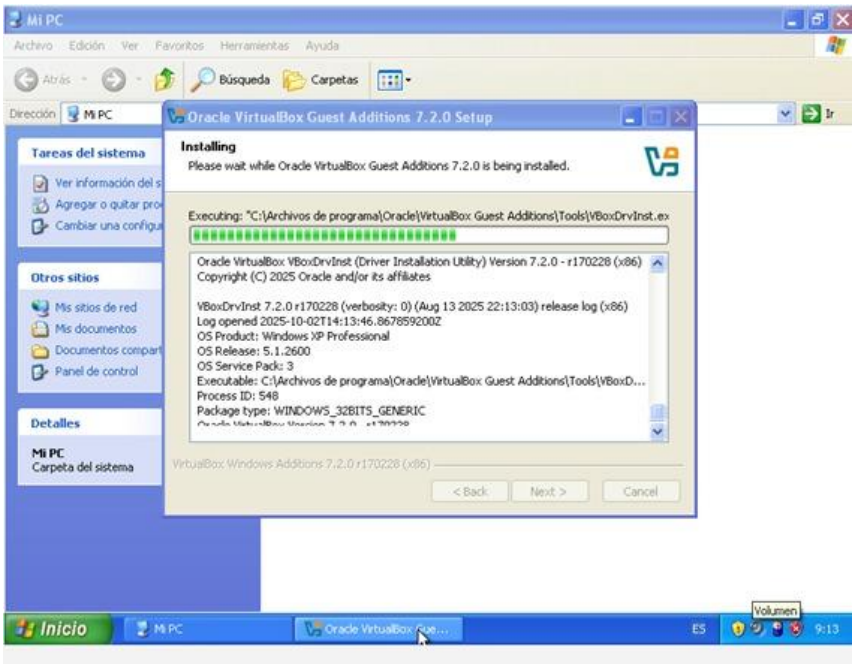
Este paso da la bienvenida al asistente de instalación, indicando que el proceso guiará al usuario para agregar los complementos de VirtualBox Guest Additions. Estos complementos mejoran el rendimiento y la integración entre el sistema anfitrión y la máquina virtual (por ejemplo, mejor resolución de pantalla, carpetas compartidas y sincronización del portapapeles).



imagenes 1 asistente de instalacion

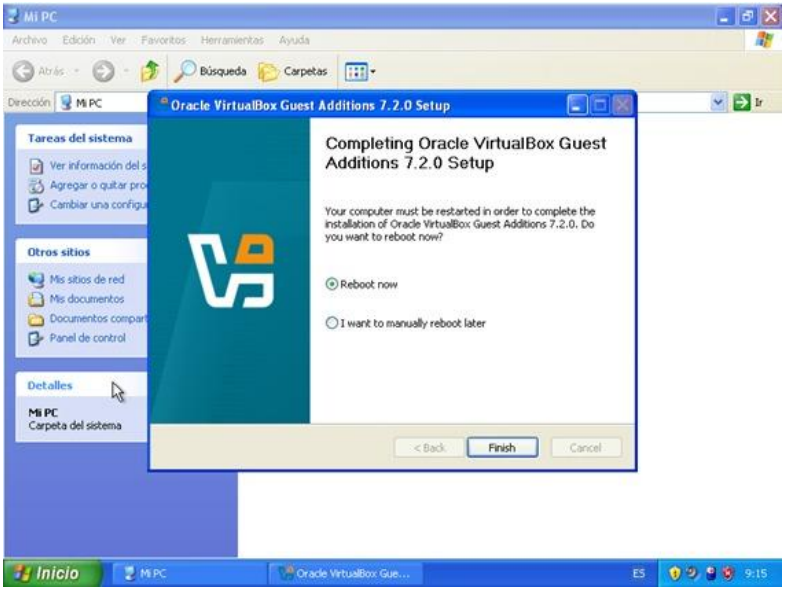
el instalador está **copiando y configurando los archivos necesarios** para integrar los controladores y servicios de VirtualBox Guest Additions. Estos componentes permiten

que la máquina virtual funcione de forma más fluida y sincronizada con el sistema anfitrión.



imagenes 2 compilador

Compilación completada

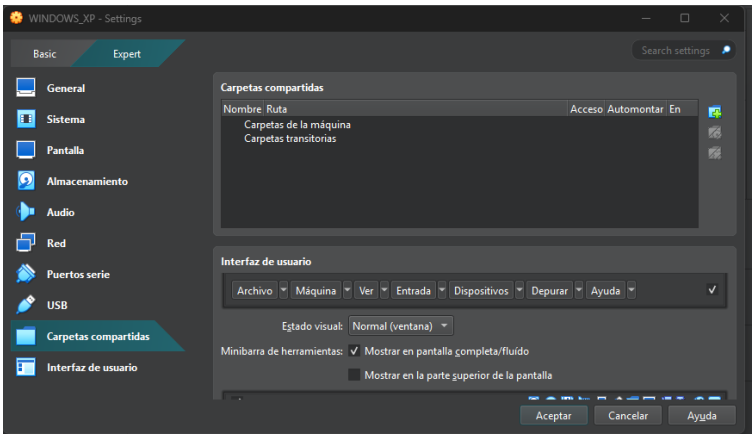


imagenes 3 compilación completada

2. CREACION DE LA CARPETA COMPARTIDA

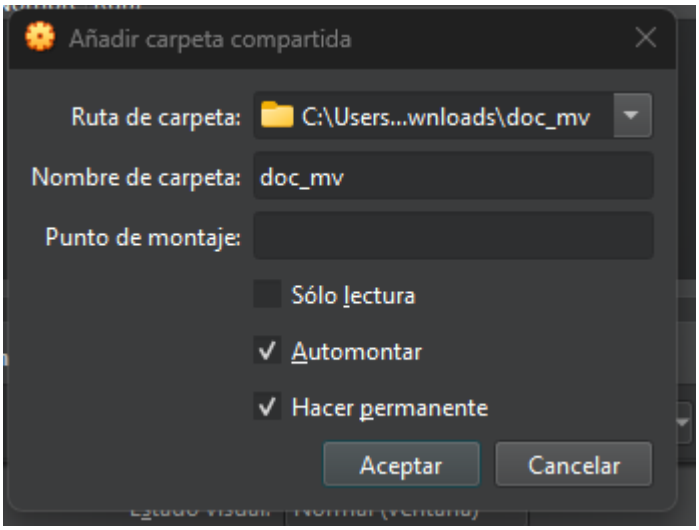
Ruta de la carpeta y nombre

En este paso se selecciona la carpeta con el signo más (+) para la creacion de la carpeta.



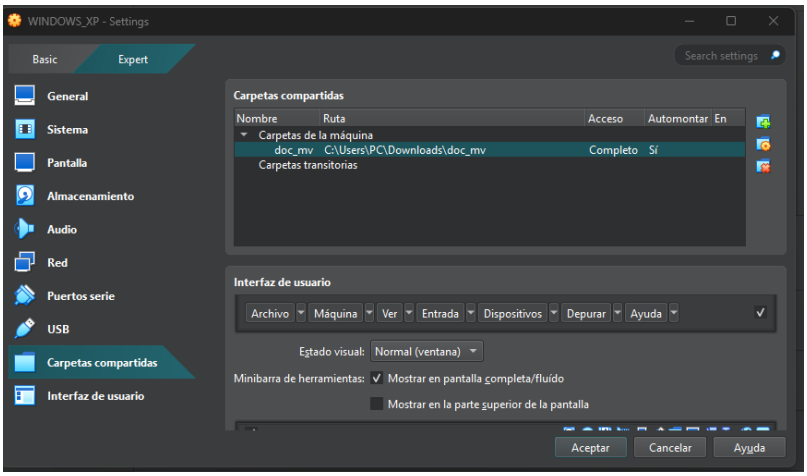
imagenes 4 paso 1 para la creacion de la carpeta compartida

Ruta y nombre de la carpeta

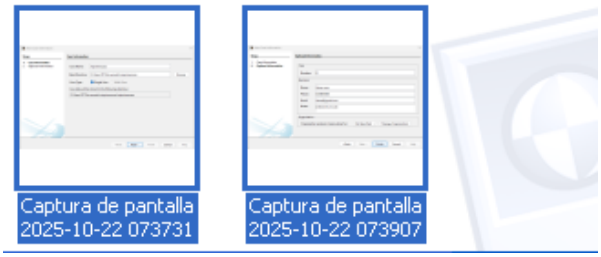


imagenes 5 ruta y nombre de la carpeta

Selecion de la carpeta compartida



imagenes 6 selecion de la carpeta

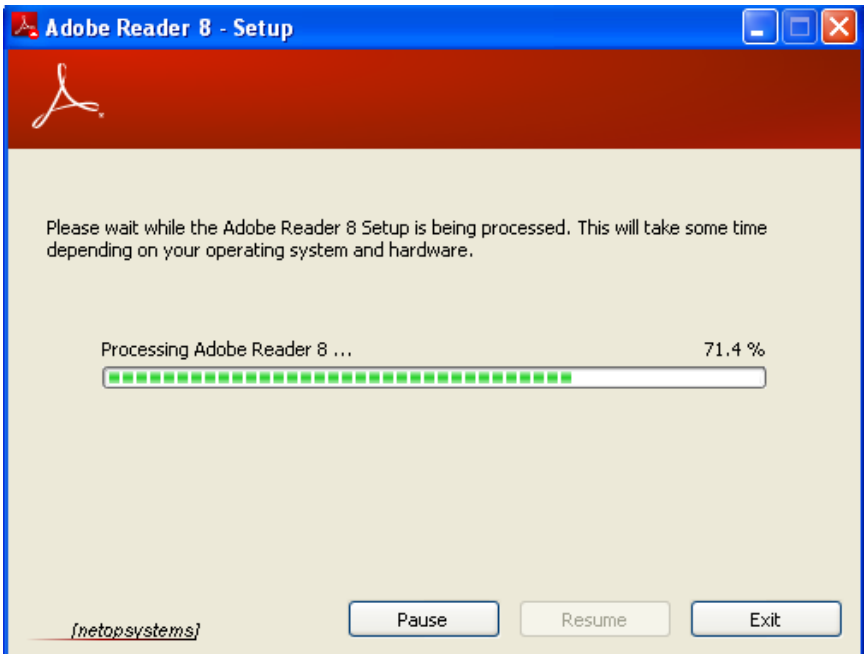


imagenes 7 información de la carpeta compartida

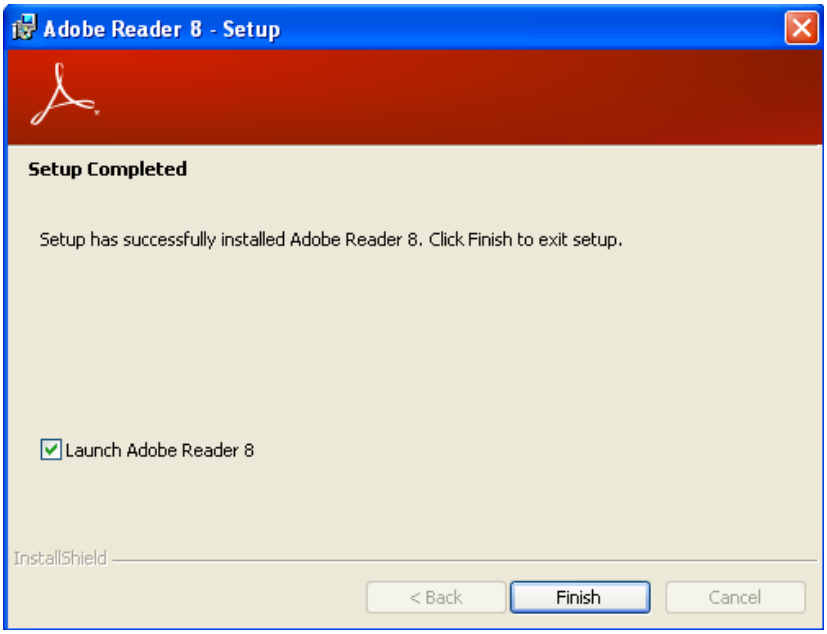
3. INSTALACION DE LAS APLICACIÓNES

INSTALACION DE ADOBE

Adobe sirve para crear, editar y gestionar contenido digital en diferentes formatos,



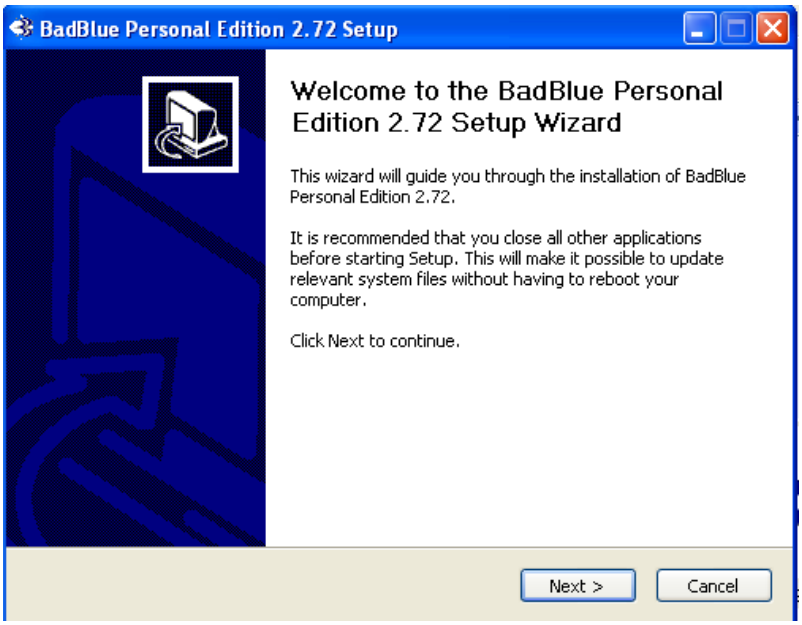
imagenes 8 proceso de instalacion



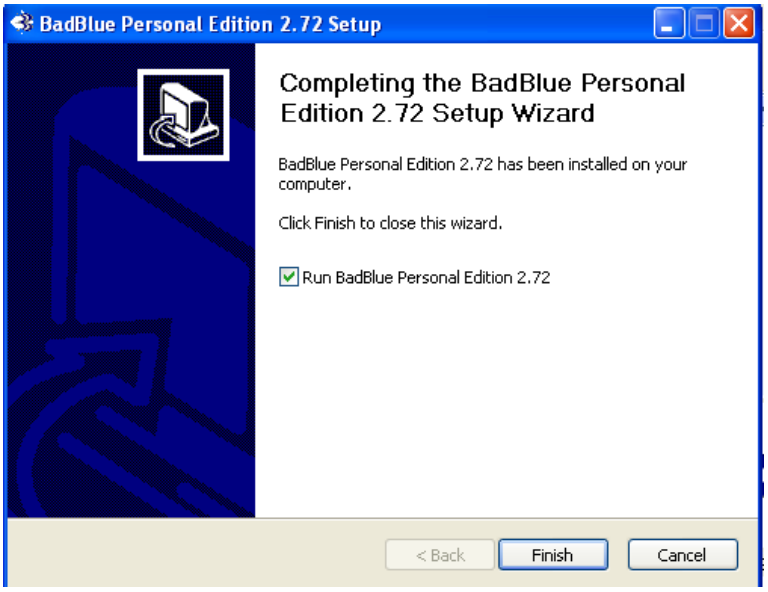
imagenes 9 instalacion terminada de adobe

INSTALACION DE BADBLUE

Badblue sirve para **convertir un computador en un pequeño servidor web o de archivos**, útil para compartir recursos o practicar conceptos de administración web y redes.



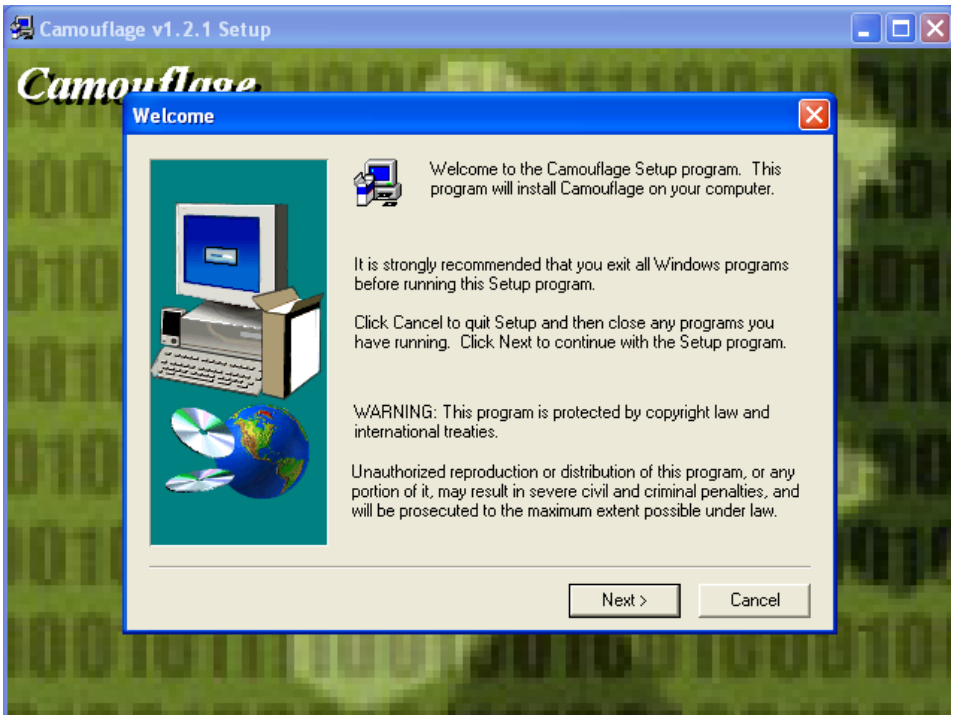
imagenes 10 instalacion de badblue



imagenes 11 instalacion completada de badblue

INSTALACION DE CAMOUFLAJE

Camouflaje sirve para **proteger y ocultar archivos sensibles o personales**, utilizando técnicas de **esteganografía** (ocultar información dentro de otro medio). Es útil para seguridad básica o para evitar que otros vean archivos confidenciales.



imagenes 12 instalacion de camouflaje

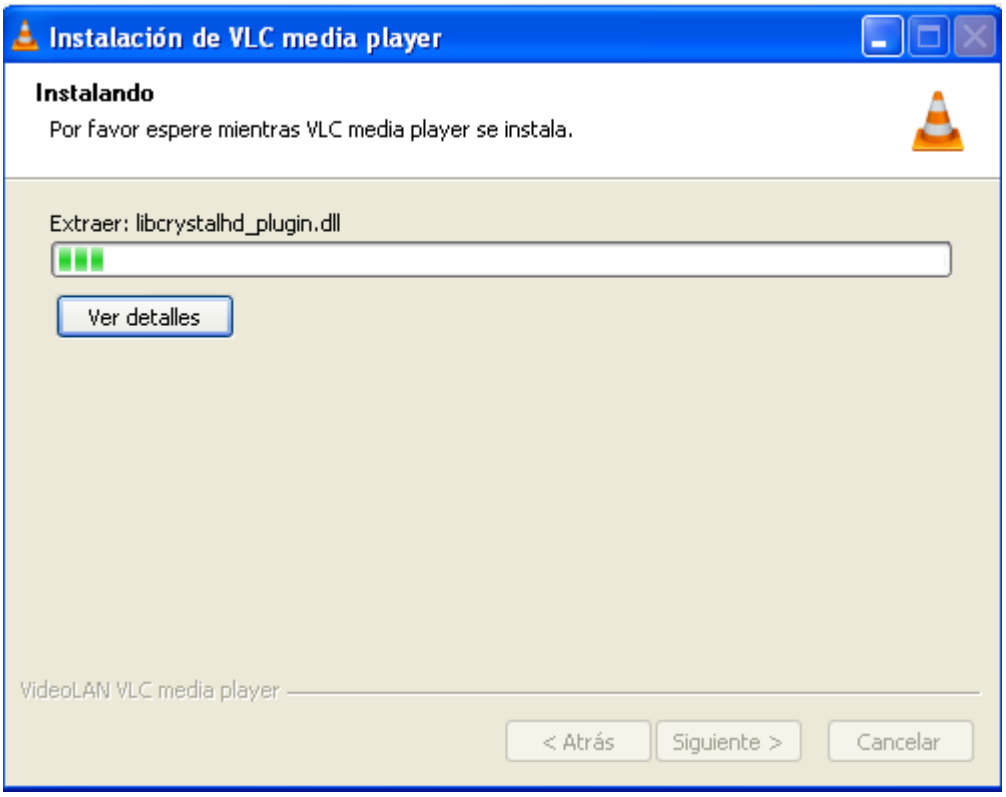
INSTALACION DE INTERNET EXPLORE

Internet Explorer sirve para conectarse y navegar por Internet, accediendo a información, servicios y aplicaciones en línea.

imagenes 13 instalacion de internet explore

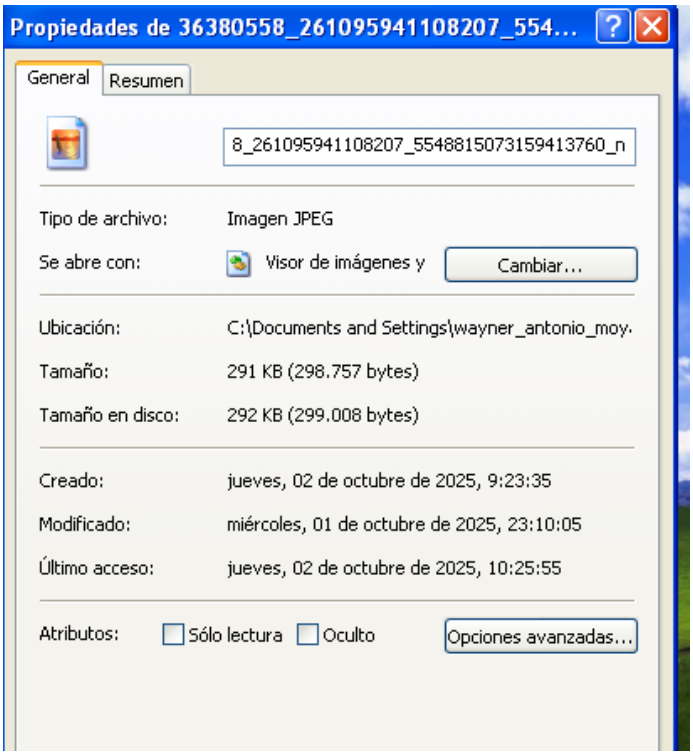
instalacion de vlc media player

VLC Media Player sirve para reproducir, transmitir y convertir archivos **multimedia**, ofreciendo compatibilidad con casi todos los formatos existentes y herramientas avanzadas de control de audio y video.



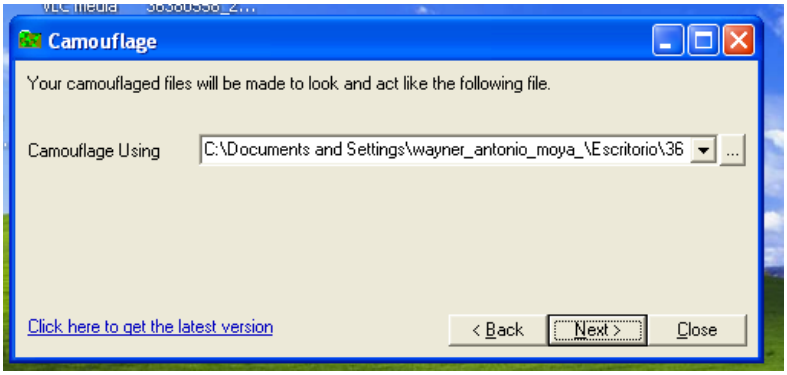
imagenes 14 instalacion de vlc media player

propiedades de un archivo jpg



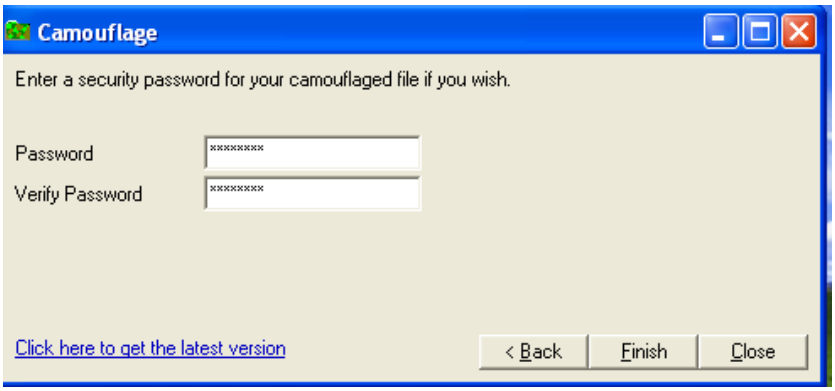
imagenes 15 propiedades de un archivo jpg antes de camuflar

Camuflaje de archivos jpg, docx, pdf



imagenes 16 dirección del archivo donde se va a camuflar

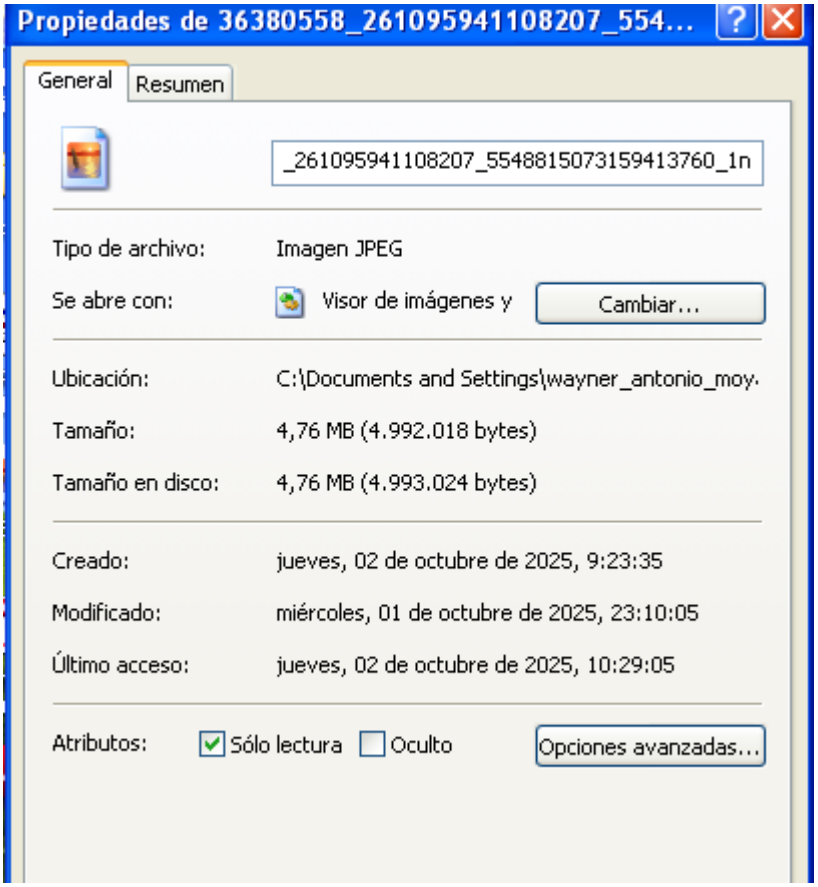
Contraseña del camuflaje



imagenes 17 contraseña

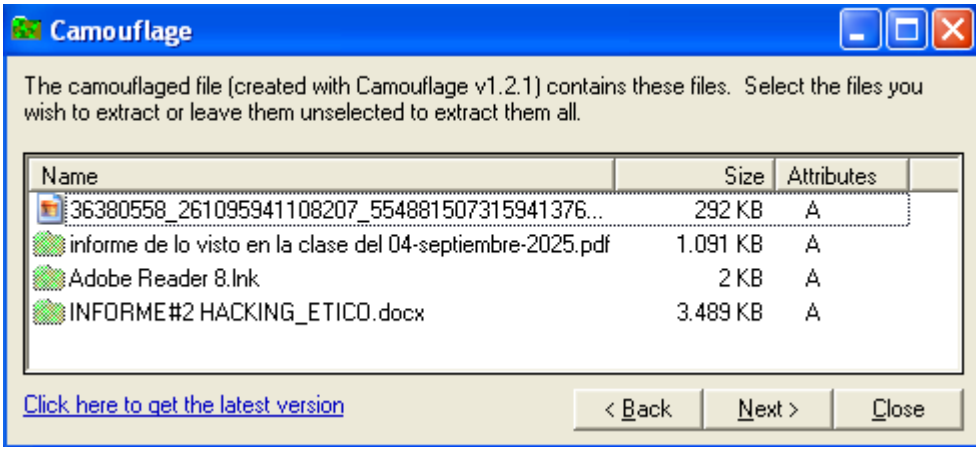
propiedades del archivo ya camuflado

aquí en este paso se nota el cambio en el tamaño



imagenes 18 propiedades del archivo camuflado

en este paso se muestra los archivos camuflados



imagenes 19 archivos camuflados

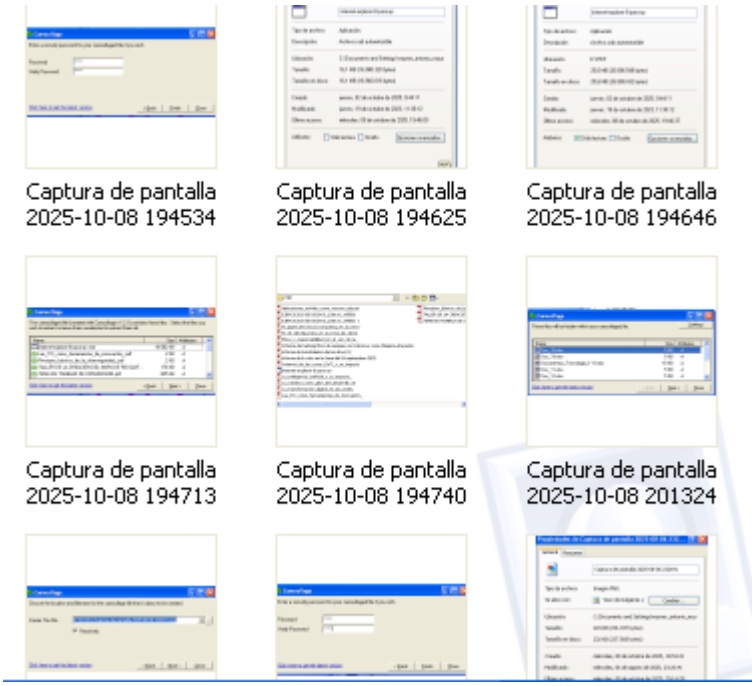
4. CAPITULO #1

En este paso de camuflo archivos (jpg, doc., xlsx, pdf)

5. CAMUFLAJE DE LOS ARCHIVOS .JPG

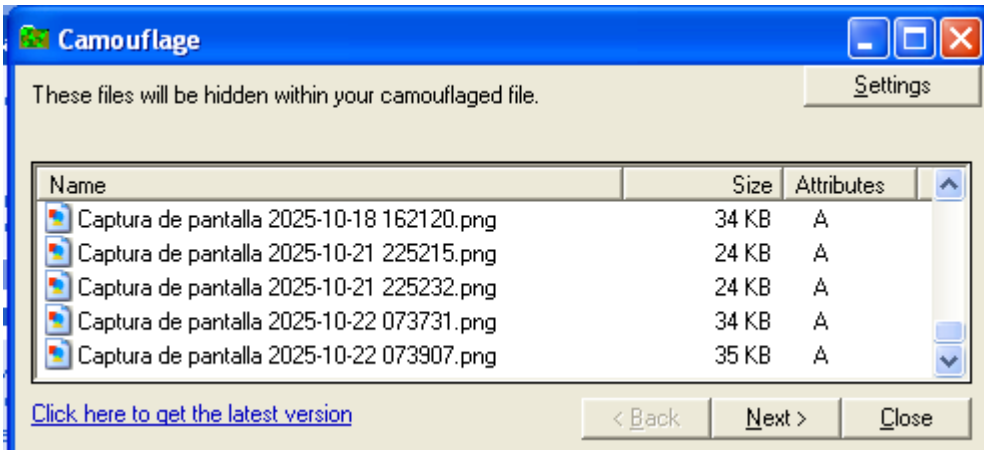
En este paso se muestra un numero de archivos jpg para su post camuflaje.

en este caso se seleccionaron 152 archivos para camuflar y no los acepto después se utilizaron 30 y los acepto.



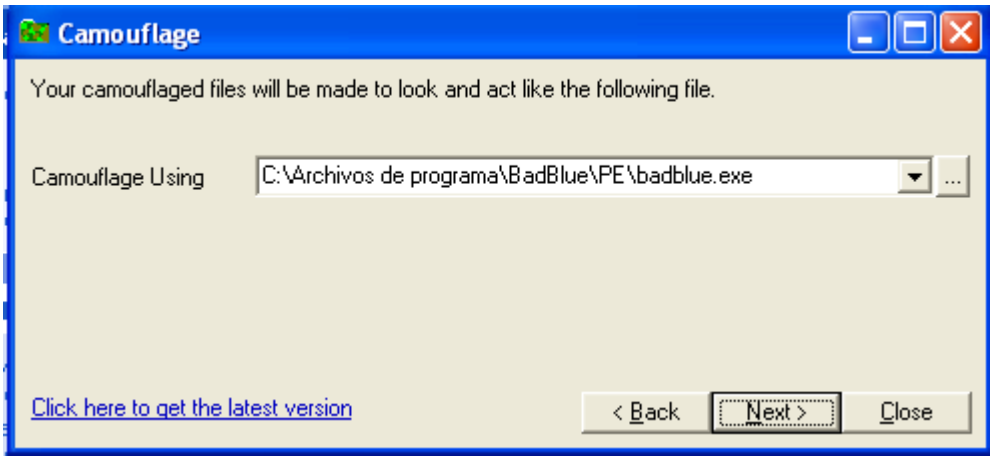
imagenes 20 archivos jpg

en este paso se selecciona todos los archivos que se van a camuflar

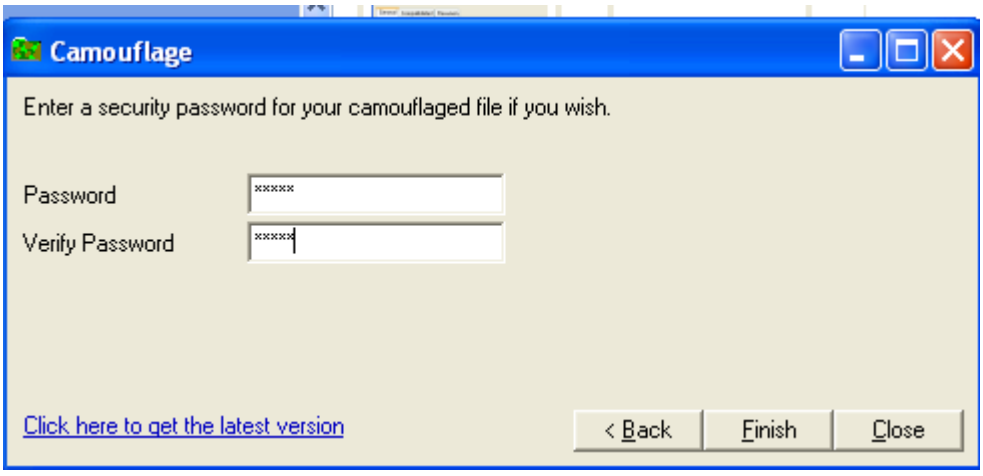


imagenes 21 archivos jpg para su post camuflaje

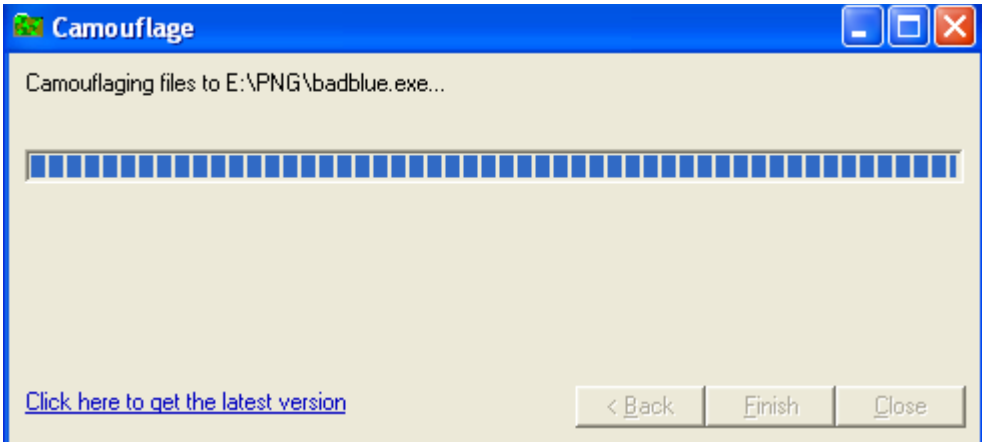
en este paso se selecciona el archivo donde se va a camuflar en este caso se eligió badblue



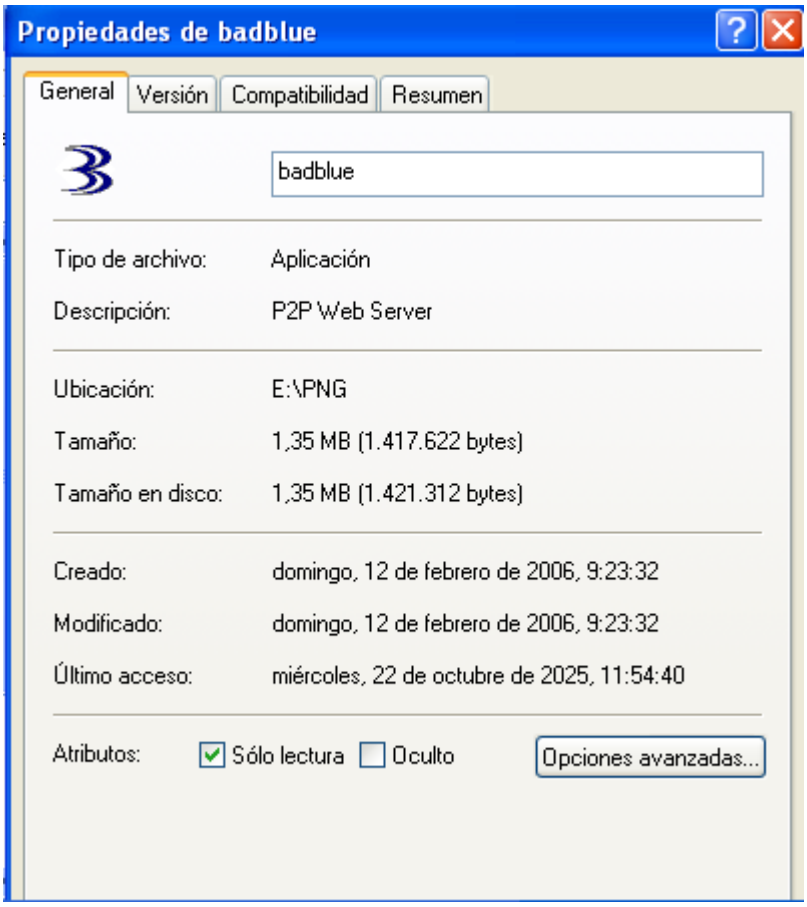
imagenes 22 selecion del archivo donde se va a camuflar

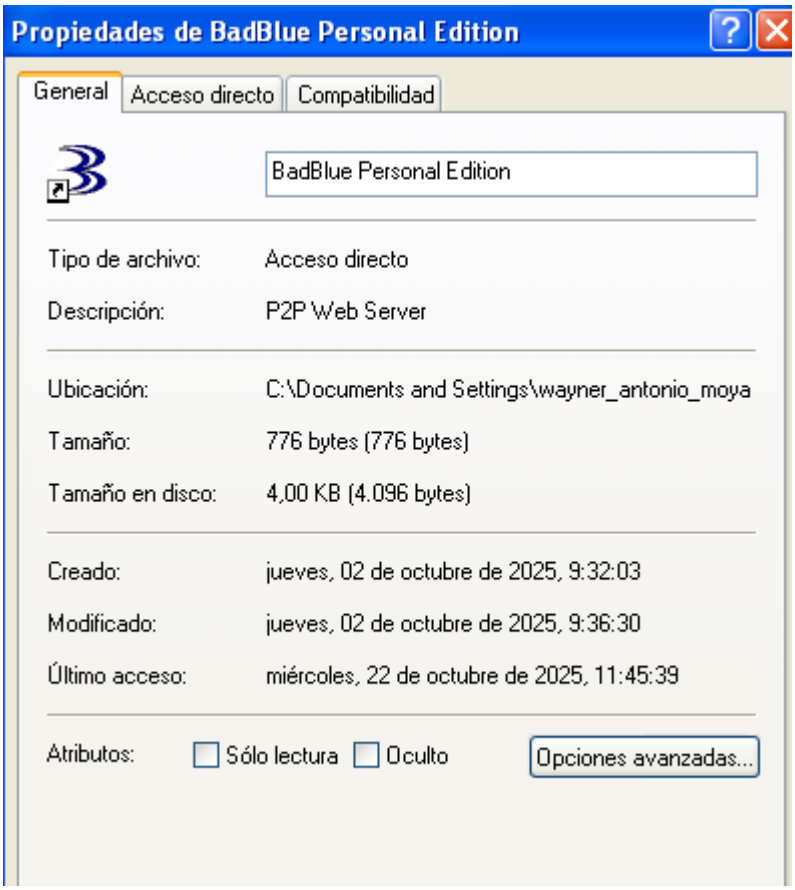


imagenes 23 configuracion de contraseña



imagenes 24 propiedades de vlc media player antes del camuflaje


Propiedades de badblue
General
Versión
Compatibilidad
Resumen
badblue
Tipo de archivo: Aplicación
Descripción: P2P Web Server
Ubicación: E:\PNG
Tamaño: 1,35 MB (1.417.622 bytes)
Tamaño en disco: 1,35 MB (1.421.312 bytes)
Creado: domingo, 12 de febrero de 2006, 9:23:32
Modificado: domingo, 12 de febrero de 2006, 9:23:32
Último acceso: miércoles, 22 de octubre de 2025, 11:54:40
Atributos: Sólo lectura Oculto
Opciones avanzadas...

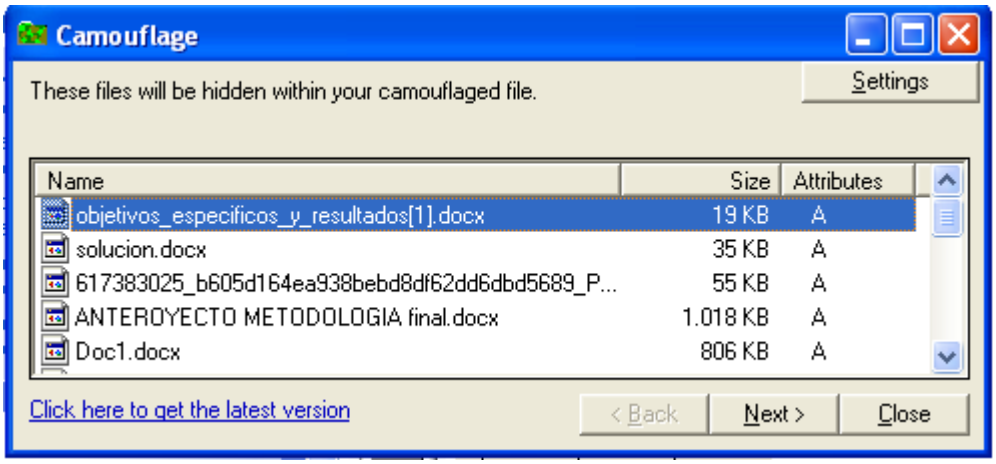


imagenes 25 propiedades de vlc media después del camuflaje

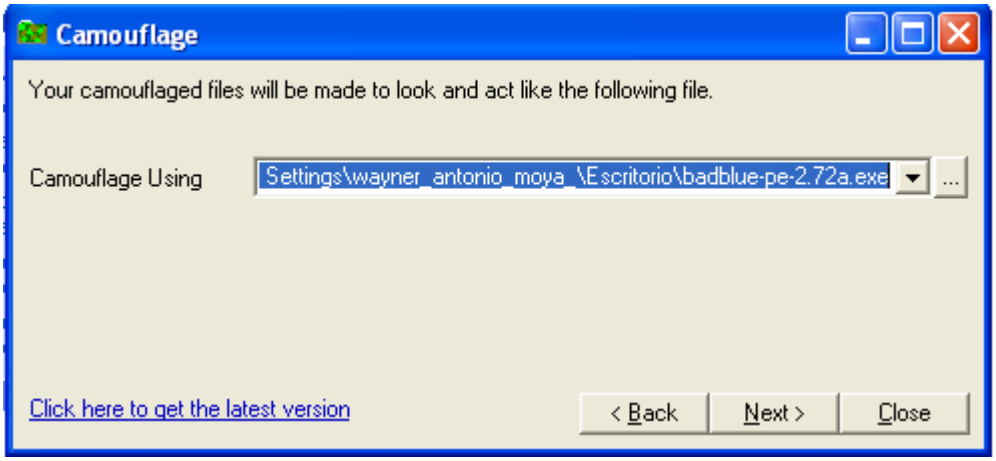
6. CAMUFLAJE DE LOS ARCHIVOS .DOC

En este paso se muestra un numero de archivos doc. para su post camuflaje.

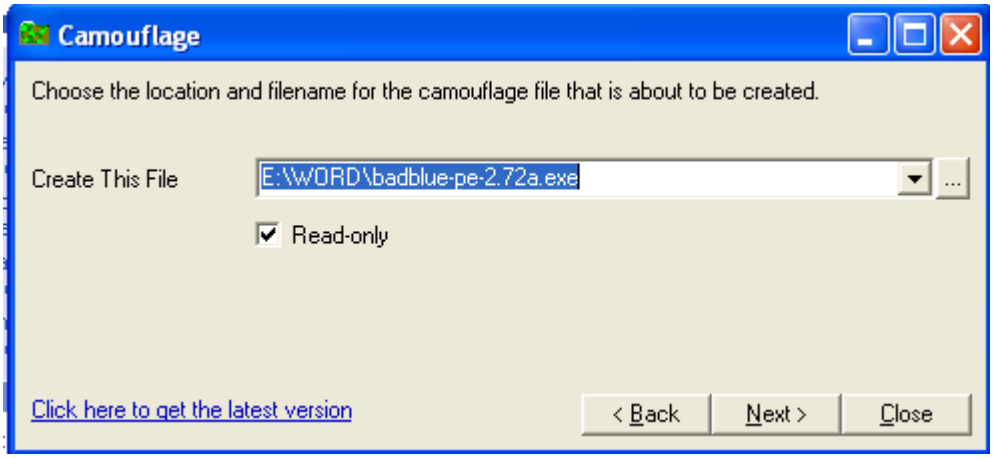
en este caso se seleccionaron 20 archivos.



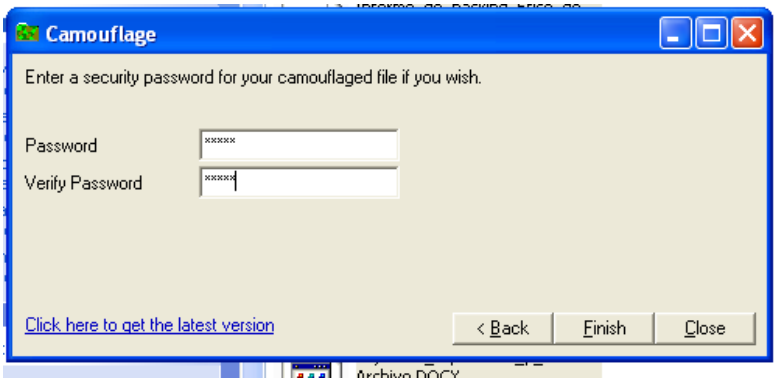
imagenes 26 archivos doc.



imagenes 27 dirección donde quedara el camuflaje de los archivos

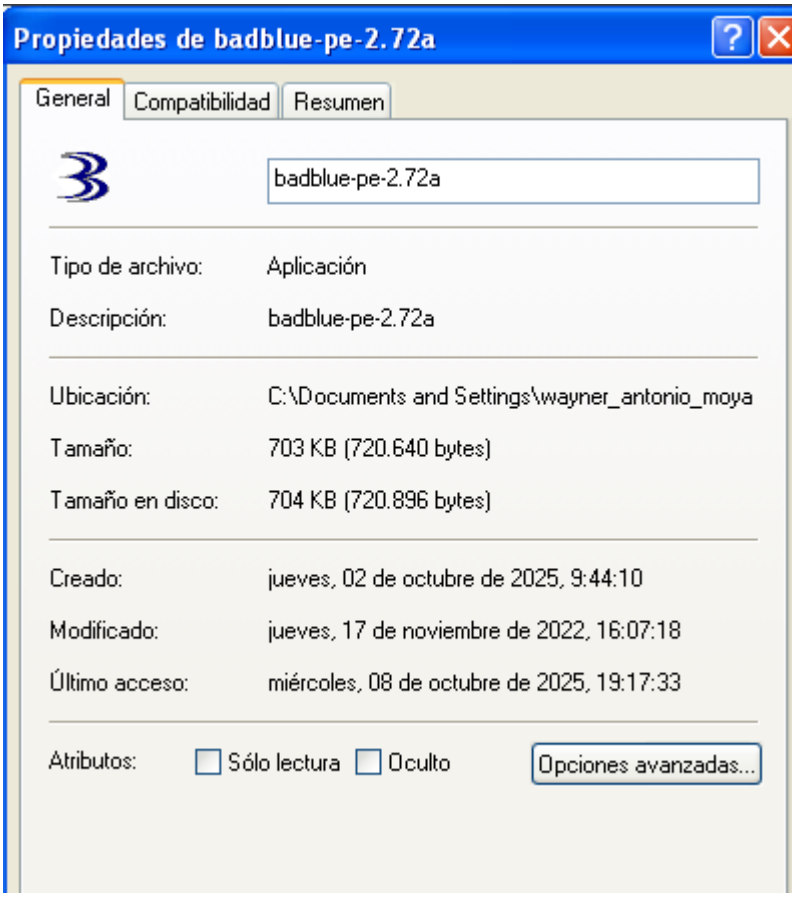


imagenes 28 archivo donde se camuflara los documentos

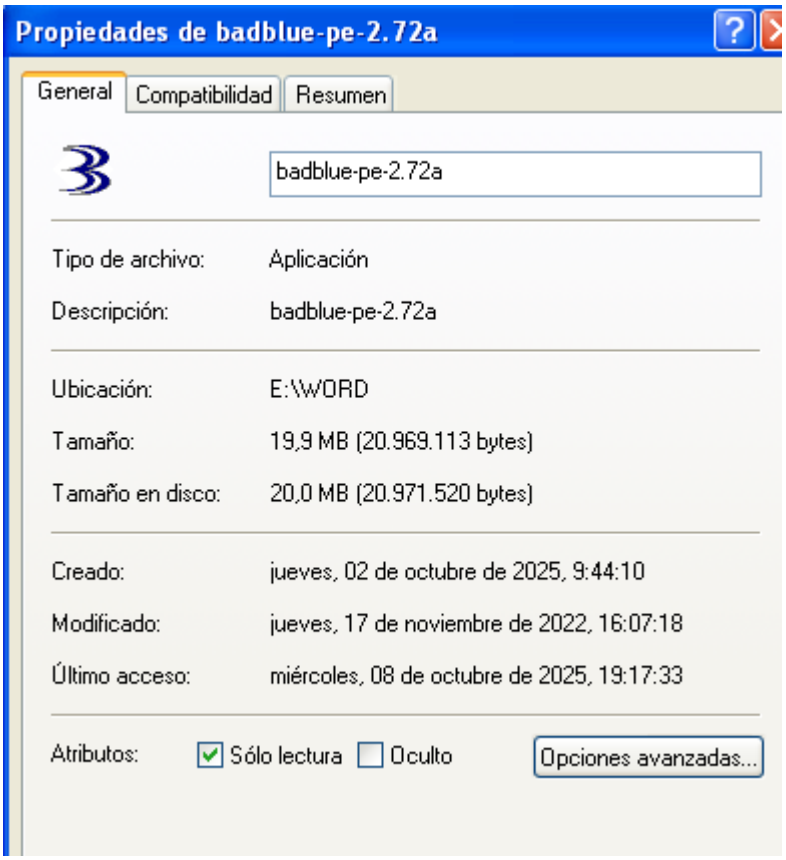


imagenes 29 contraseña del camuflaje

propiedades del archivo donde se camuflara los documentos



imagenes 30 propiedades del archivo

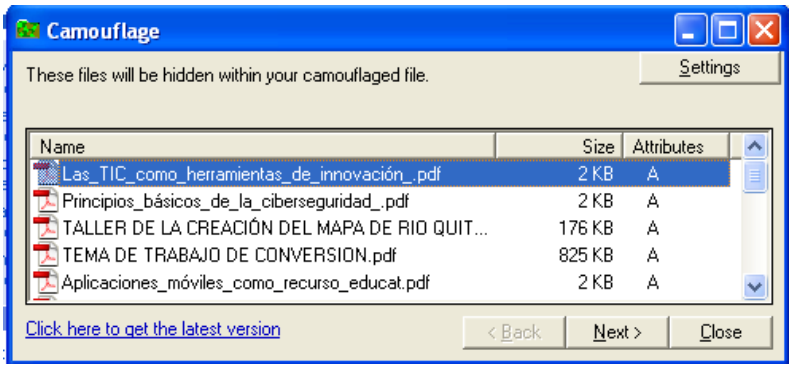


imagenes 31 propiedades post camuflaje

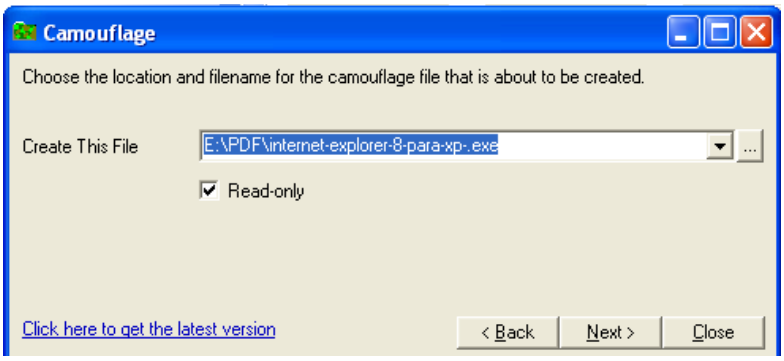
7. CAMUFLAJE DE LOS ARCHIVOS PDF

En este paso se muestra un numero de archivos pdf para su post camuflaje.

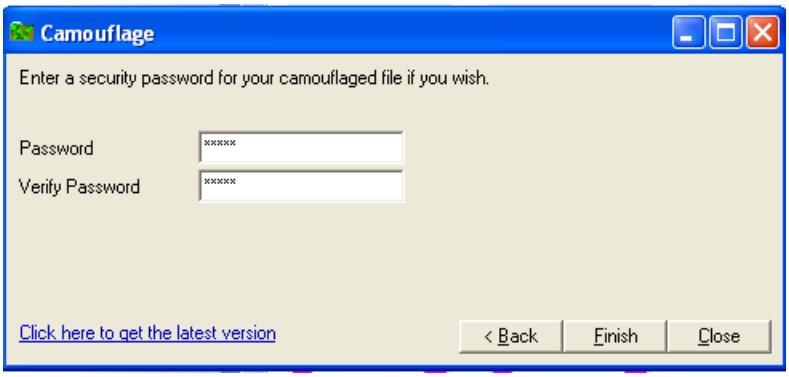
en este caso se seleccionaron 20 archivos.



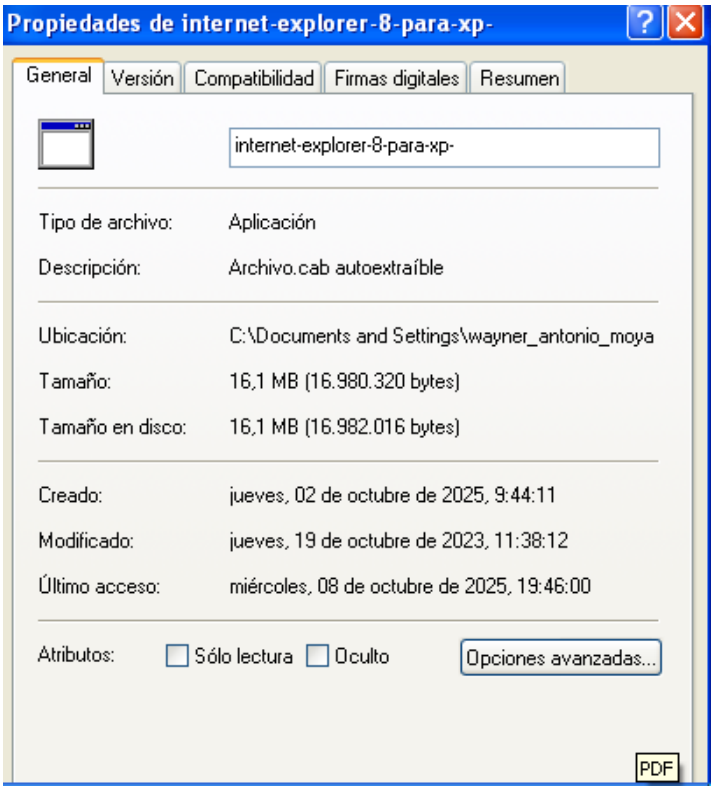
imagenes 32 archivos pdf



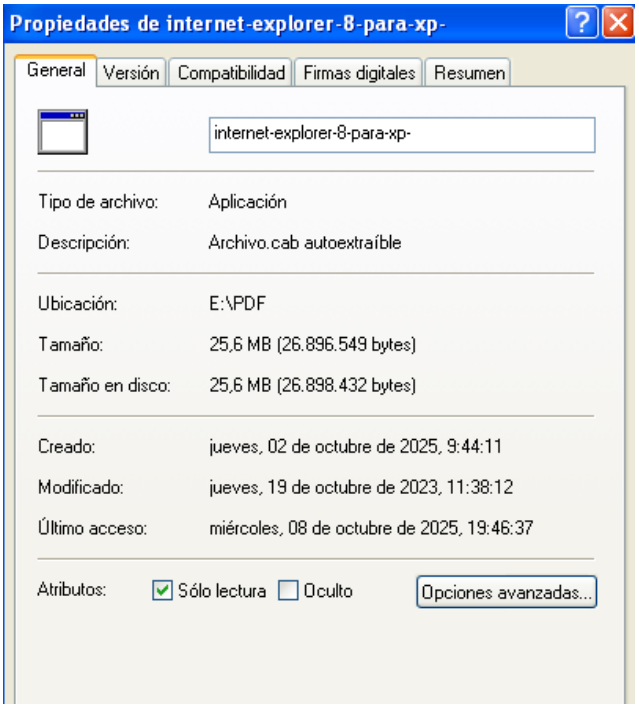
imagenes 33 dirección donde se ubicara los archivos



imagenes 34 contraseña de los archivos camuflados



imagenes 35 propiedades de internet antes del camuflaje

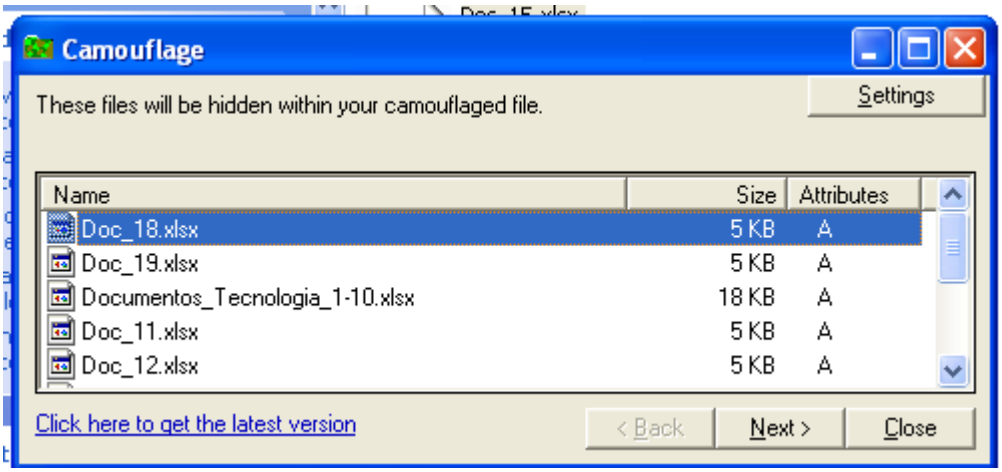


imagenes 36propiedades de internet post camuflaje

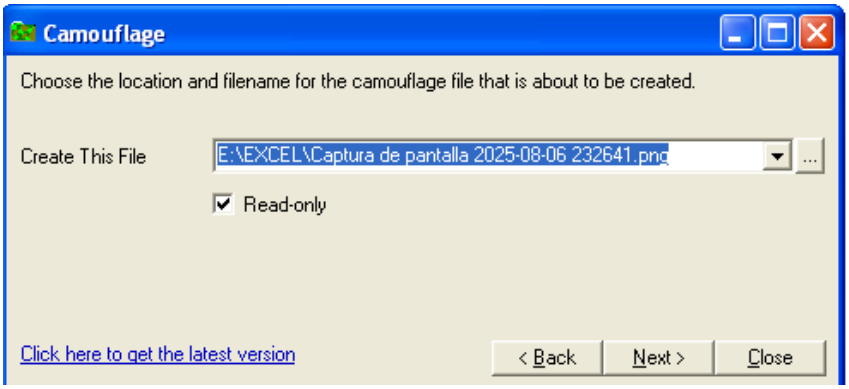
8. CAMUFLAJE DE LOS ARCHIVOS XLSX

En este paso se muestra un numero de archivos xlsx para su post camuflaje.

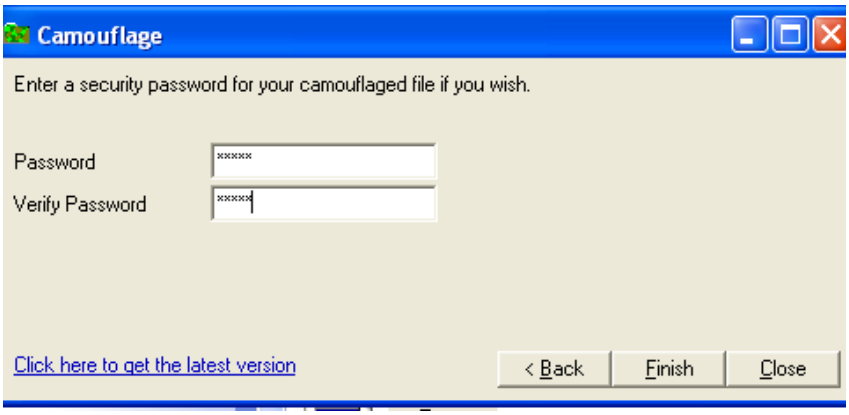
en este caso se seleccionaron 10 archivos.



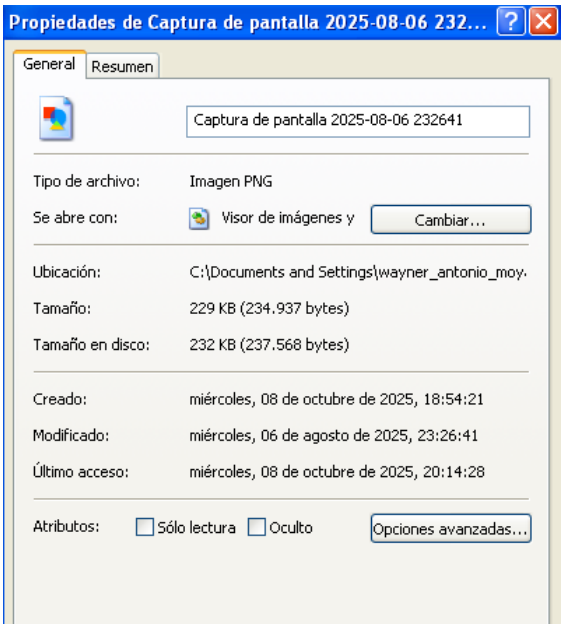
imagenes 37 archivos xlsx



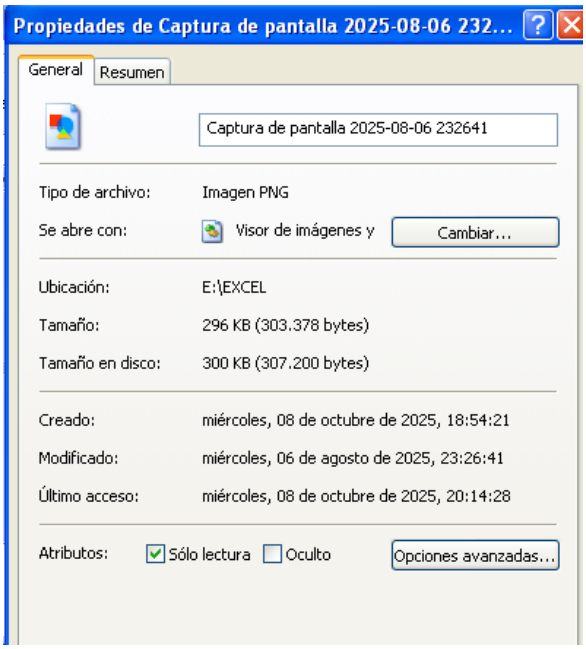
imagenes 38 dirección del camuflaje



imagenes 39 contraseña de los archivos camuflados



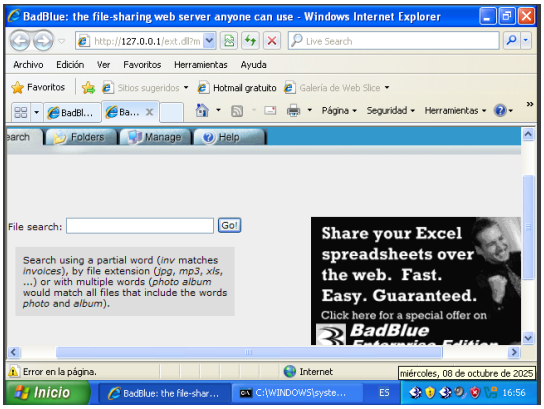
imagenes 40 propiedades del archivo antes del camuflaje



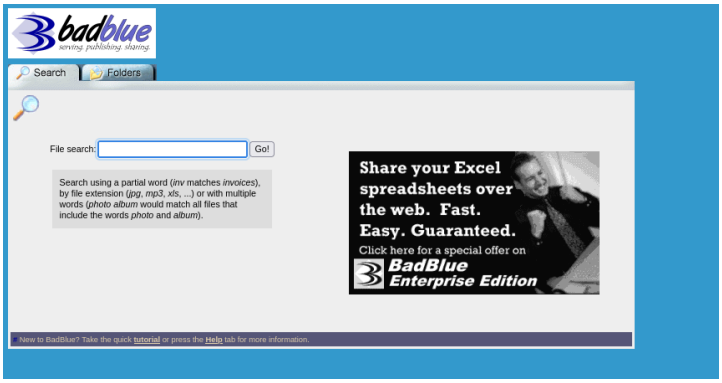
imagenes 41 propiedades del archivo post camuflaje

9. CAPITULO #2 INGRESANDO A EL SISTEMA DE BADBLUE

BadBlue es una aplicación que convierte un computador en un servidor web ligero, permitiendo compartir archivos (especialmente hojas de cálculo Excel) a través de la red local o internet. Es útil para pruebas de red, administración de recursos compartidos y análisis de vulnerabilidades.

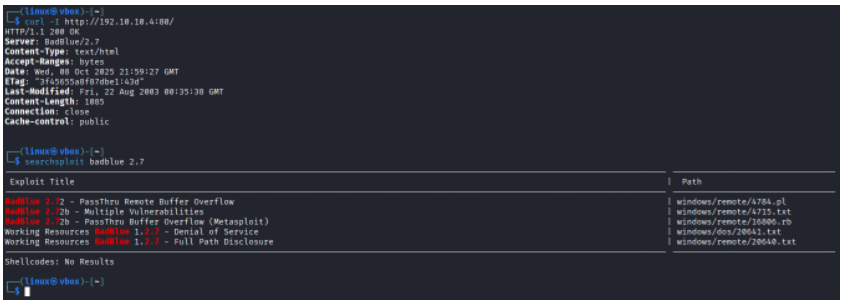


imagenes 42 aplicación badblue



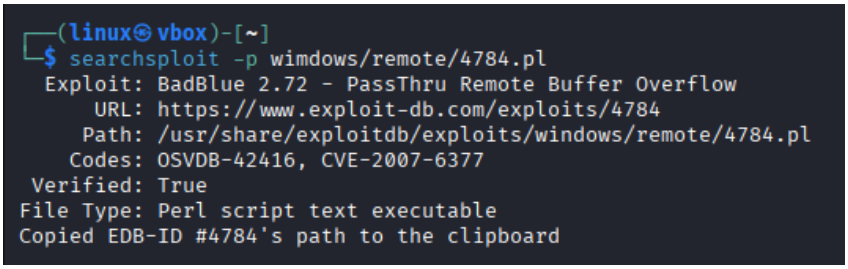
imagenes 43 interfaz de la aplicación badblue desde Linux

en este paso Se verificó la presencia del servicio BadBlue en el host mediante una solicitud HTTP (curl), confirmando que el servidor responde con el banner BadBlue/2.7. Posteriormente se ejecutó Searchsploit para identificar exploits públicos asociados a esa versión. Los resultados muestran varias vulnerabilidades conocidas para BadBlue 2.7



imagenes 44 identificación de exploit

En este paso se utilizó el comando Searchsploit -p windows/remote/4784.pl para examinar un exploit específico relacionado con el software Badblue versión 2.72. El resultado muestra un exploit catalogado como “PassThru Remote Buffer Overflow”, el cual está disponible en la base de datos de Exploit-DB bajo el EDB-ID #4784.

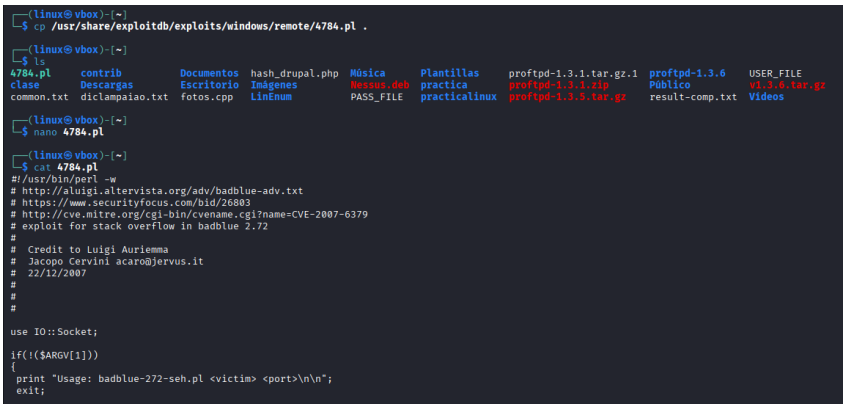


imagenes 45 busqueda del exploit

En este paso se copió el archivo del exploit correspondiente a BadBlue 2.72 desde la base de datos local de Exploit-DB hacia el directorio de trabajo, utilizando el comando cp. Posteriormente, se verificó su presencia mediante ls y se procedió a abrirlo con nano y visualizarlo con cat para revisar su contenido.

El archivo, identificado como 4784.pl, es un script en lenguaje Perl que contiene referencias a fuentes oficiales de vulnerabilidades (como SecurityFocus y CVE-2007-6377) y créditos a los investigadores Luigi Auriemma y Jacopo Cervini, autores del hallazgo documentado el 22 de diciembre de 2007.

Este análisis permitió confirmar la autenticidad y naturaleza del exploit, el cual está diseñado para aprovechar una vulnerabilidad de desbordamiento de búfer (Buffer Overflow) en el servicio BadBlue versión 2.72.

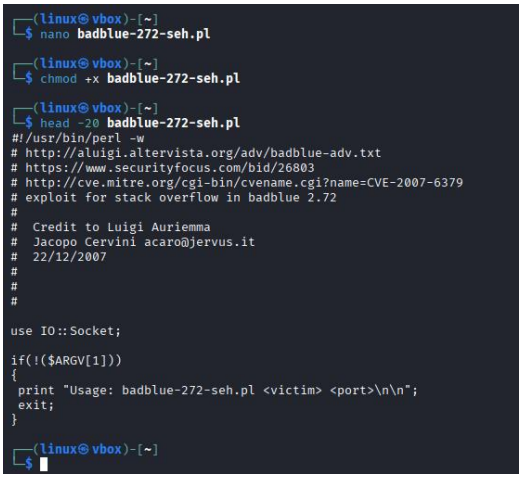


imagenes 46 exploit correspondiente

Se abrió el archivo badblue-272-seh.pl para edición/visualización (nano).

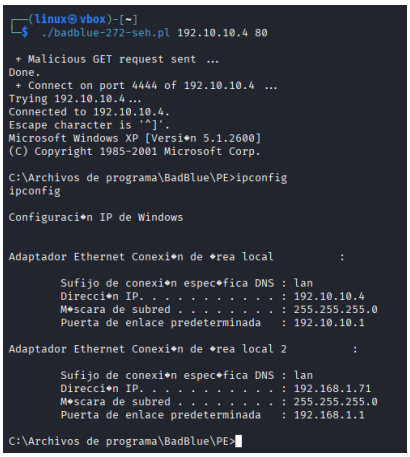
Se otorgaron permisos de ejecución al script (chmod +x badblue-272-seh.pl).

Se inspeccionaron las primeras líneas del archivo (head -20 badblue-272-seh.pl) para revisar encabezados, referencias y uso.



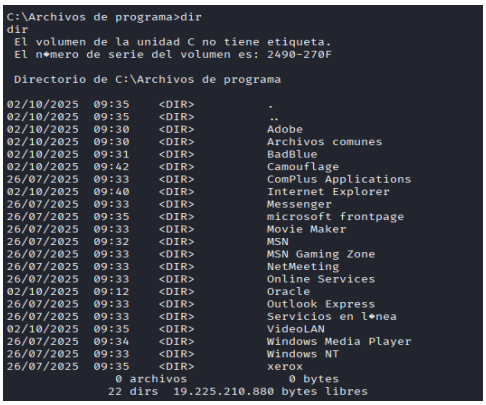
imagenes 47 inspección del archivo badblue

Se ejecutó el exploit badblue-272-seh.pl contra el host 192.10.10.4 (puerto 80). El exploit estableció una conexión remota (se muestra intento/establecimiento de conexión al puerto 4444 del objetivo) y proporcionó acceso a una consola del sistema remoto (prompt de Windows XP visible).



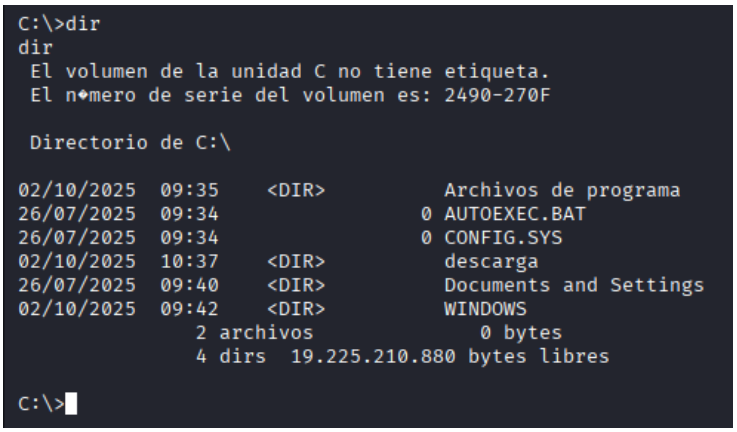
imagenes 48 ejecucion del exploit

En este paso Se muestra el resultado del comando dir ejecutado en C:\Archivos de programa sobre un sistema Windows (presumiblemente Windows XP). El listado presenta carpetas correspondientes a múltiples aplicaciones instaladas en el equipo.



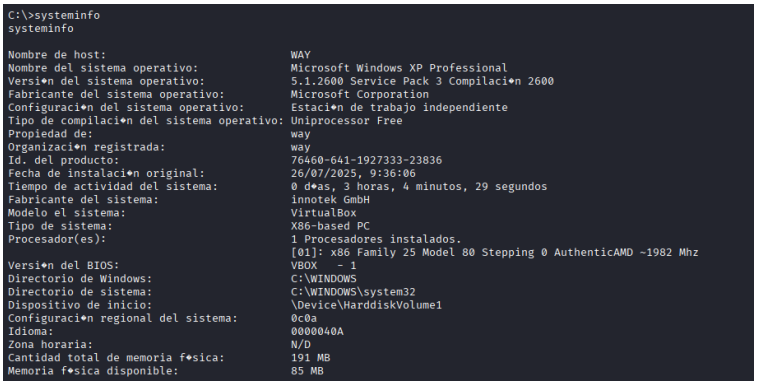
imagenes 49 comando dir

En este paso se hace la ejecución del comando dir en el directorio raíz **C:** del sistema operativo Windows. Este comando permite listar los archivos y carpetas principales del disco local, mostrando así la estructura básica del sistema.

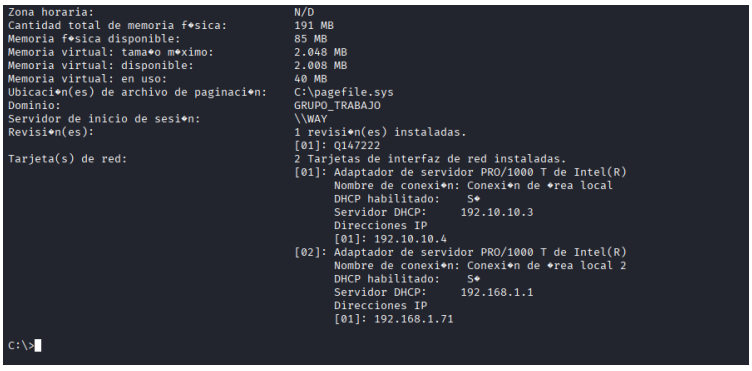


imagenes 50 ejecución del comando dir desde el directorio raíz

Ejecucion del comando systeminfo



imagenes 51 ejecucion del comando systeminfo



imagenes 52 comando systeminfo

Ejecucion del comando net users

```
C:\>net users
net users

Cuentas de usuario de \\WAY

-------------------------------------------------------------------------------
Administrador            Asistente de ayuda       Invitado
SUPPORT_388945a0         wayner_antonio_moya_
Se ha completado el comando correctamente.


C:\>
```

imagenes 53 comando net users

Ejecucion del comando tasklist

que nos sirve para:

Identificar procesos activos: Muestra el nombre del proceso, su PID (identificador de proceso), uso de memoria, y más.

Detectar software malicioso o no autorizado, Ayuda a encontrar procesos sospechosos que podrían estar ocultos o disfrazados.

```
C:\>tasklist
tasklist

Nombre de imagen             PID Nombre de sesi♦n N♦m. de  Uso de memor
========================= ===== ================ ======== ============
System Idle Process            0 Console                  0         16 KB
System                         4 Console                  0         76 KB
smss.exe                     400 Console                  0        144 KB
csrss.exe                    784 Console                  0      1.524 KB
winlogon.exe                 808 Console                  0      3.940 KB
services.exe                 852 Console                  0      1.908 KB
lsass.exe                    864 Console                  0      3.224 KB
VBoxService.exe             1028 Console                  0      2.248 KB
svchost.exe                 1084 Console                  0      2.908 KB
svchost.exe                 1184 Console                  0      2.544 KB
svchost.exe                 1428 Console                  0     12.796 KB
svchost.exe                 1476 Console                  0      2.308 KB
svchost.exe                 1520 Console                  0      2.060 KB
explorer.exe                2012 Console                  0     12.012 KB
spoolsv.exe                  208 Console                  0      2.048 KB
alg.exe                     1868 Console                  0      1.596 KB
VBoxTray.exe                 644 Console                  0      2.656 KB
ctfmon.exe                   616 Console                  0      1.516 KB
wscntfy.exe                 1796 Console                  0        876 KB
iexplore.exe                 320 Console                  0      7.404 KB
iexplore.exe                1516 Console                  0     17.092 KB
wuauclt.exe                 2268 Console                  0      2.340 KB
cmd.exe                     4068 Console                  0        100 KB
badblue.exe                 3364 Console                  0      6.608 KB
logon.scr                   4032 Console                  0      2.040 KB
cmd.exe                     3136 Console                  0      2.672 KB
tasklist.exe                1892 Console                  0      4.344 KB
```

CONCLUSIÓN

El estudio demostró que BadBlue 2.7/2.72 presenta vulnerabilidades críticas que permiten ejecución remota de comandos, lo cual representa una amenaza directa a la seguridad del sistema. Además, el uso de técnicas de camuflaje incrementa la dificultad de detección de archivos maliciosos o sensibles, afectando negativamente los procesos de auditoría y análisis forense. Se recomienda deshabilitar servicios obsoletos, aplicar parches de seguridad, implementar controles de red más estrictos y realizar escaneos periódicos para detectar artefactos ocultos. La combinación de explotación y esteganografía exige una respuesta integral que contemple tanto la prevención como la detección avanzada.